User Guide
Avaya VPN Gateway

8.0
NN46120-104, 03.04
March 2012

© 2012 Avaya Inc.

All Rights Reserved.

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: Preface 9
- Who Should Use This Book 9
- Related documentation 9
- Product Names 10
- How This Book Is Organized 10
  - Users Guide 10
  - Appendices 11
- Customer service 11
  - Getting product training 12
  - Getting help from a distributor or reseller 12
  - Getting technical documentation 12
  - Getting technical support from the Avaya Web site 12

Chapter 2: New in this release 13
- Features 13
  - Disable new IPSec Logins 13
- Other changes 13

Chapter 3: Introducing the VPN Gateway 15
- SSL Acceleration 15
- VPN 15
- Hardware Platforms 16
- Feature List 16
  - Software Features 16

Chapter 4: Introducing the ASA 310-FIPS 25
- HSM Overview 25
- Extended Mode vs. FIPS Mode 25
  - FIPS140-1 Level 3 Security 26
- The Concept of iKey Authentication 26
  - Types of iKeys 27
  - Wrap Keys for ASA 310-FIPS Clusters 27
  - Available Operations and iKeys Required 28
- Additional HSM Information 28

Chapter 5: Initial Setup 31
- Clusters 31
  - New and Join 31
  - Configuration is Replicated among Master AVGs 31
  - Clustering Over Multiple Subnets 32
- IP Address Types 32
  - Host IP Address 32
  - Management IP Address (MIP) 32
  - Virtual IP Address (VIP) 32
  - Portal IP Address 33
  - Real Server IP Address (RIP) 33
- Ports 33
- Interfaces 34

One-Armed Configuration ... 34
Two-Armed Configuration ... 34
Configuration at Boot Up ... 35
The Setup Menu ... 35
Installing an AVG in a New Cluster ... 36
Setting Up a One-Armed Configuration ... 36
Setting Up a Two-Armed Configuration ... 38
Complete the New Setup ... 40
Settings Created by the VPN Quick Setup Wizard ... 43
Joining a VPN Gateway to an Existing Cluster ... 45
Setting up a One-Armed Configuration ... 45
Setting up a Two-Armed Configuration ... 47
Complete the Join Setup ... 49
Installing an ASA 310-FIPS ... 50
Installing an ASA 310-FIPS in a New Cluster ... 50
Adding an ASA 310-FIPS to an Existing Cluster ... 55
Reinstalling the Software ... 60
Chapter 6: Upgrading the AVG Software ... 63
Performing Minor/Major Release Upgrades ... 63
Activating the Software Upgrade Package ... 65
Chapter 7: Managing Users and Groups ... 69
User Rights and Group Membership ... 69
Adding a New User ... 69
Adding Users through RADIUS ... 73
Changing a Users Group Assignment ... 74
Changing a Users Password ... 75
Changing Your Own Password ... 75
Changing Another Users Password ... 76
Deleting a User ... 77
Chapter 8: Certificates and Client Authentication ... 81
Generating and Submitting a CSR Using the CLI ... 81
Adding Certificates to the AVG ... 86
Copy-and-Paste Certificates ... 87
Copy-and-Paste Private Key ... 90
Using TFTP/FTP/SCP/SFTP to add Certificates and Keys ... 92
Update Existing Certificate ... 94
Create a New Certificate ... 94
Configure a Virtual SSL Server to Require a Client Certificate ... 95
Generating client certificates ... 97
Export Client Certificate ... 100
Transmit Private Key and Certificate to User ... 101
Managing Revocation of Client Certificates ... 102
Revoking Client Certificates Issued by an External CA ... 102
Revoking Client Certificates Issued within your Own Organization ... 103
Creating Your Own Certificate Revocation List ... 104
Automatic CRL Retrieval ... 106
Client certificate support ... 109

Signing CSRs ... 109
Generate Test Certificate ... 110
General Commands ... 111
Show Certificate Information ... 112
Show Subject Information ... 112
Check if Key and Certificate Match ... 112
Show Key Size ... 113
Show Key Information ... 113
Chapter 9: Virtual Desktop ... 115
Running the Virtual Desktop on Client Computers ... 115
Licensing vdesktop ... 115
Launch Vdesktop from Portal ... 116
Virtual Desktop Operations ... 116
Chapter 10: The Command Line Interface ... 119
Connecting to the VPN Gateway ... 119
Establishing a Console Connection ... 119
Establishing a Telnet Connection ... 120
Establishing a Connection Using SSH (Secure Shell) ... 121
Accessing the AVG Cluster ... 122
CLI vs. Setup ... 124
Command Line History and Editing ... 124
Idle Timeout ... 124
Chapter 11: Troubleshooting the AVG ... 127
Cannot Connect to VPN Gateway through Telnet or SSH ... 127
Verify the Current Configuration ... 127
Enable Telnet or SSH Access ... 128
Check the Access List ... 128
Check the IP Address Configuration ... 129
Cannot Add an AVG to a Cluster ... 130
Cannot Contact the MIP ... 130
Check the Access List ... 131
Add Interface 1 IP Addresses and MIP to Access List ... 131
The AVG Stops Responding ... 131
Telnet or SSH Connection to the Management IP Address ... 131
Console Connection ... 132
A User Password is Lost ... 132
Administrator User Password ... 132
Operator User Password ... 133
Root User Password ... 133
Boot User Password ... 133
An ASA 310-FIPS Stops Processing Traffic ... 133
Resetting HSM Cards on the ASA 310-FIPS ... 135
An ASA 310-FIPS Cluster Must be Reconstructed onto New Devices ... 137
A User Fails to Connect to the VPN ... 141
aaa ... 141
dns ... 142
ike ... 142

ipsec ... 143
ippool ... 143
ssl ... 143
tg ... 144
upref ... 144
smb ... 144
ftp ... 145
netdirect ... 145
netdirect_packet ... 145
User Unable to Connect to the VPN Gateway through the Net Direct Client ... 146
Cannot download the Net Direct Zipped file from client PC ... 148
System Diagnostics ... 148
Installed Certificates and Virtual SSL Servers ... 149
Network Diagnostics ... 149
Active Alarms and the Events Log File ... 151
Error Log Files ... 151
Unable to download Net Direct from VPN server ... 152
Appendix A: Supported Ciphers ... 153
Cipher List Formats ... 154
Modifying a Cipher List ... 155
Supported Cipher Strings and Meanings ... 155
Appendix B: The SNMP Agent ... 159
Supported MIBs ... 159
SNMPv2-MIB ... 160
SNMP-MPD-MIB ... 161
SNMP-FRAMEWORK-MIB ... 161
The SNMP-TARGET MIB ... 161
SNMP-NOTIFICATION-MIB ... 161
SNMP-VIEW-BASED-ACM-MIB ... 161
SNMP-USER-BASED-SM-MIB ... 162
S5-ETH-MULTISEG-TOPOLOGY-MIB ... 162
SYNOPTICS-ROOT-MIB ... 162
S5-TCS-MIB ... 162
S5-ROOT-MIB ... 162
IF-MIB ... 163
IP-MIB ... 163
IP-FORWARD-MIB ... 163
ENTITY-MIB ... 163
DISMAN-EVENT-MIB ... 164
ALTEON-ISD-PLATFORM-MIB ... 164
ALTEON-ISD-SSL-MIB ... 164
ALTEON-SSL-VPN-MIB ... 165
IANAifType-MIB ... 165
Supported Traps ... 165
Appendix C: Syslog Messages ... 167
List of Syslog Messages ... 167
Operating System (OS) Messages ... 167

System Control Process Messages ... 169
Traffic Processing Messages ... 172
Startup Messages ... 177
Configuration Reload Messages ... 178
AAA Subsystem Messages ... 179
IPsec Subsystem Messages ... 181
Syslog Messages in Alphabetical Order ... 185
Appendix D: License Information ... 209
Appendix E: HSM Security Policy ... 215
Rainbow Technologies CryptoSwift® HSM Cryptographic Accelerator ... 215
Scope ... 215
2.0 Applicable Documents ... 216
3.0 Overview ... 216
4.0 Capabilities ... 217
5.0 Physical Security ... 219
7.1 Module Interfaces ... 219
6.1 USB (Universal Serial Bus) Interface ... 219
6.2 Status LED (Light Emitting Diode) Interface ... 219
6.3 Serial Interface ... 220
6.4 PCI Interface ... 220
6.5 Backup Battery Interface ... 220
6.6 PCI Power Interface ... 220
7.1 Components ... 220
7.1 Bulk Crypto ... 220
7.2 Power Management and Tamper Detect ... 221
7.3 FastMap Processor ... 221
7.4 Flash ... 221
7.5 SRAM ... 221
7.6 Real Time Clock/Battery Powered RAM (RTC/BBRAM) ... 221
7.7 Programmable Logic Device (PLD) ... 222
7.8 USB (Universal Serial Bus) Controller ... 222
7.9 Universal Asynchronous Receiver Transmitter (UART) ... 222
7.10 33MHz Clock ... 222
8.0 Definition of Security Relevant Data Items ... 222
9.0 Roles and Services ... 223
9.1 Roles ... 223
9.2 Authentication ... 224
9.3 Initialization ... 224
9.4 User Creation ... 224
9.5 Services ... 225
10.0 Key Management ... 230
10.1 Key Generation ... 230
10.2 Key Storage ... 230
10.3 Key Entry and Output ... 230
10.4 Key Distribution ... 230
10.5 Key Destruction ... 231
10.6 Key Archiving ... 231

11.0 Modes ... 232
11.1 FIPS 140-1 Mode ... 232
11.2 Non-FIPS 140-1 Mode ... 232
12.0 Self-Tests ... 232
13.0 Conclusion ... 233
Appendix F: Definition of Key Codes ... 235
Syntax Description ... 235
Allowed Special Characters ... 235
Redefinable Keys ... 236
Example of a Key Code Definition File ... 237
Appendix G: SSH host keys ... 239
Methods for Protection ... 239
The VPN Gateway ... 239
Appendix H: Adding User Preferences Attribute to Active Directory ... 241
Install All Administrative Tools (Windows 2000 Server) ... 241
Register the Schema Management dll (Windows Server 2003) ... 241
Add the Active Directory Schema Snap-in (Windows 2000 Server and Windows Server 2003) ... 242
Create a Shortcut to the Console Window ... 244
Permit Write Operations to the Schema (Windows 2000 Server) ... 245
Create a New Attribute (Windows 2000 Server and Windows Server 2003) ... 245
Create New Class ... 246
Add isdUserPrefs Attribute to avayaSSLOffload Class ... 247
Add the avayaSSLOffload Class to the User Class ... 248
Appendix I: Using the Port Forwarder API ... 251
General ... 251
Creating a Port Forwarder ... 251
Demo Application ... 252
Creating a Port Forwarder Authenticator ... 253
Adding a Port Forwarder Logger ... 256
Connecting Through a Proxy ... 258
Monitoring the Port Forwarder ... 259
Status ... 259
Statistics ... 260
Glossary ... 261
Index ... 269

Chapter 1: Preface

The *Avaya VPN Gateway User Guide* describes how to perform basic configuration and maintenance of the Avaya VPN Gateway (AVG).

Who Should Use This Book

The *Avaya VPN Gateway User Guide* is intended for network installers and system administrators engaged in configuring and maintaining a network. It assumes that you are familiar with Ethernet concepts and IP addressing.

Related documentation

For full documentation on installing and using the many features available in the VPN Gateway software, see the following manuals:

- *Avaya VPN Gateway 8.0 Command Reference* describes each command in detail. The commands are listed per menu, according to the order they appear in the Command Line Interface (CLI).
- *Avaya VPN Gateway 8.0 Application Guide for SSL Acceleration* provides examples on how to configure SSL Acceleration through the CLI.
- *Avaya VPN Gateway 8.0 CLI Application Guide for VPN* provides examples on how to configure VPN deployment through the CLI.
- *Avaya VPN Gateway 8.0 BBI Application Guide for VPN* provides examples on how to configure VPN deployment through the BBI (Browser-Based Management Interface).
- *Avaya VPN Gateway 8.0 VPN Administrator Guide* — VPN management guide intended for end-customers in a Secure Service Partitioning configuration.
- *Avaya VPN Gateway 3050/3070 Hardware Installation Guide* describes installation of the VPN Gateway 3050 and 3070 hardware models.
- *Avaya VPN Gateway 8.0 Configuration-Secure Portable Office Client*
- *Avaya VPN Gateway 8.0 Troubleshooting Guide* describes the prerequisites and various tools used to troubleshoot the Avaya VPN Gateway (AVG).
- *Avaya VPN Gateway 8.0 Release Notes* Lists new features available in version 8.0 and provides up-to-date product information.

The preceding manuals are available for download (see Customer service on page 11).

Product Names

The software described in this manual runs on several different hardware models. Whenever the generic terms *Avaya VPN Gateway, VPN gateway or AVG* are used in the documentation, the following hardware models are implied:

- Avaya VPN Gateway 3050 (AVG 3050)
- Avaya VPN Gateway 3070 (AVG 3070)

Similarly, all references to the old product name – iSD-SSL or iSD – in commands or screen outputs should be interpreted as applying to the preceding hardware models.

Note:

Manufacturing of the Avaya SSL Accelerator (formerly Alteon SSL Accelerator) has been discontinued.

How This Book Is Organized

The chapters in this book are organized as follows:

Users Guide

Introducing the VPN Gateway on page 15 provides an overview of the major features of the VPN Gateway, including its physical layout and the basic concepts of its operation.

Introducing the ASA 310-FIPS on page 25 provides information about the ASA 310 equipped with HSM cards, as well as information about the available security modes and the concept of iKey authentication.

Initial Setup on page 31 describes how to install the AVG in a new cluster, and how to add an AVG to an existing cluster. The chapter also provides information about the concept of AVG clusters, as well as the usage and configuration of ports and networks within a cluster. A section describing how to reinstall the software is also included.

Upgrading the AVG Software on page 63 describes how to upgrade the AVG software for a minor release upgrade, and a major release upgrade, as well as upgrading from software versions earlier than 2.0.11.16 to version 3.0.7.

Managing Users and Groups on page 69 describes the management of users, groups, and passwords. The chapter also explains how the Administrator user role can be fully separated from the Certificate Administrator user role.

Certificates and Client Authentication on page 81 describes how to generate and prepare keys and certificates for use with the AVG.

The Command Line Interface on page 119 describes how to connect to the AVG and access the information and configuration menus.

Troubleshooting the AVG on page 127 provides suggestions for troubleshooting basic problems. Information about performing system diagnostics on the AVG is also included, as well as some operations related to the ASA 310-FIPS model.

Appendices

provides a list of ciphers supported in this product.

The SNMP Agent on page 159 provides information about the SNMP agent on the AVG, and which MIBs (Management Information Bases) are supported.

Syslog Messages on page 167, contains a list of all syslog messages that can be sent to a syslog server that is added to the AVG system configuration.

License Information on page 209 provides licensing information for the software used in this product.

HSM Security Policy on page 215 provides detailed information about the security policy of the CryptoSwift® HSM card that comes installed in the ASA 310-FIPS.

Definition of Key Codes on page 235 provides information about how to compile a keycode definition file to be used with the Terminal applet available on the Telnet/SSH tab (located under the Portal's Advanced tab).

SSH host keys on page 239 provides information about the purpose of SSH host keys and how they are used to protect the connection between the SSH client and the VPN Gateway.

Adding User Preferences Attribute to Active Directory on page 241 provides step-by-step instructions on how to add the User Preferences attribute to Active Directory. This is required to support storage of Portal bookmarks in Active Directory.

Using the Port Forwarder API on page 251 provides instructions on how to perform the tasks needed when using the Port Forwarder API. The Port Forwarder API is used to provide tunnels through the Avaya VPN Gateway (AVG) without the user having to start any applets from the Portal.

Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to http://www.avaya.com or go to one of the pages listed in the following sections.

Navigation

- Getting technical documentation on page 12
- Getting product training on page 12
- Getting help from a distributor or reseller on page 12
- Getting technical support from the Avaya Web site on page 12

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at http://www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to http://www.avaya.com/support.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at http://www.avaya.com/support.

Chapter 2: New in this release

The following sections detail what's new in *Avaya VPN Gateway User's Guide*, (NN46120-104) Release 8.0.

Features

See the following section for information about feature changes:

Disable new IPSec Logins

The option Disable new IPSec logins has been added to allow maintenance of the VPN Gateway without forcing current users to log-off. During the maintenance interval, new IPSec logins to the node can be redirected to the other nodes. When troubleshooting a login failure to a specific VPN host, contact the System Administrator for a status report on the host.

For more information, see Cannot Connect to VPN Gateway through Telnet or SSH on page 127.

Other changes

See the following sections for information about changes that are not feature-related:

- Avaya 2424-SSL switch and Avaya SSL VPN Module 1000 (SVM 1000) are not supported. The related information is deleted in the document.
- Added information about disk repartitioning in the section Performing Minor/Major Release Upgrades. See Performing Minor/Major Release Upgrades on page 63.

Comments? infodev@avaya.com

Chapter 3: Introducing the VPN Gateway

The Avaya VPN Gateway (AVG) software includes two major functionality groups:

- SSL Acceleration
- VPN

These features can be used separately or be combined. This *Avaya User's Guide* covers the basic tasks that need to be completed irrespective of which feature you wish to deploy.

SSL Acceleration

The VPN Gateway can function as a peripheral Secure Sockets Layer (SSL) offload platform that attaches to an Application Switch or a comparable switch from another vendor. (The VPN Gateway can also operate in standalone mode without being connected to a switch.)

The VPN Gateway performs a TCP three-way handshake with the client through the Application Switch and performs all the SSL encryption and decryption for the session. Combined with the load balancing features of the Application Switch, the VPN Gateway offloads SSL encryption/decryption functions from back-end servers.

For examples on how to configure the VPN Gateway for SSL Acceleration, see the *Avaya Application Guide for SSL Acceleration*.

For more information about the basic operations of the VPN Gateway, see the "Public Key Infrastructure and SSL" chapter in the *Avaya Application Guide for SSL Acceleration*.

VPN

The VPN feature supports remote access to intranet or extranet resources (applications, mail, files, intranet web pages) through a secure connection. What information should be accessible to the remote user after login is determined by access rules (ACLs).

The intranet's resources can be accessed in clientless mode, transparent mode or both:

- From any computer connected to the Internet (clientless mode). The remote user connects to the VPN Gateway through a secure SSL connection through the web browser. When successfully authenticated, the user can access services and resources on the intranet from a Web Portal provided by the VPN Gateway. Clientless mode also enables

download of the Net Direct client, a simple and secure method for accessing intranet resources through the remote user's native applications.

- From a computer with the Avaya VPN client (formerly Contivity VPN client) or the Avaya SSL VPN client installed (transparent mode).

For examples on how to configure the VPN Gateway for VPN deployment, see the *Avaya Application Guide for VPN*.

Hardware Platforms

The VPN Gateway software is supported on the following hardware platforms:

- Avaya VPN Gateway 3050 and 3070
- Avaya SSL Accelerator 310 and 410
- Avaya SSL Accelerator 310-FIPS, with FIPS-compliant Hardware Security Module (HSM). See Introducing the ASA 310-FIPS on page 25.

For a detailed technical specification of the hardware platforms, see the "Specifications" appendix in the *Avaya VPN Gateway 3050/3070 Hardware Installation Guide* and the *Avaya Alteon SSL Accelerator Hardware Installation Guide* respectively.

Note:

Manufacturing of the Avaya SSL Accelerator (formerly Alteon SSL Accelerator) has been discontinued.

Feature List

Software Features

Web Portal

- Web Portal interface for remote users accessing the VPN Gateway in clientless mode, that is, through the browser.
- Corporate resources available to users as preconfigured group links or accessible through the Portal tabs.
- Support for native Telnet and SSH (including X11 forwarding) access to intranet servers through terminal Java applet (available on the Portal's Advanced tab).

- Support for handling plugins, Flash and Java applets using HTTP proxy Java applet (available on the Portal's Advanced tab).
- Support for application tunneling (port forwarding) through SOCKS encapsulated in SSL (available on the Portal's Advanced tab).
- API provided for developing a custom application that automatically logs in the user to the desired VPN and executes a previously configured port forwarder link
- Support for customizing the Web Portal, for example, color, logo, language and company name.
- Three user views available (novice, medium and advanced) to limit access to Portal tabs.
- Support for automatic redirection of requests to another URL (Portal pass-through).
- Support for Portal bookmarks.
- Ability to specify domains for which single sign-on is allowed.
- Net Direct client (SSL). VPN client temporarily downloaded from the Portal and removed when the user exits the session. On Windows, Net Direct is also available as an installable client (setup.exe file).

Transparent Mode Access

Access to intranet resources in transparent mode, that is, without going through the Web Portal, is accomplished using Windows VPN clients installed on the client PCs. In this mode, remote users will experience network access as if sitting within the local area network. The following VPN clients are available:

- Avaya SSL VPN client (TDI and LSP version).
- Avaya VPN client (formerly the Contivity VPN client). Not supported on the ASA 310, ASA 310-FIPS and ASA 410 hardware models.
- Net Direct installable client.

Bandwidth Management

Bandwidth Management (BWM) enables administrators to allocate a portion of the available bandwidth for specific users or groups. The bandwidth policies take lower and upper bound. The lower bound (soft limit) is guaranteed and the upper bound (hard limit) is available according to the requirement. The BWM provides bandwidth policy management for user traffic and IPsec Passthrough. For more information about configuration, see *Avaya VPN Gateway CLI Application Guide*, (NN46120-101)

User Authentication

User authentication is supported using the following methods:

- RADIUS (including Challenge/Response)
- LDAP (including Microsoft Active Directory)
- NTLM (Windows NT Domain, including Microsoft Active Directory)
- Secure Computing SafeWord (RADIUS)
- Netegrity SiteMinder
- RSA SecurID (native or through RADIUS)
- RSA ClearTrust
- ActivCard (RADIUS)
- Novell NDS/eDirectory (LDAP)
- Client certificate authentication
- Local database authentication

User Authorization

User authorization is controlled through the user's group membership. Two different authorization profile types are supported:

- The base profile defines a group member's access rights to networks, services and paths.
- The extended profile (optional) also defines a group member's access rights depending on conditions related to the user's connection, for example, source network, authentication method, access method, client certificate installed and/or Tunnel Guard checks passed.

Client Security

- Tunnel Guard. Feature for checking the security aspects of the remote PC client, that is, installed antivirus software, DLLs, executables and so on.
- WholeSecurity support. Lets you enable a scan of the client PC before the remote user is allowed to log in to the VPN.
- User session auto-logoff.
- Cache and browser history automatically cleared (only for Internet Explorer).

Comments? infodev@avaya.com

Accounting and Auditing

- Support for logging user session start and stop messages to a syslog or RADIUS accounting server. The messages can include VPN ID, user name, gateway address, session ID, session time and cause of termination.
- Support for logging CLI and Web User Interface operations (for example, login, logout and executed operation) to a syslog or RADIUS accounting server.

Networking

- Supports creating multiple interfaces within a cluster, for example, to separate client traffic and management traffic.
- Support for clustering over multiple subnets.
- Supports assigning two physical network ports to one interface, to create a port failover (high availability) solution where one VPN Gateway is attached to two Application Switches.

Secure Service Partitioning

The AVG software provides the ability to partition a cluster of VPN Gateways into separate VPNs. This gives service providers (ISPs) the possibility to host multiple VPN end-customers on a shared Remote Access Services (RAS) platform. Requires a license.

- Supports hosting of up to 250 public termination points for end-customer SSL and IPsec VPNs.
- Secure VPN binding. Each VPN is bound to a private IP interface. VLAN tagging can be used when private IP address spaces overlap.
- Private network authentication. Existing authentication servers within the customer's private network can be used.
- Access control. Unique access rules can be specified for each user group in the various VPNs.
- Private network name resolution. If desired, private network DNS servers can be mapped to the VPN.
- Split administration. VPN Portal management is enabled for each VPN customer through a web interface, without exposing global administration access.
- High availability. The Secure Service Partitioning solution is compatible with the AVG cluster's high availability solutions.

Branch Office Tunnels

The AVG software provides the ability to configure IPsec-based *branch office* tunnels. Several peer-to-peer branch office tunnels can be configured for each virtual private network (VPN).

The following number of branch office tunnels can be configured per hardware model:

- AVG 3070: 2500
- AVG 3050: 1000

For example, a cluster of two AVG 3070s support 5000 branch office tunnels.

Portal Guard

Feature used to "convert" an existing HTTP site to generate HTTPS links, secure cookies and so on. The VPN Gateway will not only handle the SSL processing but also see to it that all existing web links are rewritten to HTTPS. This eliminates the need to rewrite each link manually. Requires a license.

SSL Acceleration

The AVG software also includes features for SSL acceleration. Note that these features in some cases require interoperation with an Application Switch.

- Supports accelerated SSL processing by offloading SSL encryption and decryption from backend servers.
- Supports load balancing of encrypted and unencrypted traffic for up to 256 backend servers, with health checking and persistent client connections.
- Ability to create multiple clusters of VPN Gateways, each capable of serving its own group of real servers.
- Supports rewriting of client requests.
- Ability to transmit additional information to the backend servers.
- Supports end-to-end encryption.
- Compatible with all Application Switches, Avaya Web Switches and comparable switches from other vendors.

SSL Acceleration is covered in the *Avaya Application Guide for SSL Acceleration*.

Scalability and Redundancy

- Support for 256 VPN Gateways per cluster
- Support for 256 virtual SSL servers
- Provides dynamic plug and play – VPN Gateways can be added to or removed from a cluster dynamically without disrupting network traffic
- Provides a single system image (SSI) – all VPN Gateways in a given cluster are configured as a single system
- High level of redundancy in the master/slave cluster design; even if three master VPN Gateways in a cluster would fail, additional slave AVGs will still be operational and can accept configuration changes

Certificate and Key Management

- Server and client authentication
- Generation and revocation of client certificates
- Automatic retrieval of certificate revocation lists (CRLs)
- Validation of private keys and certificates
- Generation of certificate signing requests (CSRs)
- Generation of self-signed certificates

Public Key Infrastructure

- RSA pair key generation
- Server certificate enrollment
- Server key and certificate import/export
- Key and certificate renewal

Supported Key and Certificate Formats

- PEM
- DER
- NET
- PKCS12

- PKCS8
- KEY(MS IIS4.0)

Supported Handshake Protocols

- SSL versions 2.0, 3.0
- TLS version 1.0

Hash Algorithms

- Message Digest 5 (MD5)
- SHA1

Cipher Suites

All ciphers covered by SSL version 2.0, 3.0 and TLS version 1.0, except the IDEA and FORTEZZA ciphers. Also see Supported Ciphers on page 153.

Management

- Web User Interface (HTTP or HTTPS).
- Command Line Interface (CLI) access through Telnet/SSH or serial port.
- SNMP version 1, version 2c and version 3.
- RADIUS authentication of CLI/BBI administrator users (including console access).

Statistics

- Statistics can be viewed per access method (SSL or IPsec) for the whole cluster as well as for specific VPN Gateways, SSL servers and VPNs.
- Support for histograms, for example, to measure transactions per second (TPS) and throughput.

Virtual Desktop

Symantec On-Demand Agent (SODA) provides a Virtual Desktop environment to secure Web-based applications and services. Virtual Desktop is a Java application that provides protection against lost or theft of sensitive information. Files created while in the virtual desktop are encrypted as they are saved to a hard drive or removable media. Integrating Virtual Desktop

with AVG will provide a secure environment for end users while accessing confidential information.

Secure Portable Office (SPO) Client

The SPO client provides VPN access from portable storage such as USB flash memory and CDROM.

The SPO client provides enhanced mobility, portability, and security compared to traditional VPN access methods. You can deploy and manage the SPO client from the AVG server to simplify SPO client maintenance and updates.

For more information about Secure Portal Office Client, see *Configuration - Secure Portable Client Guide*.

Comments? infodev@avaya.com

Chapter 4: Introducing the ASA 310-FIPS

This section provides information about the ASA 310-FIPS model, which comes installed with the HSM (Hardware Security Module) card. The HSM card complies with all the security requirements specified by the Federal Information Processing Standard (FIPS) 140-1, Level 3 standards. Each ASA 310-FIPSASA 310-FIPS device is equipped with two identical HSM cards.

Note:

When using the ASA 310-FIPS device in a cluster, remember that *all* AVG devices in the cluster must be of the ASA 310-FIPS ASA 310-FIPS model.

HSM Overview

The HSM card found on the ASA 310-FIPS model is an SSL accelerator, just like the ordinary CryptoSwift card found on the regular ASA 410 model. In addition to cryptographic acceleration, the HSM card brings extra security to sensitive operations and is designed to withstand physical tampering.

- The HSM card provides a secure storage area for cryptographic key information. The storage area is secured by a constantly monitored tamper detection circuit. If tampering is detected, the battery backup power to memory circuits on the card is removed. Critical security parameters, such as private keys that are in the storage area, will then be destroyed and rendered useless to the intruder.
- Any sensitive information that is transferred between two HSM cards within the same ASA 310-FIPS, or between any number of HSM cards within a cluster of ASA 310-FIPS devices, is encrypted using a shared secret stored (also known as a wrap key) on the HSM card.
- Some user operations require a two-phase authentication, which involves using both hardware tokens (called iKeys) and an associated password to provide an extra layer of security. For example, if the ASA 310-FIPSASA 310-FIPS is power cycled (as in the case of theft), no SSL traffic is processed until the operator logs in to the HSM card using both an iKey and the correct password.
- All cryptographic requests, such as generating private keys or performing encryption, are automatically routed to the HSM card by the AVG application and performed on the HSM card only.

Extended Mode vs. FIPS Mode

When installing the very first ASA 310-FIPS into a new cluster, you can choose to initialize the HSM cards in either Extended mode or FIPS mode. Extended mode is the default selection,

and is appropriate whenever your security policy does not explicitly require that you conform to the FIPS 140-1, Level 3 standard (see the following for more information).

The main difference between Extended mode and FIPS mode involves how private keys are handled. For both modes, all private keys are stored encrypted in the database on the ASA 310 FIPS. When the HSM card is initialized in Extended mode, the encrypted private key needed to perform a specific operation is transferred to the HSM card over the PCI bus. The private key is then decrypted on the HSM card itself, using the wrap key that was generated during the initialization and because stored on the card. The private key is thus never exposed in plain text outside the HSM card.

When the HSM card is initialized in FIPS mode, the encrypted private key needed to perform a specific operation is read from the database into RAM, together with the wrap key from the HSM card. The private key is then decrypted in RAM, where it remains accessible for subsequent operations.

Also, when the ASA 310-FIPS is initialized in FIPS mode, all private keys must be generated on the ASA 310-FIPS device itself. Importing private keys, or certificate files that contain private keys, is not allowed due to the FIPS security requirements. This means that certain CLI commands that are used for importing certificates and keys through a copy and paste operation, or through TFTP/FTP/SCP/SFTP, cannot be used when the ASA 310-FIPS is initialized in FIPS mode.

FIPS140-1 Level 3 Security

The HSM card contains all of the security requirements specified by the FIPS 140-1, Level 3 standards. FIPS 140-1 is a U.S. government standard for implementations of cryptographic modules, that is, hardware or software that encrypts and decrypts data or performs other cryptographic operations (such as creating or verifying digital signatures).

FIPS 140-1 is binding on U.S. government agencies deploying applications that use cryptography to secure sensitive but unclassified (SBU) information, unless those agencies have been specifically exempted from compliance by the relevant U.S. laws referenced in the standard.

For more information about the FIPS specification, visit http://csrc.nist.gov/publications/fips/index.htmland scroll down to "FIPS 140-1".

The Concept of iKey Authentication

Access to sensitive data on a ASA 310-FIPS is protected by a combination of hardware tokens (called iKeys), passwords, and encryption procedures.

The iKey is a cryptographic token that is used as part of the authentication process for certain operations involving the HSM cards. Whenever you perform an operation on the ASA 310-FIPS calling for iKey authentication, you are prompted by the Command Line Interface to insert

Comments? infodev@avaya.com

the requested iKey into the USB port on the appropriate HSM card. (When prompted for a particular iKey, a flashing LED always directs you to the correct HSM card.)

Types of iKeys

For each HSM card there are two unique iKeys used for identity-based authentication: the HSM-SO iKey, and the HSM-USER iKey. Each of these iKeys define the two user roles available: Security Officer and User. A password must be defined for each user role, and the passwords are directly associated with the corresponding iKey. The ASA 310-FIPS is equipped with two HSM cards, and you therefore need to maintain two pairs of HSM-SO and HSM-USER iKeys with their associated passwords for each single ASA 310-FIPS ASA 310-FIPS device.

After a HSM card has been initialized, that card will only accept the HSM-SO and HSM-USER iKeys that were used when initializing that particular card. You cannot create backup copies of the associated HSM-SO iKey and HSM-USER iKey, and a lost HSM-SO or HSM-USER password cannot be retrieved. It is therefore extremely important that you establish routines for how the iKeys are handled.

Wrap Keys for ASA 310-FIPS Clusters

In addition to the HSM-SO and HSM-USER iKeys specific for each HSM card, one pair of iKeys (the black HSM-CODE iKeys) need also be maintained for each cluster of ASA 310-FIPS units.

Note:

You are strongly recommended to label two of the black HSM-CODE iKeys "CODE-SO" and "CODE-USER" respectively; these iKeys will be referred to as such both in the documentation and in the Command Line Interface.

During the initialization of the first ASA 310-FIPS in a cluster, a *wrap key* is automatically generated. The wrap key is a secret shared among all ASA 310-FIPS in the cluster. It encrypts and decrypts sensitive information that is sent over the PCI bus within an ASA 310-FIPS, and over the network among the ASA 310-FIPS devices in the cluster. By inserting the CODE-SO iKey and the CODE-USER iKey in turns when requested by the Setup utility, the wrap key is split onto these two iKeys. When adding an additional ASA 310-FIPS to the cluster, the CODE-SO and the CODE-USER iKeys are used to transfer the wrap key to the HSM cards on AVG device(s) that have been added. Once the wrap key has been transferred, all synchronization of sensitive information within the cluster takes place transparently to the user.

No passwords are associated with the CODE-SO and CODE-USER iKeys. However, for all operations that involves using the CODE-SO and CODE-USER iKeys, these keys are used in *addition* to the HSM-SO and HSM-USER iKeys (which in turn require the correct passwords for successful authentication).

Caution:

If you enter the wrong password for the HSM-USER fifteen (15) times in a row, the HSM-USER iKey will be rendered unusable. This is due to the strict security specifications placed on the ASA 310-FIPS.

Available Operations and iKeys Required

For information about the type of iKeys required to perform a specific operation, see Table 1: Available Operations and iKeys Required on page 28.

Table 1: Available Operations and iKeys Required

	Type of iKey Required		
Operation Performed	**HSM-SO**	**HSM-USER**	**CODE-SO and CODE-USER**
Installing a new ASA 310-FIPS in a new cluster	■	■	■
Adding an ASA 310-FIPS to an existing cluster	■	■	■
Logging in to the HSM card		■	
Splitting the wrap key onto a pair of CODE iKeys	■	■	■
Changing the HSM-SO iKey password **Note:** To resume normal operations after having changed the HSM-SO iKey password, the HSM-USER iKey is required to re-login to the HSM card.	■	■	
Changing the HSM-USER iKey password		■	

Additional HSM Information

- For detailed information about installing a new ASA 310-FIPS ASA 310-FIPS in a new cluster or adding an ASA 310-FIPS ASA 310-FIPS in an existing cluster, see Installing an ASA 310-FIPS on page 50.
- For detailed information about how to log in to the HSM card after a reboot, see An ASA 310-FIPS Stops Processing Traffic on page 133.

- For information about how to split the wrap key onto a backup set of CODE-SO and CODE-USER iKeys, or how to change an HSM-SO or HSM-USER iKey password, see the Hardware Security Module Menu under the Maintenance Menu in the *User's Guide*.
- For information about how to reset the HSM cards, see Resetting HSM Cards on the ASA 310-FIPS on page 135.
- For information about HSM card LED status, see Chapter 1 of the *Hardware Installation Guide*.
- For information about the HSM card's security policy, see HSM Security Policy on page 215 .
- To view the HSM card's FIPS 140-1 validation certificate, see Appendix B, "FIPS 140-1 Validation Certificate" in the *Hardware Installation Guide*

Comments? infodev@avaya.com

Chapter 5: Initial Setup

This chapter covers the basic setup and initialization process for the Avaya VPN Gateway (AVG). It introduces the concept of *clusters*, and provides detailed instructions for reinstalling the VPN Gateway software, should it become necessary.

Clusters

All VPN Gateways are members of a *cluster*. A cluster can consist of one single VPN Gateway or a group of AVGs that share the same configuration parameters. There can be more than one AVG cluster in the network, each with its own set of parameters and services. If the VPN Gateway is used for SSL Acceleration, each cluster can be set up to serve different real servers.

New and Join

Each time you perform an initial setup of an VPN Gateway and select

`new`

in the Setup menu, you create a new cluster which initially only has one single member. You can add one or more VPN Gateways to any existing cluster by performing an initial setup and select

`join`

in the Setup menu.

Configuration is Replicated among Master AVGs

The configuration parameters are stored in a database, which is replicated among the VPN Gateways designated as masters in a cluster. By default, the first four VPN Gateways in a given cluster are set up as masters. Additional AVGs are automatically set up as slaves, which means they depend on a master AVG in the same cluster for proper configuration. However, even if three of the masters fail, the remaining (AVGs) are still operational and can have configuration changes made to them. Note that one master at a minimum has to be functional to be able to make configuration changes. If all masters have failed, the slaves will still be capable of processing SSL traffic.

Clustering Over Multiple Subnets

The SSL VPN software supports clustering over multiple subnets. If more than one VPN Gateway is required and the VPN Gateway you wish to join to the cluster is installed in a different subnet, the new AVG must be configured as a slave. Master AVGs cannot exist on different intranet subnets.

IP Address Types

When configuring the VPN Gateway you will come across quite a number of IP address types. Following are the most commonly used:

Host IP Address

Each VPN Gateway can be assigned one or several host (machine) IP addresses for network connectivity. You will be asked to enter a host IP address when performing the initial setup.

Management IP Address (MIP)

When you create a new cluster you will be prompted for a Management IP (MIP) address, which is an IP alias to one of the VPN Gateways in the cluster. The MIP address identifies the cluster and is used when making configuration changes through Telnet or SSH or when configuring the system using the Browser-Based Management Interface (BBI). The MIP always resides on a master VPN Gateway. If the master AVG that currently holds the MIP should fail, the MIP automatically migrates to a functional master AVG.

Virtual IP Address (VIP)

When the VPN Gateway is used in conjunction with an Application Switch. For example, for SSL acceleration, the client connects to the VIP on the Application Switch. The VIP is used by the Application Switch to load balance particular service requests (like HTTP) to other servers.

Comments? infodev@avaya.com

Portal IP Address

When the VPN Gateway is used to set up a web Portal, the Portal IP address is the address that is assigned to the VPN Gateway's portal server. To display the web Portal, the remote user should enter the Portal IP address or the corresponding domain name in the available browser.

Real Server IP Address (RIP)

When the VPN Gateway is used for SSL Acceleration, the RIP is the IP address of the real server, sometimes called the backend server. It is the IP address that the Application Switch load balances to when requests are made to a virtual server IP address (VIP). The VPN Gateway's host IP address will in fact be one of the switch's RIPs.

Ports

When installing a VPN Gateway (or any of the other supported hardware models) in a new cluster, or adding a VPN Gateway to an existing cluster, you are asked to specify a port number by the Setup utility.

The port number you specify refers to a physical port on the Network Interface Card (NIC) of a particular hardware model.

Depending on your model, the Setup utility will automatically detect the number of available ports and display the valid range within square brackets when prompting for a port number.

- The VPN Gateway 3050 has four copper port NICs (numbered as 1-4).
- The VPN Gateway 3070 comes in two versions:
  - One with four copper port NICs (numbered as 1-4).
  - One with two copper port NICs (number as 1-2) and two fiber-optic ports (numbered as 3-4).
- The ASA 410 Copper NIC has two copper port NICs (numbered as 1-2).
- The ASA 410 Fiber NIC has two copper port NICs (numbered as 1-2) and one Gigabit fiber-optic port NIC for Gigabit Ethernet (numbered as 3).
- The ASA 310-FIPS has two copper port NICs (numbered as 1-2).

Each port should be marked with the appropriate number on the device. If not, see the *Alteon SSL Accelerator 310, 310-FIPS, 410 Hardware Installation Guide* and the *VPN 3050/3070 Hardware Installation Guide* respectively.

Interfaces

During the initial setup procedure (see Configuration at Boot Up on page 35), you will be asked if you want to set up a one-armed configuration or a two-armed configuration.

One-Armed Configuration

In a one-armed configuration, only one interface is configured. It acts as both a public interface (facing the Internet) and a private interface (facing the intranet).

The interface (Interface 1) on the SSL VPN will handle public traffic, that is, client traffic from and to the Internet, as well as private traffic, that is, connecting the SSL VPN to internal resources and configuring the SSL VPN from a management station.

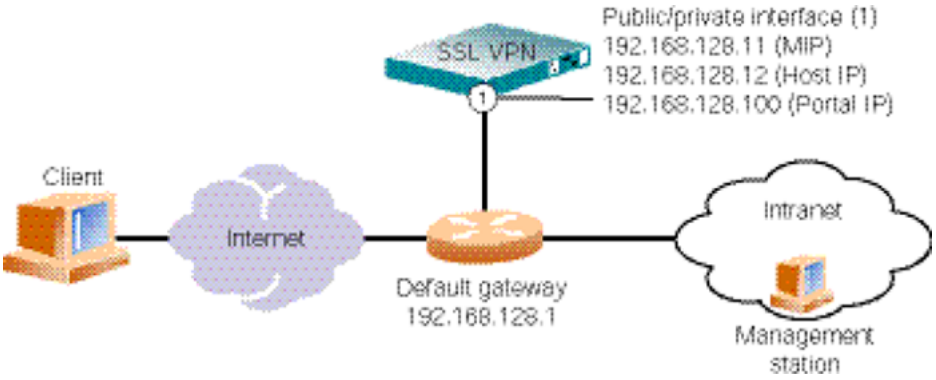


Figure 1: One-Armed Configuration without Application Switch

Two-Armed Configuration

In a two-armed configuration, two separate interfaces are configured on the VPN Gateway.

Interface 1 will handle private traffic (between the SSL VPN and the trusted intranet), that is, connecting the SSL VPN to internal resources and configuring the SSL VPN from a management station.

Interface 2 will handle public traffic, that is, client traffic from and to the Internet.

A two-armed configuration is considered more secure.

Comments? infodev@avaya.com

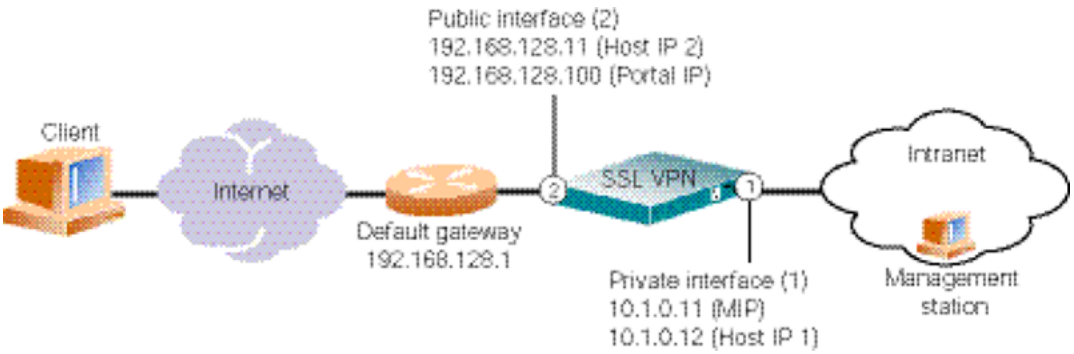


Figure 2: Two-Armed Configuration without Application Switch

Configuration at Boot Up

When starting a VPN Gateway for the very first time, you need to do the following:

- Connect the device's uplink port(s) to the appropriate network device(s). During the initial setup you will be asked to configure the desired ports for network connectivity.
  - To use the VPN Gateway with an Application Switch, for example, for SSL Acceleration, connect the uplink port to a compatible port on an Application Switch.
- Connect a computer to the VPN Gateway's console port through serial cable.
- Use a terminal application (for example, TeraTerm) to configure the VPN Gateway. For more information, see Connecting to the VPN Gateway on page 119.
- Press the power-on button on the VPN Gateway.
- Wait until you get a login prompt.
- Log in as `user: admin`, `password: admin`

Note:

If you have the ASA 310-FIPS model, see the instructions from Installing an ASA 310-FIPS on page 50 page 54 and onwards.

The Setup Menu

When you log in after having started the VPN Gateway the first time, you will enter the Setup menu. After selecting

```
new
```

or

```
join
```

, you will be prompted for the information required to make the VPN Gateway operational.

Table 2: The Setup Menu

```
[Setup Menu]

join          - Join an existing iSD cluster

new           - Initialize iSD as a new installation

boot          - Boot menu

Info          - Information menu

exit          - Exit  [global command, always available]
```

Installing an AVG in a New Cluster

When you are installing a VPN Gateway as the first (or only) member in a new cluster, you can either create a one-armed or a two-armed configuration.

Setting Up a One-Armed Configuration

In a one-armed configuration, only one interface is configured. It is used as both the public (traffic) and the private (management) interface. See figure on Two-Armed Configuration on page 34.

1. Choose new from the Setup menu.

```
[Setup Menu]
join          - Join an existing iSD cluster
new           - Initialize iSD as a new installation
boot          - Boot menu
info          - Information menu
exit          - Exit  [global command, always available]

>> Setup#new

Setup will guide you through the initial configuration.
```

2. Specify the port you want to use for network connectivity.

Comments? infodev@avaya.com

```
Enter port number for the management interface [1-4]:1
```

This port will be assigned to Interface 1. As you are currently configuring a one-armed setup, this interface will be used for both private traffic (for example, SSL VPN management and connections to intranet resources) and public traffic (for example, client connections from the Internet).

3. Specify the current host IP address of the VPN Gateway.

```
Enter IP address for this machine (on management interface):<IP address>
```

This IP address must be unique on your network and be within the same network address range as the Management IP address. The host IP address will be assigned to Interface 1.

You can later use the **`/cfg/sys/host 1/interface 1`** command to view the resulting settings for Interface 1.

Note:

If needed, you can later create a two-armed configuration by adding a new interface to the cluster, exclusively used for client traffic, and assign an unused port to that interface. For information about how to add a new interface, see the "Interface Configuration " section under Configuration Menu>System Configuration in the *Avaya Command Reference*. For information about how to assign ports to an interface, see the "Interface Ports Configuration " section in the same chapter.

4. Enter network mask and VLAN tag ID.

```
Enter network mask [255.255.255.0]:<Press ENTER if correct>

Enter VLAN tag id (or zero for no VLAN) [0]:<VLAN tag id or ENTER>
```

Specify the desired network mask or accept the suggested value by pressing ENTER. If a connected router or switch attaches VLAN tag IDs to incoming packets, specify the VLAN tag ID used.

5. Press ENTER to continue with creating a one-armed configuration.

```
Setup a two armed configuration (yes/no) [no]:<Press ENTER>
```

6. Enter a default gateway address.

```
Enter default gateway IP address (or blank to skip):<gateway IP address>
```

Enter a default gateway IP address that is within the same network address range as the host IP address configured in step 3.

7. Enter a Management IP address (MIP).

   Enter a unique Management IP address (MIP) that is within the same network address range as the host IP address and the default gateway IP address.

```
Enter the Management IP (MIP) address:<IP address>

Making sure the MIP does not exist...ok
Trying to contact gateway...ok
```

   Complete the

   `new`

   setup by following the instructions in the section Complete the New Setup on page 40.

Setting Up a Two-Armed Configuration

In a two-armed configuration, two separate interfaces are configured on the VPN Gateway, one private interface for AVG management and intranet connections and one public interface for Internet connections. Also see figure on Two-Armed Configuration on page 34.

1. Choose `new` from the Setup menu.

```
[Setup Menu]
join          - Join an existing iSD cluster
new            - Initialize iSD as a new installation
boot          - Boot menu
info          - Information menu
exit          - Exit     [global command, always available]
>> Setup# new

Setup will guide you through the initial configuration of the
iSD.
```

2. Configure the management interface port number.

```
Enter port number for the management interface [1-4]:1
```

   Specify the port you want to use for AVG management and other private traffic between the VPN Gateway and the intranet. This port will be assigned to the private interface (Interface 1).

3. Specify the host IP address for the current VPN Gateway.

Comments? infodev@avaya.com

```
Enter IP address for this machine (on management interface):<IP
address>
```

Specify a host IP address on the management (private) interface. This IP address must be unique on the network and be within the same network address range as the Management IP address (see step 10 on page 40). The management interface host IP address is assigned to Interface 1.

4. Enter network mask and VLAN tag ID.

```
Enter network mask [255.255.255.0]:<Press ENTER if correct>

Enter VLAN tag id (or zero for no VLAN) [0]:<VLAN tag id or ENTER>
```

Specify the desired network mask for the host IP address on the management interface or accept the suggested value by pressing ENTER. If a connected router or switch attaches VLAN tag IDs to incoming packets, specify the VLAN tag ID used.

5. Enter `yes` and press ENTER to continue with creating a two-armed configuration.

```
Setup a two armed configuration (yes/no) [no]:yes
```

6. Specify a new port number for the traffic interface.

```
Enter port number for the traffic interface [1-4]:2
```

The traffic (public) interface port number will automatically be assigned to Interface 2.

7. Specify a host IP address on the traffic (public) interface.

```
Enter IP address for this machine (on traffic interface):<IP
address>
```

This IP address will be assigned to Interface 2 on the VPN Gateway, that is, the public interface.

8. Enter network mask and VLAN tag ID.

```
Enter network mask [255.255.255.0]:
Enter VLAN tag id (or zero for no VLAN) [0]:
```

Specify the desired network mask for the host IP address on the traffic interface or accept the suggested value by pressing ENTER. If a connected router or switch attaches VLAN tag IDs to incoming packets, specify the VLAN tag ID used.

9. Enter a default gateway address on the traffic interface.

```
Enter default gateway IP address (on the traffic
interface):<gateway IP address>
```

Specify a default gateway IP address that is within the same network address range as the host IP address on the traffic (public) interface.

10. Enter a Management IP address (MIP) on the management interface.

```
Enter the Management IP (MIP) address:<IP address>

Making sure the MIP does not exist...ok
Trying to contact gateway...ok
```

Finally enter a unique Management IP address (MIP) that is within the same network address range as the host IP address on the management (private) interface.

Complete the new setup by following the instructions in the next section, "Complete the New Setup".

Complete the New Setup

1. Configure the time zone and NTP and DNS server settings.

   If you don't have access to the IP address of an NTP server at this point, you can configure this item after the initial setup is completed. See the "NTP Servers Configuration" section under Configuration menu>System Configuration in the *Avaya Command Reference*.

```
(new setup, continued)

Enter a timezone or 'select' [select]:<Press ENTER to select>

Select a continent or ocean:<Continent or ocean by number>

Select a country:<Country by number>

Select a region:<Region by number, if applicable>

Selected timezone:<Suggested timezone, based on your selections>

Enter the current date (YYYY-MM-DD) [2006-03-01]:<Press ENTER if
correct>
```


Comments? infodev@avaya.com

```
Enter the current time (HH:MM:SS) [09:26:16]:<Press ENTER if
correct>

Enter NTP server address (or blank to skip):<IP address>

Enter DNS server address:<IP address>
```

2. Generate new SSH host keys and define a password for the admin user.

   To maintain a high level of security when accessing the VPN Gateway through an SSH connection, it is recommended that you accept the default choice to generate new SSH host keys.

   Make sure you remember the password you define for the admin user. You will need to provide the correct admin user password when logging in to the cluster for configuration purposes, and also when adding another VPN Gateway to the cluster by performing a join in the Setup menu.

```
(new setup, continued)

Generate new SSH host keys (yes/no) [yes]:<Press ENTER to accept>

This may take a few seconds...ok
Enter a password for the "admin" user:
Re-enter to confirm:
```

3. If you will be using the VPN feature, run the VPN quick setup wizard to set up a working VPN for SSL access in a few steps.

   The VPN quick setup wizard creates all the settings required to enable a fully functional Portal for testing purposes. You can later let your test Portal evolve to a fully operative Portal.

```
Run VPN quick setup wizard [yes]:<press ENTER to run the wizard>

   Creating default networks under /cfg/vpn 1/aaa/network
Creating default services under /cfg/vpn 1/aaa/service
Enter VPN Portal IP address:<IP address>

Is this VPN device used in combination with an Alteon switch?
[no]: Enter comma separated DNS search list
(eg company.com,intranet.company.com):example.com

Create HTTP to HTTPS redirect server [yes]:<press ENTER to accept>

Create a trusted portal account [yes]:<press ENTER to create the
account>

User name:john

User password:password
```

```
   Creating group 'trusted' with secure access.
Creating user 'john' in group 'trusted'.
Creating empty portal linkset 'base-links' for group trusted.
```

- VPN Portal IP address. Used by remote users to connect to the VPN.
- DNS search list. Enables use of short names on the Portal, for example,

  `inside`

  to connect the server inside.example.com.
- HTTP to HTTPS redirection. Automatically redirects requests made with HTTP to the proper HTTPS server configured for the VPN, for example, http://vpn.example.com gets redirected to https://vpn.example.com.

To view all settings created by the VPN quick setup wizard, see Settings Created by the VPN Quick Setup Wizard on page 43.

4. To configure IPsec access in your VPN, run the IPsec quick setup wizard.

   With IPsec access enabled, remote users can access the VPN through a secure IPsec tunnel using the Avaya VPN client (formerly Contivity).

```
Setup IPsec [no]:yes

     Creating default IKE profile under ipsec/ikeprof 1
Creating default user tunnel profile under ipsec/utunprof 1
Configuring IPsec Group login under aaa/group trusted/ipsec
Do you want to use IPsec Group login [no]:yes

Enter IPsec secret:secret

Enter Lower IP address in pool range:10.10.10.1

Enter Upper IP address in pool range:10.10.20.99

Enter Network mask for the pool range: [255.255.255.0]:16

     Creating IP pool 1
```

- IPsec group login and secret. Enables IPsec access for the trusted group, if this group was created with the VPN quick setup wizard (see step 3 on page 41).
- Lower/upper IP address in pool range. Lets you specify an IP address range for use in the unencrypted connection between the VPN Gateway and the destination host.
- Network mask for IP pool range. Lets you enter a custom network mask if the default network mask does not cover the pool range.

Comments? infodev@avaya.com

Note:

The IPsec quick setup wizard is only displayed if the VPN quick setup wizard has been run and if the VPN Gateway has a default IPsec license (not available on the ASA 310 models).

5. When the Setup utility has finished you can continue with the configuration.

   If you wish to continue configuring the system through the command line interface (CLI), log in as the admin user with the password you defined in , and the Main menu is displayed. For more information about the CLI, see step 2 on page 41.

   If you rather configure the system through the Browser-Based Management Interface (BBI), see the *Avaya BBI Quick Guide* for instructions.

```
Initializing system......ok
Setup successful. Relogin to configure.
login:
```

   For instructions on how to deploy a pure VPN solution, continue with the "VPN Introduction" chapter in the *Application Guide for VPN*. For instructions on how to deploy the SSL acceleration feature, continue with the "Basic Applications" chapter in the *Application Guide for SSL Acceleration*.

   To join an additional VPN Gateway to the cluster, see Joining a VPN Gateway to an Existing Cluster on page 45.

Settings Created by the VPN Quick Setup Wizard

If you ran the VPN quick setup wizard during the initial setup, a large number of settings were configured automatically.

Basic VPN Setup

The following settings have been created:

- A VPN. The VPN is typically defined for access to an intranet, parts of an intranet or to an extranet.
- A virtual SSL server of the portal type. A portal IP address is assigned to it, to which the remote user should connect to access the Portal. If you chose to use the VPN feature without an Application Switch, the portal server is set to standalone mode.
- A test certificate has been installed and mapped to the portal server.
- The authentication method is set to Local database and you have one test user configured. The test user belongs to a group called

  `trusted`

, whose access rules allow access to all networks, services and paths.

- One or several domain names are added to the DNS search list, which means that the remote user can enter a short name in the Portal's various address fields (for example, inside instead of inside.example.com if example.com is added to the search list).
- If you chose to enable HTTP to HTTPS redirection, an additional server of the HTTP type was created to redirect requests made with HTTP to HTTPS, because the portal server requires an SSL connection.

Default Network

The wizard also creates a default network definition called **intranet**. In short, network definitions are used to limit a remote user's access rights to different networks. Once a network definition has been created it can be referenced in an access rule. The access rule states whether access to the referenced network should be rejected or allowed.

Network definitions can be created, viewed or edited using the **`/cfg/vpn #/aaa/network`** command. See the "Groups, Access Rules and Profiles" chapter in the *Application Guide for VPN* for a full explanation of network definitions in conjunction with access rules.

The **intranet** network definition is configured as Network 1. The subnets included in **intranet** are based on private IP address space reservations as defined in the RFC 1918 document:

- Network address: 192.168.0.0 Network mask: 255.255.0.0
- Network address: 10.0.0.0 Network mask: 255.0.0.0
- Network address: 172.16.0.0 Network mask: 255.240.0.0

Default Services

The following service definitions were configured automatically. Service definitions can be referenced in access rules to allow or deny access to a specific application or protocol. Service definitions can be viewed or edited using the **`/cfg/vpn #/aaa/service`** command.

See the "Groups, Access Rules and Profiles" chapter in the *Application Guide for VPN* for a full explanation of service definitions.

- **http.** Uses TCP port 80.
- **https.** Uses TCP port 443.
- **web.** Uses TCP ports 20, 21, 80 and 443.
- **smtp.** Uses TCP port 25.
- **pop3.** Uses TCP port 110.
- **imap.** Uses TCP port 143.
- **email.** Uses TCP ports 25, 110 and 443.

Comments? infodev@avaya.com

- **telnet.** Uses TCP port 23.
- **ssh.** Uses TCP port 22.
- **ftp.** Uses TCP ports 20 and 21.
- **smb.** Uses TCP port 139.
- **fileshare.** Uses TCP ports 20, 21 and 139.

Joining a VPN Gateway to an Existing Cluster

After having installed the first VPN Gateway in a cluster, additional AVGs may be added to the same cluster by specifying the Management IP address (MIP) that identifies the cluster. When you are installing the VPN Gateway to join an existing cluster, less information is needed because the new VPN Gateway will fetch most of the configuration from the other AVG(s) in the cluster.

The following applies when joining a new VPN Gateway to an existing cluster:

- If the VPN Gateway you are about to join is installed on a different subnet than existing AVGs, this new device must be configured as a slave. Master AVGs cannot exist on different subnets.
- If the Access list consists of entries (for example, IP addresses for control of Telnet and SSH access), also add the cluster's MIP, the existing VPN Gateway's host IP address on Interface 1, and the host IP address you have in mind for the new AVG to the Access list. This must be done before joining the new VPN Gateway, otherwise the devices will not be able to communicate. Use the **`/cfg/sys/accesslist`** command. If the Access list is empty, this step is not required.
- If the VPN Gateway you are about to join has a different software version than existing AVGs, install the preferred software version on the new VPN Gateway before joining it (see Reinstalling the Software on page 60) or upgrade the whole cluster to the same software version as the new VPN Gateway (see Performing Minor/Major Release Upgrades on page 63). Use the **`/boot/software/cur`** command to check the currently installed software version.

Setting up a One-Armed Configuration

If the currently installed VPN Gateway(s) in the cluster are set up for a one-armed configuration you probably want the new VPN Gateway to be set up similarly.

When you log in after having started the VPN Gateway the first time, you will enter the Setup menu.

1. Choose `join` from the Setup menu to add a VPN Gateway to an existing cluster.

```
[Setup Menu]
join          - Join an existing iSD cluster
new            - Initialize iSD as a new installation
boot          - Boot menu
info          - Information menu
exit          - Exit     [global command, always available]
>> Setup#join

Setup will guide you through the initial configuration of the
iSD.
```

2. Specify the port to be used for network connectivity.

```
Enter port number for the management interface [1-4]:1
```

This port will automatically be assigned to Interface 1. As you are currently configuring a one-armed configuration, this interface will be used for both management traffic (coming from the private intranet) and client traffic (coming from the public Internet).

If you have configured port 1 as the management interface port for existing VPN Gateways, it is recommended (for consistency) that you configure port 1 for the AVG you are joining as well.

3. Enter the VPN Gateway 's host IP address.

```
Enter IP address for this machine (on management interface):<IP
address>
```

This IP address should be within the same network address range as the cluster's Management IP address.

4. Enter network mask and VLAN tag ID.

```
Enter network mask [255.255.255.0]:<Press ENTER if correct>

Enter VLAN tag id (or zero for no VLAN) [0]:<VLAN tag id or ENTER>
```

Specify the desired network mask or accept the suggested value by pressing ENTER. If a connected router or switch attaches VLAN tag IDs to incoming packets, specify the VLAN tag ID used.

5. Press ENTER to continue with creating a one-armed configuration.

```
Setup a two armed configuration (yes/no) [no]:<Press ENTER>
```

6. Enter the Management IP address (MIP) of the existing cluster.

Comments? infodev@avaya.com

```
The system is initialized by connecting to the management server
on an existing iSD, which must be operational and initialized.
Enter the Management IP (MIP) address:<IP address>
```

Provide the Management IP address of the cluster to which you want to join the current VPN Gateway. To check the Management IP of an existing cluster, connect to the cluster and use the **`/cfg/sys/cur`** command.

Complete the join setup by following the instructions in the section Complete the Join Setup on page 49.

Setting up a Two-Armed Configuration

If the currently installed VPN Gateway(s) in the cluster are set up for a two-armed configuration you probably want the new VPN Gateway to be set up like the previously installed AVG(s).

To set up a two-armed configuration, proceed as follows:

1. Choose `join` from the Setup menu.

```
[Setup Menu]
join          - Join an existing iSD cluster
new            - Initialize iSD as a new installation
boot          - Boot menu
info          - Information menu
exit          - Exit     [global command, always available]
>> Setup#join

Setup will guide you through the initial configuration of the
iSD.
```

2. Configure the management interface port number.

```
Enter port number for the management interface [1-4]:1
```

Specify the port you want to use for management traffic. This port will be assigned to an interface for management purposes only (Interface 1).

3. Specify a host IP address on the management interface for the current VPN Gateway.

```
Enter IP address for this machine (on management interface):<IP
address>
```

This IP address must be unique on the network and be within the same network address range as the Management IP address (see step 9 on page 48). The management interface host IP address will be assigned to Interface 1.

4. Enter network mask and VLAN tag ID.

```
Enter network mask [255.255.255.0]:<Press ENTER if correct>

Enter VLAN tag id (or zero for no VLAN) [0]:<VLAN tag id or ENTER>
```

   Specify the desired network mask for the host IP address on the management interface or accept the suggested value by pressing ENTER. If a connected router or switch attaches VLAN tag IDs to incoming packets, specify the VLAN tag ID used.

5. Enter `yes` and press ENTER to continue with creating a two-armed configuration.

```
Setup a two armed configuration (yes/no) [no]:yes
```

6. Specify a new port number for the traffic interface.

```
Enter port number for the traffic interface [1-4]:2
```

   The traffic interface port number will automatically be assigned to Interface 2.

7. Specify a host IP address and network mask on the traffic interface for the current VPN Gateway.

```
Enter IP address for this machine (on traffic interface):<IP
address>

Enter network mask [255.255.255.0]:<press ENTER to accepts>
```

   In a two-armed configuration, the traffic interface host IP address will be assigned to Interface 2.

8. If a connected router or switch attaches VLAN tag IDs to incoming packets, specify the VLAN tag ID used.

```
Enter VLAN tag id (or zero for no VLAN) [0]:
```

9. Enter the Management IP address (MIP) of the existing cluster.

```
The system is initialized by connecting to the management server
on an existing iSD, which must be operational and initialized.
Enter the Management IP (MIP) address:<IP address>
```


Comments? infodev@avaya.com

Provide the Management IP address of the cluster to which you want to join the current VPN Gateway. To check the Management IP of an existing cluster, connect to the cluster and use the **/cfg/sys/cur** command.

10. Enter the default gateway on the traffic interface.

```
Enter default gateway IP address (on the traffic interface):<IP
addr>
```

The default gateway IP address should be within the same network address range as the host IP address on the traffic interface.

Complete the join setup by following the instructions in the next section, "Complete the Join Setup".

Complete the Join Setup

1. Provide the correct admin user password.

   Type the correct password for the admin user.

```
( join setup, continued)

Enter the existing admin user password:
```

2. Specify the VPN Gateway type.

   When adding up to three additional master AVGs to a cluster containing a single VPN Gateway, you may configure each additional AVG as either master or slave. For up to three additional AVGs, the default setting is master. When adding one or more VPN Gateways to a cluster that already contains four master AVGs, each additional AVG is automatically configured as slave.

   It is recommended that there are 2-4 master AVGs in each cluster, so in most cases there is no need to change the default setting. If needed, you can always reconfigure a VPN Gateway by changing the Type setting after the initial setup. For more information, see the **type** command in the "iSD Host Configuration" section under Configuration Menu>System Configuration in the *Avaya Command Reference*.

```
Enter the type of this iSD (master/slave) [master]:
......ok
```

3. Wait until the Setup utility has finished.

```
Setup successful.
login:
```

The setup is now finished. The VPN Gateway that has been joined to the cluster will automatically pick up all configuration data from one of the already installed AVG(s) in the cluster. After a short while you will get a login prompt.

If needed, you can now continue with the configuration of the AVG cluster using the Command Line Interface (CLI) or the Browser-Based Management Interface (BBI). Log in as the admin user.

For more information about the CLI, see The Command Line Interface on page 119.

For more information about the BBI, see the *Avaya SSL VPN BBI Quick Guide*.

Installing an ASA 310-FIPS

The ASA 310-FIPS model is an ASA 310 where the ordinary SSL accelerator card has been replaced by the HSM (Hardware Security Module) SSL accelerator card. For more information about the ASA 310-FIPS model, see Introducing the ASA 310-FIPS on page 25.

After having installed the first ASA 310-FIPS, additional ASA 310-FIPS units can be added to the same cluster by specifying the Management IP (MIP) address that identifies the cluster. For more information about adding an ASA 310-FIPS to an existing cluster, see Adding an ASA 310-FIPS to an Existing Cluster on page 55.

Before installing or adding an ASA 310-FIPS, make sure that you have fully understood the concept of iKeys. You might also want to decide the labeling scheme you want to use for identifying which iKey is used to initialize a certain HSM card, and also label two of the black cluster-specific iKeys "CODE-SO" and "CODE-USER" respectively in advance. For more information about the concept of iKeys and the ASA 310-FIPS ASA 310-FIPS model in general, see Introducing the ASA 310-FIPS on page 25. You should also decide a password scheme because you will define passwords not only for the **admin** user, but also for the HSM-SO iKeys, the HSM-USER iKeys, and possibly a secret passphrase (when selecting FIPS mode).

Installing an ASA 310-FIPS in a New Cluster

When you log in as the admin user after having started the ASA 310-FIPS the first time, the Setup menu is displayed.

1. Choose `new` from the Setup menu to install the ASA 310-FIPS as the first member in a new cluster.

Comments? infodev@avaya.com

```
[Setup Menu]
join          - Join an existing iSD cluster
new            - Initialize iSD as a new installation
boot           - Boot menu
info           - Information menu
exit           - Exit     [global command, always available]
>> Setup#new

Setup will guide you through the initial configuration of the
iSD.
```

2. Follow the instructions for installing a VPN Gateway in a new cluster.

   Read the sections starting with Installing an AVG in a New Cluster on page 36. When the basic setup is completed, new prompts for configuring an ASA 310-FIPS will automatically appear.

3. Choose the appropriate security mode for the ASA 310-FIPS cluster.

   Decide which security mode to use for the new ASA 310-FIPS cluster—FIPS mode or Extended Security mode. The default Extended Security mode should be used whenever your security policy does not explicitly require conforming to the FIPS 140-1, Level 3 standard.

   For more information about the FIPS mode and the Extended Security mode, see Introducing the ASA 310-FIPS on page 25.

```
( new setup, continued)

Use FIPS or Extended Security Mode? (fips/extended)
[extended]:<Press ENTER to accept the default extended mode, or
change the security mode to fips>
```

4. Initialize HSM card 0 by inserting the first pair of HSM-SO and HSM-USER iKeys, and by defining passwords.

   Step 4 on page 51 and step 5 on page 52 are related to initializing the HSM cards that your ASA 310-FIPS is equipped with. The Setup utility will identify the first HSM card as card 0, and the second HSM card as card 1. Each HSM card is initialized by inserting the proper iKeys and defining a password for each user role. To successfully initialize both HSM cards, you need to have the following iKeys:

   - One pair of iKeys to be used for initializing HSM card 0.
     - The purple HSM Security Officer iKey, embossed with "HSM-SO".
     - The blue HSM User iKey, embossed with "HSM-USER".

   Label these iKeys and HSM card 0 in a way so that the connection between them is obvious. After HSM card 0 has been initialized, this card will only accept the HSM-SO and HSM-USER iKeys that were used when initializing this particular HSM card. Even if you choose to use the same HSM-SO and HSM-USER passwords when you initialize card 1 as the passwords you defined

when initializing card 0, the HSM-SO and HSM-USER iKeys for card 1 are not interchangeable with the HSM-SO and HSM-USER iKeys for card 0.

- One pair of iKeys to be used for initializing HSM card 1.

  - The purple HSM Security Officer iKey, embossed with "HSM-SO".

  - The blue HSM User iKey, embossed with "HSM-USER".

  Label these iKeys and HSM card 1 in a way so that the connection between them is obvious. If you will use more than one ASA 310-FIPS device in the cluster, you must also take steps to identify which pair of iKeys is used on which HSM card on which device in the cluster.

You also need to make sure that you can easily access the USB ports on the HSM cards, located on the rear of the ASA 310-FIPS device. When an operation requires inserting an HSM iKey, a flashing LED will direct you to the USB port on the correct HSM card.

```
( new setup, continued)

Verify that HSM-SO iKey (purple) is inserted in card 0 (with
flashing LED).
Hit enter when done.
Enter a new HSM-SO password for card 0:<define an HSM-SO password>

Re-enter to confirm:
The HSM-SO iKey has been updated.
Verify that HSM-USER iKey (blue) is inserted in card 0 (with
flashing LED).
Hit enter when done.
Enter a new HSM-USER password for card 0:<define an HSM-USER
password>

Re-enter to confirm:
The HSM-USER iKey has been updated.
Card 0 successfully initialized.
```

Note:

For more information about iKeys, see The Concept of iKey Authentication on page 26.

5. Initialize HSM card 1 by inserting the second pair of HSM-SO and HSM-USER iKeys, and by defining passwords.

   Remember to take steps to label each pair of HSM-SO and HSM-USER iKeys and the HSM card to which each set of iKeys is associated during the initialization.

```
(newsetup, continued)

Verify that HSM-SO iKey (purple) is inserted in card 1 (with
flashing LED).
Hit enter when done.
Enter a new HSM-SO password for card 1:<define a new HSM-SO
password, or use the same HSM-SO password as for card 0>
```


Comments? infodev@avaya.com

```
Re-enter to confirm:
The HSM-SO iKey has been updated.
Verify that HSM-USER iKey (blue) is inserted in card 1 (with
flashing LED).
Hit enter when done.
Enter a new HSM-USER password for card 1:<define a new HSM-USER
password, or use the same HSM-USER password as for card 0>

Re-enter to confirm:
The HSM-USER iKey has been updated.
Card 1 successfully initialized.
```

6. Split the wrap key from HSM card 0 onto the CODE-SO and CODE-USER iKeys.

   This step is related to splitting the software wrap key used internally in the cluster, and then loading the split wrap key onto the two black CODE-SO and CODE-USER iKeys. These iKeys will then be used to transfer the cluster wrap key onto another HSM card either within the same ASA 310-FIPS device (as in step 7 on page 54), or to HSM cards in an ASA 310-FIPS device that is added to the current cluster.

   Each ASA 310-FIPS device is shipped with four black CODE iKeys. However, you will only need to use two of these in one given cluster. The extra two black iKeys can be used to create a pair of backup CODE iKeys. For more information about how to create a pair of backup CODE iKeys, see the **`splitkey`** command on the HSM menu (described under Maintenance Menu in the *Command Reference*).

   To successfully split and load the cluster wrap key onto the correct iKeys, you need the following:

   - Two black CODE iKeys, supposedly labeled "CODE-SO" and "CODE-USER" respectively.

   If the black iKeys are not already labeled CODE-SO and CODE-USER respectively, you are recommended to do so before inserting them. Whenever the cluster wrap key needs to be transferred onto an initialized HSM card, you will be prompted for the specific CODE iKey, in turns. Having each iKey properly labeled CODE-SO and CODE-USER respectively will make this procedure easier.

```
( newsetup, continued)

Should new or existing CODE iKeys be used? (new/existing)
[new]:<press ENTER to select new>

Verify that CODE-SO iKey (black) is inserted in card 0 (with
flashing LED).
Hit enter when done.
Verify that HSM-USER iKey (blue) is inserted in card 0 (with
flashing LED).
Hit enter when done.
Verify that CODE-USER iKey (black) is inserted in card 0 (with
flashing LED).
Hit enter when done.
Wrap key successfully split from card 0.
```

Note:

Unlike the HSM-SO and the HSM-USER iKeys, the CODE-SO and CODE-USER iKeys are not specific for each HSM card. Instead, the CODE-SO and CODE-USER iKeys are specific for each cluster of ASA 310-FIPS ASA 310-FIPS units. Therefore, if you have more than one cluster of ASA 310-FIPS units, you need to take steps so that you can identify to which cluster a pair of CODE-SO and CODE-USER iKeys is associated.

7. Transfer the cluster wrap key from the CODE-SO and CODE-USER iKeys onto HSM card 1.

```
(newsetup, continued)

Verify that CODE-SO iKey (black) is inserted in card 1 (with
flashing LED).
Hit enter when done.
Verify that HSM-USER iKey (blue) is inserted in card 1 (with
flashing LED).
Hit enter when done.
Verify that CODE-USER iKey (black) is inserted in card 1 (with
flashing LED).
Hit enter when done.
Wrap key successfully combined to card 1.
```

8. If you have selected FIPS mode as the security mode, define a passphrase.

   If you selected FIPS mode prior to initializing HSM card 0 (step 3 on page 51), you will also be asked to define a passphrase. Make sure you remember the passphrase as you will be prompted for the same passphrase when adding other ASA 310-FIPS ASA 310-FIPS units to the same cluster. When selecting Extended Security mode, this step will not appear.

```
(newsetup, continued)

Enter a secret passphrase (it will be used during addition of new
iSDs to the cluster):
Re-enter to confirm:
```

9. When the Setup utility has finished, log in to the ASA 310-FIPS again and continue with the configuration.

```
(newsetup, continued)

Initializing system......ok
Setup successful. Relogin to configure.

login:
```

   The setup is now finished, and after a short while you will get a login prompt. Log in as the admin user with the password you defined during the initial setup. The Main menu is then displayed. You can now continue with the configuration of the

Comments? infodev@avaya.com

ASA 310-FIPS ASA 310-FIPS using the command line interface (CLI). For more information about the CLI, see The Command Line Interface on page 119.

Note:

After successfully having initialized the HSM cards, you are automatically logged in to each HSM card as USER. You can verify the current HSM card login status by using the **`/info/hsm`** command. After a reboot has occurred (whether intentionally invoked, or due to a power failure), you must manually log in to the HSM cards for the ASA 310-FIPS device to resume normal operations. For more information about logging in to the HSM cards after a reboot, see An ASA 310-FIPS Stops Processing Traffic on page 133.

Adding an ASA 310-FIPS to an Existing Cluster

You add additional ASA 310-FIPS units to an existing cluster by selecting `join` from the Setup menu in the ASA 310-FIPS, after it has booted.

The following applies when joining a new ASA 310-FIPS to an existing cluster:

- If the ASA 310-FIPS you are about to join is installed on a different subnet than existing units, this new ASA must be configured as a slave. Master ASAs cannot exist on different subnets.
- If the Access list consists of entries (for example, IP addresses for control of Telnet and SSH access), also add the cluster's MIP, the existing ASA's host IP address on Interface 1, and the host IP address you have in mind for the new ASA to the Access list. This must be done before joining the new ASA, otherwise the ASAs will not be able to communicate. Use the **`/cfg/sys/accesslist`** command. If the Access list is empty, this step is not required.
- If the ASA you are about to join has a different software version than existing ASAs, install the preferred software version on the new ASA before joining it (see Reinstalling the Software on page 60) or upgrade the whole cluster to the same software version as the new ASA (see Performing Minor/Major Release Upgrades on page 63). Use the **`/boot/software/cur`** command to check the currently installed software version.

When you log in as the admin user after having started the ASA 310-FIPS the first time, the Setup menu is displayed.

1. Choose `join` from the Setup menu to add the ASA 310-FIPS to an existing cluster.

```
[Setup Menu]
join          - Join an existing iSD cluster
new            - Initialize iSD as a new installation
boot          - Boot menu
info          - Information menu
exit          - Exit     [global command, always available]
>> Setup#join
```

```
Setup will guide you through the initial configuration of the
iSD.
```

2. Follow the instructions for joining a VPN Gateway to an existing cluster.

   Read the sections starting with Joining a VPN Gateway to an Existing Cluster on page 45. When the basic setup is completed, new prompts for configuring the ASA 310-FIPS will automatically appear (see 3 on page 56).

3. Initialize HSM card 0 by inserting the first pair of HSM-SO and HSM-USER iKeys, and by defining passwords.

   Step 3 on page 57 and step 4 on page 57 are related to initializing the HSM cards that your ASA 310-FIPS is equipped with. The Setup utility will identify the first HSM card as card 0, and the second HSM card as card 1. Make sure you have the required iKeys before proceeding. To successfully initialize both HSM cards, you need to have the following iKeys:

   - One pair of iKeys to be used for initializing HSM card 0.
     - The purple HSM Security Officer iKey, embossed with "HSM-SO".
     - The blue HSM User iKey, embossed with "HSM-USER".

     Label these iKeys and HSM card 0 in a way so that the connection between them is obvious. After HSM card 0 has been initialized, this card will only accept the HSM-SO and HSM-USER iKeys used when initializing this particular HSM card. Even if you choose to use the same HSM-SO and HSM-USER passwords when you initialize card 1 as the passwords you defined when initializing card 0, the HSM-SO and HSM-USER iKeys for card 1 are not interchangeable with the HSM-SO and HSM-USER iKeys for card 0.
   - One pair of iKeys to be used for initializing HSM card 1.
     - The purple HSM Security Officer iKey, embossed with "HSM-SO".
     - The blue HSM User iKey, embossed with "HSM-USER".

     Label these iKeys and HSM card 1 in a way so that the connection between them is obvious. Because you will have more than one ASA 310-FIPS ASA 310-FIPS device in the cluster, you must also take steps to identify which pair of iKeys is used on which HSM card on which device in the cluster.

   You also need to make sure that you can easily access the USB ports on the HSM cards, located on the rear of the ASA 310-FIPS device. When an operation requires inserting an HSM iKey, a flashing LED will direct you to the USB port on the correct HSM card.

```
(joinsetup, continued)

Verify that HSM-SO iKey (purple) is inserted in card 0 (with
flashing LED).<insert the HSM-SO iKey specific for this HSM card>
```


Comments? infodev@avaya.com

```
Hit enter when done.
Enter a new HSM-SO password for card 0:<define an HSM-SO password>

Re-enter to confirm:
The HSM-SO iKey has been updated.
Verify that HSM-USER iKey (blue) is inserted in card 0 (with
flashing LED).<insert the HSM-USER iKey specific for this HSM
card>

Hit enter when done.
Enter a new HSM-USER password for card 0:<define an HSM-USER
password>

Re-enter to confirm:
The HSM-USER iKey has been updated.
Card 0 successfully initialized.
```

Note:

For more information about iKeys, see The Concept of iKey Authentication on page 26.

4. Initialize HSM card 1 by inserting the second pair of HSM-SO and HSM-USER iKeys, and by defining passwords.

   Remember to take steps to label each pair of HSM-SO and HSM-USER iKeys and the HSM card to which each set of iKeys is associated during the initialization. Because each ASA 310-FIPS ASA 310-FIPS device in the cluster will have two HSM cards, you must also take steps to identify to which ASA 310-FIPS device each pair of iKeys are associated. Your labeling must ensure that the connection is obvious between a pair of HSM-SO/HSM-USER iKeys, the HSM card that was initialized by using those iKeys, and the ASA 310-FIPS device holding that particular HSM card.

```
(joinsetup, continued)

Verify that HSM-SO iKey (purple) is inserted in card 1 (with
flashing LED).<insert the HSM-SO iKey specific for this HSM card>

Hit enter when done.
Enter a new HSM-SO password for card 1:<define a new HSM-SO
password, or use the same HSM-SO password as for card 0>

Re-enter to confirm:
The HSM-SO iKey has been updated.
Verify that HSM-USER iKey (blue) is inserted in card 1 (with
flashing LED).<insert the HSM-USER iKey specific for this HSM
card>

Hit enter when done.
Enter a new HSM-USER password for card 1:<define a new HSM-USER
password, or use the same HSM-USER password as for card 0>

Re-enter to confirm:
The HSM-USER iKey has been updated.
Card 1 successfully initialized.
```

5. Transfer the cluster wrap key from the CODE-SO and CODE-USER iKeys onto HSM card 0.

   Step 5 on page 58 and step 6 on page 58 are related to transferring the cluster wrap key onto the two HSM cards in the ASA 310-FIPS ASA 310-FIPS you are adding to the cluster. The wrap key is transferred onto each HSM card in two steps, where each half of the cluster wrap key stored on the two black CODE-SO and CODE-USER iKeys is loaded and combined on the HSM card in the new ASA 310-FIPS cluster member.

   To successfully load and combine the cluster wrap key onto the HSM cards, you need the following:

   - The two black HSM Code iKeys, labeled "CODE-SO" and "CODE-USER" respectively, that you used when installing the first ASA 310-FIPS in the cluster.

   If you have more than one cluster of ASA 310-FIPS units, make sure that you can identify to which cluster the pair of CODE iKeys are associated. The cluster wrap key that is split and stored on the two CODE iKeys is specific for each cluster of ASA 310-FIPS units.

```
(joinsetup, continued)

Verify that CODE-SO iKey (black) is inserted in card 0 (with
flashing LED).<insert the same CODE-SO iKey that you used when
installing the firstASA 310-FIPS  in the cluster>

Hit enter when done.
Verify that HSM-USER iKey (blue) is inserted in card 0 (with
flashing LED).
Hit enter when done.
Verify that CODE-USER iKey (black) is inserted in card 0 (with
flashing LED).<insert the same CODE-USER iKey that you used when
installing the very firstASA 310-FIPS in the cluster>

Hit enter when done.
Wrap key successfully combined to card 0.
```

6. Transfer the cluster wrap key from the CODE-SO and CODE-USER iKeys onto HSM card 1.

```
(joinsetup, continued)

Verify that CODE-SO iKey (black) is inserted in card 1 (with
flashing LED).<insert the same CODE-SO iKey that you used in Step
5 >

Hit enter when done.
Verify that HSM-USER iKey (blue) is inserted in card 1 (with
flashing LED).
Hit enter when done.
Verify that CODE-USER iKey (black) is inserted in card 1 (with
flashing LED).<insert the same CODE-USER iKey that you used in
Step 5 >
```


Comments? infodev@avaya.com

```
Hit enter when done.
Wrap key successfully combined to card 1.
```

7. If you selected FIPS mode when installing the first ASA 310-FIPS in the cluster, provide the correct passphrase.

   If you selected FIPS mode when installing the first ASA 310-FIPS ASA 310-FIPS in the cluster, you will also be asked to provide the passphrase you defined at that time. If you selected Extended Security mode, this step will not appear.

```
(joinsetup, continued)

Enter the secret passphrase (as given during initialization of
the first iSD in the cluster):
```

8. Wait until the Setup utility has finished.

```
(joinsetup, continued)

Setup successful.


login:
```

   The setup utility is now finished. The ASA 310-FIPS that has now been added to the cluster will automatically pick up all configuration data from one of the already installed ASA 310-FIPS units in the cluster. After a short while you will get a login prompt.

   Note:

   After successfully having initialized the HSM cards, you are automatically logged in to each HSM card as USER. You can verify the current HSM card login status by using the **`/info/hsm`** command. After a reboot has occurred (whether intentionally invoked, or due to a power failure), you must manually log in to the HSM cards for the ASA 310-FIPS device to resume normal operations. For more information about logging in to the HSM cards after a reboot, see An ASA 310-FIPS Stops Processing Traffic on page 133.

   If needed, you can now continue with the configuration of the ASA 310-FIPS ASA 310-FIPS units using the command line interface (CLI). Log in as the

```
admin
```

   user, and the Main menu is displayed. For more information about the CLI, see The Command Line Interface on page 119.

Reinstalling the Software

When adding a new VPN Gateway to an existing cluster, and the software version on the new VPN Gateway is different from the AVGs in the cluster, you will need to reinstall the software on the new VPN Gateway. Otherwise, reinstalling the software is seldom required except in case of serious malfunction.

When you log in as the boot user and perform a reinstallation of the software, the VPN Gateway is reset to its factory default configuration. All configuration data and current software is wiped out, including old software image versions or upgrade packages that may be stored in the flash memory card or on the hard disk. Also note that a reinstall must be performed on each VPN Gateway through a console connection.

Note:

A reinstall wipes out all configuration data (including network settings). Therefore you should first save all configuration data to a file on a TFTP/FTP/SCP/SFTP server. Using the **ptcfg** command, installed keys and certificates are included in the configuration data, and can later be restored by using the **gtcfg** command. For more information about these commands, see the "Configuration Menu " chapter in the *Command Reference*. If you prefer to make backup copies of your keys and certificates separately, you can use the **`display`** or **`export`** command. For more information about these commands, see the "Certificate Management Configuration " section under Configuration Menu>SSL Configuration Menu in the *Avaya Command Reference*.

To reinstall a VPN Gateway you will need the following:

- Access to the VPN Gateway through a console connection.
- An install image, loaded on a FTP/SCP/SFTP server on your network.
- The IP address of the FTP/SCP/SFTP server.
- The name of the install image.
- Log in as `user: boot`, `password: ForgetMe`

When performing a reinstallation of the AVG software, access to the VPN Gateways must be accomplished through the console port.

1. Log in as the boot user and provide the correct password.

```
login:boot

Password:ForgetMe

               *** Reinstall Upgrade Procedure ***
If you proceed beyond this point, the active network
configuration will be reset, requiring a reboot to restore any
current settings. However, no permanent changes will be done
```


Comments? infodev@avaya.com

```
until the boot image has been downloaded.
Continue (y/n)? [y]:<Press ENTER to continue>
```

2. Confirm the network port setting, and the IP network settings.

```
(reinstall procedure, continued)

Select a network port (1-4, or i for info) [1]:<Press ENTER if
correct, or change to the port you are using for network
connectivity>

Enter VLAN tag id (or zero for no VLAN tag) [0]:<VLAN tag id or
ENTER>

Enter IP address for this iSD [192.168.128.185]: <Press ENTER if
the IP address displayed within square brackets is correct.>

Enter network mask [255.255.255.0]:<Press ENTER if correct.>

Enter gateway IP address [192.168.128.1]:<Press ENTER if
correct.>
```

Note:

If the VPN Gateway has not been configured for network access previously, or if you have deleted the VPN Gateway from the cluster by using the **/boot/delete** command, you must provide information about network settings such as interface port, IP address, network mask, and gateway IP address. No suggested values related to a previous configuration will be presented within square brackets.

3. Select a download method, specify the server IP address, and the boot image file name.

```
(reinstall procedure, continued)

Select protocol (ftp/scp/sftp) [ftp]:ftp

Enter FTP server address:10.0.0.1

Enter file name of boot image:SSL-7.0.x-boot.img

Enter FTP Username [anonymous]:john

Password:password

Downloading boot image...
Installing new boot image...
Done
```

If the FTP server does not support anonymous login, enter the required FTP user name and password. Anonymous login is the default option.

4. Log in to the VPN Gateway as the admin user, after the device has rebooted on the newly installed boot image.

(reinstall procedure, continued)

```
Restarting...
Restarting system.
Alteon WebSystems,I   nc.               0004004C
Booting...


Login:
```

After the new boot image has been installed, the VPN Gateway will reboot and you can log in again when the login prompt appears. This time, log in as the admin user to enter the Setup menu. For more information about the Setup menu.

Chapter 6: Upgrading the AVG Software

The Avaya VPN Gateway (AVG) software image is the executable code running on the VPN Gateway. A version of the image ships with the VPN Gateway, and comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your VPN Gateway. Before upgrading, check the accompanying release notes for any specific actions to take for the particular software upgrade package or install image.

There are the following types of upgrades:

- **Minor release upgrade:** This is typically a bug fix release. Usually this kind of upgrade can be done without the VPN Gateway rebooting. Thus, the normal operation and traffic flow is maintained. All configuration data is retained. When performing a minor upgrade, you should connect to the Management IP address of the cluster you want to upgrade.
- **Major release upgrade:** This kind of release may contain both bug fixes as well as feature enhancements. The VPN Gateway may automatically reboot after a major upgrade, because the operating system may have been enhanced with new features. All configuration data is retained. When performing a major upgrade, you should connect to the Management IP address of the cluster you want to upgrade.
- **Upgrading from software version 2.0 to software version 3.0.7:** This upgrade needs to be performed intwo steps, due to the new database format and software management introduced in version 3.0.7. For more information on procedures, see"UpgradingiSD-SSL Software from Version 2.0.x to Version 3.x"

Upgrading the software on your VPN Gateway requires the following:

- Loading the new software upgrade package or install image onto a FTP/SCP/SFTP server on your network.
- Downloading the new software from the FTP/SCP/SFTP server to your VPN Gateway.

Performing Minor/Major Release Upgrades

The following description applies to a minor or a major release upgrade.

To upgrade the VPN Gateway you will need the following:

- Access to one of your VPN Gateways through a remote connection (Telnet or SSH), or a console connection.
- The software upgrade package, loaded on a FTP/SCP/SFTP server on your network.
- The host name or IP address of the FTP/SCP/SFTP server. If you choose to specify the host name, note that the DNS parameters must have been configured. For more

information, see the "DNS Servers Configuration " section under Configuration Menu>System Configuration in the *Avaya Command Reference*.

- The name of the software upgrade package (upgrade packages are identified by the .pkg file name extension).

It is important to realize that the set of installed VPN Gateways you are running in a cluster are cooperating to give you a single system view. Thus, when performing a minor or a major release upgrade, you only need to be connected to the Management IP address of the cluster. The upgrade will automatically be executed on all the VPN Gateways in operation at the time of the upgrade. All configuration data is retained. For a minor upgrade, normal operations are usually unaffected, whereas a major upgrade may cause the VPN Gateway to reboot.

You need to perform a disk repartitioning on AVG 3050 and 3070 before upgrading from Release 7.x to 8.0.0.0. You can use the following commands to repartition the hard disk:

- **`/boot/repartition`** to initiate repartitioning for the local host.
- **`/cfg/sys/host<id>/repartition /cfg/sys/cluster/host <id>/repartition`** to initiate repartitioning for the given running host.

These commands are hidden and are not shown in the menu or considered for auto-completion through <TAB>; they cannot be used in normal operation. Disk repartition takes approximately 5 to 7 minutes to complete the operation; it includes two automatic reboots, and makes the host effectively out of service.

Access to the Management IP address can be accomplished through a Telnet connection or SSH (Secure Shell) connection. Note however that Telnet and SSH connections to the VPN Gateway are disabled by default, after the initial setup has been performed. For more information about enabling Telnet and SSH connections, see Connecting to the VPN Gateway on page 119. When you have gained access to the VPN Gateway, use the following procedure.

1. To download the software upgrade package, enter the following command at the Main menu prompt. Then select whether to download the software upgrade package from a FTP/SCP/SFTP server.

   ```
   >> Main#boot/software/download

   Select protocol (ftp/scp/sftp) [ftp]:ftp
   ```

2. Enter the host name or IP address of the server.

   ```
   Enter hostname or IP address of server:<server host name or IP>
   ```

3. Enter the file name of the software upgrade package to download.

   If needed, the file name can be prefixed with a search path to the directory on the FTP/SCP/SFTP server.

   If you are using anonymous mode when downloading the software package from an FTP server, the following string is used as the password (for logging purposes): `admin@hostname/IP.isd`.

Comments? infodev@avaya.com

```
Enter filename on server:<filename.pkg>

FTP User (anonymous):<username or press ENTER for anonymous mode>

Password:<password or press ENTER for default password in
anonymous mode>

Received 28200364 bytes in 4.0 seconds

Unpacking...
ok

>> Software Management#
```

Activating the Software Upgrade Package

The VPN Gateway can hold up to two software versions simultaneously. To view the current software status, use the **/boot/software/cur** command. When a new version of the software is downloaded to the VPN Gateway, the software package is decompressed automatically and marked as unpacked. After you activate the unpacked software version (which may cause the VPN Gateway to reboot), the software version is marked as permanent. The software version previously marked as permanent will then be marked as old.

For minor and major releases, the software upgrade will take part synchronously among the set of VPN Gateways in a cluster. If one or more VPN Gateways are not operational when the software is upgraded, they will automatically pick up the new version when they are started.

Note:

If more than one software upgrade has been performed to a cluster while a VPN Gateway has been out of operation, the VPN Gateway must be reinstalled with the software version currently in use in that cluster. For more information about how to perform a reinstall, see Reinstalling the Software on page 60.

When you have downloaded the software upgrade package, you can inspect its status with the **/boot/software/cur** command.

1. At the `Software Management#` prompt, enter the following command:

```
>> Software Management# cur

Version             Name            Status
-------             ----            ------
8.0.0                 SSL           unpacked
5.1.5                 SSL           permanent
```

The downloaded software upgrade package is indicated with the status unpacked. The software versions can be marked with one out of four possible status values. The meaning of these status values are:

- unpacked means that the software upgrade package has been downloaded and automatically decompressed.
- permanent means that the software is operational and will survive a reboot of the system.
- old means the software version has been permanent but is not currently operational. If a software version marked old is available, it is possible to switch back to this version by activating it again.
- current means that a software version marked as old or unpacked has been activated. As soon as the system has performed the necessary health checks, the current status changes to permanent.

To activate the unpacked software upgrade package, use the **`activate`** command.

2. At the `Software Management#` prompt, enter:

```
>> Software Management#activate 8.0.0

Confirm action 'activate'? [y/n]:y

Activate ok, relogin<you are logged out here>



Restarting system.

login:
```

Note:

Activating the unpacked software upgrade package may cause the command line interface (CLI) software to be upgraded as well. Therefore, you will be logged out of the system, and will have to log in again. Wait until the login prompt appears. This may take up to 2 minutes, depending on your type of hardware platform and whether the system reboots.

3. After having logged in again, verify the new software version:

```
>> Main#boot/software/cur

Version                          Name                       Status
-------                          ----                       ------
8.0.0                                  SSL
 permanent
5.1.5                                SSL                      old
```


Comments? infodev@avaya.com

In this example, version 8.0.0 is now operational and will survive a reboot of the system, while the software version previously indicated as permanent is marked as old.

Note:

If you encounter serious problems while running the new software version, you can revert to the previous software version (now indicated as old). To do this, activate the software version indicated as old. When you log in again after having activated the old software version, its status is indicated as current for a short while. After about one minute, when the system has performed the necessary health checks, the current status is changed to permanent.

Comments? infodev@avaya.com

Chapter 7: Managing Users and Groups

This chapter describes the rules that govern administrator/operator user rights, how to add or delete users from the system, how to set or change group assignments, and how to change login passwords.

User Rights and Group Membership

Group membership dictates user rights, according to User Rights and Group Membership. When a user is a member of more than one group, user rights accumulate. The admin user, who by default is a member of all four groups, therefore has the same user rights as granted to members in the certadmin and oper group, in addition to the specific user rights granted by the admin group membership. The most permissive user rights become the effective user rights when a user is a member of more than one group. For more information about default user groups and related access levels, see also Accessing the AVG Cluster on page 122.

Group Account	User Account	Add User to System	Delete User from System	Add User to Group	Remove User from Group	Change own Password	Change other User's Password	Manage Tunnel Guard (via BBI)
admin	admin	Yes	Yes	Yes, to own group	Yes	Yes	Yes, if admin is a member of the other user's first group	Yes
certadmin	admin	No	No	Yes, to own group	No	Yes	No	No
oper	oper admin	No	No	Yes, to own group	No	Yes	No	No
tunnelguard	admin	No	No	Yes, to own group	No	Yes	No	Yes

Adding a New User

To add a new user to the system, you must be a member of the admin group. By default, only the admin user is a member of the admin group.

In this configuration example, a Certificate Administrator user is added to the system, and then assigned to the certadmin group. The Certificate Administrator is supposed to specialize in managing certificates and private keys, without the possibility to change system parameters

or configure virtual SSL servers. A user who is a member of the certadmin group can therefore access the Certificate menu (**/cfg/cert**), but not the SSL Server menu (**/cfg/ssl/server**). Access to the System menu (**/cfg/sys**) is limited, and entails access only to the User Access Control submenu (**/cfg/sys/user**).

1. Log in to the AVG cluster as the admin user.

```
login:admin

Password:(admin user password)
```

2. Access the User Menu.

```
>> Main#                          /cfg/sys/user

-------------------------------------------------------
-------

[User Menu]

passwd                          - Change own password

expire                          - Set password expire time
                                interval

list                            - List all users

del                             - Delete a user

add                             - Add a new user

edit                            - Edit a user

caphrase                        - Certadmin export
                                passphrase
```

3. Add the new user and designate a user name.

   The maximum length for a user name is 255 characters. No spaces are allowed. Each time the new user logs in to the AVG cluster, the user must enter the name you designate as the user name in this step.

```
>> User#add

Name of user to add:cert_admin

(maximum 255 characters, no spaces)
```

4. Assign the new user to a user group.

   You can only assign a user to a group in which you yourself are a member. When this criteria is met, users can be assigned to one or more of the following groups:

   - oper

Comments? infodev@avaya.com

- admin
- certadmin
- tunnelguard

By default, the admin user is a member of all preceding groups, and can therefore assign a new or existing user to any of these groups. The group assignment of a user dictates the user rights and access levels to the system.

```
>> User#edit cert_admin

>> User cert_admin#groups/add

Enter group name:certadmin
```

5. Verify and apply the group assignment.

   When typing the **list** command, the current and pending group assignment of the user being edited is listed by index number and group name. Because the cert_admin user is a new user, the current group assignment listed by Old: is empty.

```
>> Groups#list

Old:
Pending:
1: certadmin
>> Groups#apply

Changes applied successfully.
```

6. Define a login password for the user.

   When the user logs in to the AVG cluster the first time, the user will be prompted for the password you define in this step. When successfully logged in, the user can change his or her own password. The login password is case sensitive and can contain spaces.

```
>> Groups#/cfg/sys/user

>> User#edit cert_admin

>> User cert_admin#password

Enter admin's current password:(admin user password)

Enter new password for cert_admin:(cert_admin user password)

Re-enter to confirm:(reconfirm cert_admin user password)
```

7. Apply the changes.

```
>> User cert_admin#apply

Changes applied successfully.
```

8. Let the Certificate Administrator user define an export passphrase.

   This step is only necessary if you want to fully separate the Certificate Administrator user role from the Administrator user role. If the admin user is removed from the certadmin group, a Certificate Administrator export passphrase (caphrase) must be defined.

   As long as the admin user is a member of the certadmin group (the default configuration), the admin user is prompted for an export passphrase each time a configuration backup that contains private keys is sent to a TFTP/FTP/SCP/SFTP server (command: **/cfg/ptcfg**). When the admin user is not a member of the certadmin group, the export passphrase defined by the Certificate Administrator is used instead to encrypt private keys in the configuration backup. The encryption of private keys using the export passphrase defined by the Certificate Administrator is performed transparently to the user, without prompting. When the configuration backup is restored, the Certificate Administrator must enter the correct export passphrase.

   Note:

   If the export passphrase defined by the Certificate Administrator is lost, configuration backups made by the admin user while he or she was not a member of the certadmin group cannot be restored.

   Note:

   When using the **/cfg/ptcfg** command on an ASA 310-FIPS, private keys are always encrypted using the wrap key that was generated when the first HSM card in the cluster was initialized.

   The export passphrase defined by the Certificate Administrator remains the same until changed by using the **/cfg/sys/user/caphrase** command. For users who are not members of the certadmin group, the **caphrase** command in the User menu is hidden. Only users who are members of the certadmin group should know the export passphrase. The export passphrase can contain spaces and is case sensitive.

```
>> User cert_admin#../caphrase

Enter new passphrase:
Re-enter to confirm:
Passphrase changed.
```

9. Remove the admin user from the certadmin group.

   Again, this step is only necessary if you want to fully separate the Certificate Administrator user role from the Administrator user role. Note however, once the admin user is removed from the certadmin group, only a user who is already a

Comments? infodev@avaya.com

member of the certadmin group can grant the admin user certadmin group membership.

When the admin user is removed from the certadmin group, only the Certificate Administrator user can access the Certificate menu (**/cfg/cert**).

```
>> User#edit admin

>> User admin#groups/list

   1: tunnelguard
2: admin
3: oper
4: certadmin
>> Groups#del 4
```

Note:

It is critical that a Certificate Administrator user is created and assigned certadmin group membership before the admin user is removed from the certadmin group. Otherwise there is no way to assign certadmin group membership to a new user, or to restore certadmin group membership to the admin user, should it become necessary.

10. Verify and apply the changes.

```
>> Groups#list

Old:
1: tunnelguard
2: admin
3: oper
4: certadmin
Pending:
1: tunnelguard
2: admin
3: oper
>> Groups#apply
```

Adding Users through RADIUS

The RADIUS system administrator can add VPN Gateway administrator users to the RADIUS configuration without being an administrator of the AVG, because the users do not need to be configured locally on the AVG. By assigning suitable administrator groups to these users in RADIUS, the users can be given the desired access rights to the CLI/BBI.

When the user logs in to the CLI/BBI and is successfully authenticated, the RADIUS server returns the groups to which the user belongs. The groups are compared to the fixed administrator groups on the VPN Gateway, that is, tunnelguard, admin, oper and certadmin. If a match is found, the logged on user is given the administration rights pertaining to matching group(s). Otherwise, the user is denied access.

See the **/cfg/sys/adm/auth/group** command in the *Avaya User's Guide*.

Changing a Users Group Assignment

Only users who are members of the admin group can remove other users from a group. All users can add an existing user to a group, but only to a group in which the "granting" user is already a member. The admin user, who by default is a member of all four groups (admin, oper, tunnelguard and certadmin) can therefore add users to any of these groups.

1. Log in to the AVG cluster.

   In this example the cert_admin user, who is a member of the certadmin group, will add the admin user to the certadmin group. The example assumes that the admin user previously removed himself or herself from the certadmin group, to fully separate the Administrator user role from the Certificate Administrator user role.

```
login:cert_admin

Password:( cert_admin user password)
```

2. Access the User Menu.

```
>> Main#                        /cfg/sys/user

[User Menu]

-------------------------------------------------------
-------

passwd                         - Change own password

expire                         - Set password expire time
                                 interval

list                           - List all users

del                            - Delete a user

add                            - Add a new user

edit                           - Edit a user

caphrase                       - Certadmin export
                                 passphrase
```

3. Assign the admin user certadmin user rights by adding the admin user to the certadmin group.

```
>> User#edit admin
```


Comments? infodev@avaya.com

```
>> User admin#groups/add

Enter group name:certadmin
```

Note:

A user must be assigned to at least one group at any given time. If you want to replace a user's single group assignment, you must therefore always first add the user to the desired new group, then remove the user from the old group.

4. Verify and apply the changes.

```
>> Groups#list

Old:
1: tunnelguard
2: admin
3: oper
Pending:
1: tunnelguard
2: admin
3: oper
4: certadmin
>> Groups#apply
```

Changing a Users Password

Changing Your Own Password

All users can change their own password. Login passwords are case sensitive and can contain spaces.

1. Log in to the AVG cluster by entering your user name and current password.

```
login:cert_admin

Password:( cert_admin  user password)
```

2. Access the User Menu.

```
>> Main#                        /cfg/sys/user

[User Menu]
```

```
-------------------------------------------------------
-------

passwd                          - Change own password

expire                          - Set password expire time
                                interval

list                            - List all users

del                             - Delete a user

add                             - Add a new user

edit                            - Edit a user

caphrase                        - Certadmin export
                                passphrase
```

3. Type the **passwd** command to change your current password.

   When your own password is changed, the change takes effect immediately without having to use the **apply** command.

```
>> User#passwd

Enter cert_admin's current password:(current cert_admin  user
password)

Enter new password:(new cert_admin  user password)

Re-enter to confirm:(reconfirm new cert_admin  user password)

Password changed.
```

Changing Another Users Password

Only the admin user can change another user's password, and also only if the admin user is a member of the other user's first group, the group that is listed first for the user with the **/cfg/sys/user/edit <username>/groups/list** command. Login passwords are case sensitive and can contain spaces.

1. Log in to the AVG cluster as the admin user.

```
login:admin

Password:( admin  user password)
```

2. Access the User Menu.

Comments? infodev@avaya.com

```
>> Main#                        /cfg/sys/user

-------------------------------------------------------
-------

[User Menu]

passwd                         - Change own password

expire                         - Set password expire time
                               interval

list                           - List all users

del                            - Delete a user

add                            - Add a new user

edit                           - Edit a user

caphrase                       - Certadmin export
                               passphrase
```

3. Specify the user name of the user whose password you want to change.

```
>> User#edit

Name of user to edit:cert_admin
```

4. Type the `password` command to initialize the password change.

```
>> User cert_admin#password

Enter admin's current password:( admin  user password)

Enter new password for cert_admin:(new password for user being
edited) Re-enter to confirm: (confirm new password for user being
edited)
```

5. Apply the changes.

```
>> User cert_admin#apply

Changes applied successfully.
```

Deleting a User

To delete a user from the system, you must be a member of the admin group. By default, only the admin user is a member of the admin group.

Note:

Remember that when a user is deleted, that user's group assignment is also deleted. If you are deleting a user who is the sole member of a group, none of the remaining users on the system can then be added to that group. Existing users can only be added to a group by a user who is already a member of that group. Before deleting a user, you may therefore want to verify that the user is not the sole member of a group.

1. Log in to the AVG cluster as the admin user.

```
login:admin
Password:( admin  user password)
```

2. Access the User Menu.

```
>> Main#                    /cfg/sys/user
-------------------------
-------------------------
----------
[User Menu]
passwd                      - Change own password
expire                      - Set password expire time
                            interval
list                        - List all users
del                         - Delete a user
add                         - Add a new user
edit                        - Edit a user menu
caphrase                    - Certadmin export
                            passphrase
```

3. Specify the user name of the user you want to remove from the system configuration.

   In this example, the cert_admin user is removed from the system. To list all users that are currently added to the system configuration, use the `list` command.

```
>> User#del cert_admin
```

4. Verify and apply the changes.

   The imminent removal of the cert_admin user is indicated as a pending configuration change by the minus sign (-). To cancel a configuration change that has not yet been applied, use the **`revert`** command.

Comments? infodev@avaya.com

```
>> User#list

   oper
root
admin
-cert_admin
>> User#apply
```

Comments? infodev@avaya.com

Chapter 8: Certificates and Client Authentication

This chapter describes common tasks involving certificates and client authentication. The chapter also provides detailed step-by-step instructions for generating certificate signing requests, adding certificates to the Avaya VPN Gateway (AVG), generating and revoking client certificates, as well as configuring the VPN Gateway to require client certificates.

The VPN Gateway supports importing certificates in the PEM, NET, DER, PKSCS7, and PKCS12 formats. The certificates must conform to the X.509 standard. You can create a new certificate, or use an existing certificate. The VPN Gateway supports using up to 1500 certificates. The basic steps to create a new certificate using the command line interface of the VPN Gateway are:

- Generate a Certificate Signing Request (CSR) and send it to a Certificate Authority (CA, such as Entrust or VeriSign) for certification.
- Add the signed certificate to the VPN Gateway.

Note:

Even though the VPN Gateway supports keys and certificates created by using Apache-SSL, OpenSSL, or Stronghold SSL, the preferred method from a security point of view is to create keys and generate certificate signing requests from within the VPN Gateway by using the command line interface. This way, the encrypted private key never leaves the VPN Gateway, and is invisible to the user.

Generating and Submitting a CSR Using the CLI

1. Initiate requesting a certificate signing request (CSR), and provide the necessary information.

```
>> Main# cfg/cert
Enter certificate number (1-): <certificate number>
Creating Certificate 1
>> Certificate 1# request
The combined length of the following parameters may not exceed 225
bytes.
Country Name (2 letter code):
State or Province Name (full name):
Locality Name (e.g., city):
Organization Name (e.g., company):
Organizational Unit Name (e.g., section):
Common Name (e.g., your name or your server's hostname):
E-mail Address:
Subject alternative name (blank or comma separated list of
URI:<uri>, DNS:<fqdn>, IP:<ip-address>, email:<email-address>):
Generate new key pair (y/n) [y]:
Key size [1024]:
Request a CA certificate (y/n) [n]:
Specify challenge password (y/n) [n]:
```

Note:

When specifying a certificate number, make sure not to use a number currently used by an existing certificate. To view basic information about all configured certificates, use the **/info/certs** command. The information displayed lists all configured certificates by their main attributes, including the certificate number (in the Certificate Menu line, such as "Certificate Menu 1:").

Explanations for the requested units of information: Note that you do not have to complete all fields. Only one of Common Name and E-mail Address is strictly required.

- Country Name: The two-letter ISO code for the country where the Web server is located. For current information about ISO country codes, visit for example http://www.iana.org/.
- State or Province Name: This is the name of the state or province where the head office of the organization is located. Enter the full name of the state or province.
- Locality Name: The name of the city where the head office of the organization is located.
- Organization Name: The registered name of the organization. This organization must own the domain name that appears in the common name of the Web server.

  Do not abbreviate the organization name and do not use any of the following characters:

  < > ~ ! @ # $ % ^ * / \ ( ) ?
- Organizational Unit Name: The name of the department or group that uses the secure Web server.

Comments? infodev@avaya.com

- Common Name: The name of the Web server as it appears in the URL. This name must be the same as the domain name of the Web server that is requesting a certificate. If the Web server name does not match the common name in the certificate, some browsers will refuse a secure connection with your site. Do not enter the protocol specifier (http://) or any port numbers or path names in the common name. Wildcards (such as * or ?) and IP address are not allowed.
- E-mail Address: Enter the user's e-mail address.
- Subject Alternative Name: Comma-separated list of URI:<uri>, DNS:<fqdn>, IP:<IP address>, email:<e-mail address>.

  Example:

  ```
  URI:http://www.example.com,email:john@example.com,IP:10.1.2.3
  ```

- Generate new key pair [y]: In most cases you will want to generate a new key pair for a CSR. However, if a configured certificate is approaching its expiration date and you want to renew it without replacing the existing key, answering no (n) is appropriate. The CSR will then be based on the existing key (for the specified certificate number) instead.
- Key size [1024]: Specify the key length of the generated key. The default value is 1024.
- Request a CA certificate (y/n) [n]: Lets you specify whether to request a CA certificate to use for client authentication. Requesting a CA certificate is appropriate if you plan to issue your own server certificates or client certificates, generating them from the requested CA certificate. The default value is to not request a CA certificate.
- Specify challenge password (y/n) [n]:

2. Generate the CSR.

   Press ENTER after you have provided the requested information. The CSR is generated and displayed on screen:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB+jCCAWMCAQAwgZQxCzAJBgNVBAYTAlNFMRIwEAYDVQQIEwlTdG9ja2hvbG0x
DjAMBgNVBAcTBUtpc3RhMREwDwYDVQQKEwhCbHVldGFpbDENMAsGA1UECxMERG9j
dTEZMBcGA1UEAxMQd3d3LmJsdWV0YWlsLmNvbTEkMCIGCSqGSIb3DQEJARYVdG9y
Ympvcm5AYmx1ZXRhaWwuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCX
2rSY81cgKJODuUreGF3ZnK7RvlRqSV/TIMS4UerqXPKpTjfMAWDjBG77hjIAOOZO
FQKFB5x/Zs9kNMBUmPBokA1/GXghomOvBhMIJBZBiUVtJNGmv2sjeqNXxsUg5XfJ
iwV2LjUvw65EzCLpq5dhq6ZPEx7tAgqB2Wgu8MolwQIDAQABoCUwIwYJKoZIhvcN
AQkHMRYTFEEgY2hhbGxlbmdlIHBhc3N3b3JkMA0GCSqGSIb3DQEBBAUAA4GBACem
SJr8Xuk9PQZPuIPV7iCDG+eWneU3HH3F3DigW3MILCLNqweljKw5pZdAr9HbDwU+
2iQGbTSH0nVeoqn4TJujq96XpIrbiAFdE1tR7Lmf6oGdrwG8ypfRpp3PmfId6lp+
HJ2fUGliPYyNtd/94AL6wW8un208+icCHq/S0yjz
-----END CERTIFICATE REQUEST-----

Use 'apply' to store the private key in the iSD until
the signed certificate is entered.
The private key will be lost unless you 'apply' or
save it elsewhere using 'export'.
```

3. Apply your changes.

```
>> Certificate 1#apply

Changes applied successfully.
```

4. Save the CSR to a file.

   Copy the entire CSR, including the

   ```
   "-----BEGIN CERTIFICATE REQUEST----- " and "-----END CERTIFICATE
   REQUEST----- "
   ```

   lines, and paste it into a text editor. Save the file with a .csr extension. The name you define can indicate the server on which the certificate is to be used.

5. Save the private key to a file.

   Note:

   Provided you intend to use the same certificate number when adding the certificate returned to you (after the CSR has been processed by a certificate authority), this step is only necessary if you want to create a backup copy of the private key. When generating a CSR, the private key is created and stored (encrypted) on the VPN Gateway using the specified certificate number. When you receive the certificate (containing the corresponding public key) and add it to the VPN Gateway, make sure you specify the same certificate number that is used for storing the private key. Otherwise, the private key and the public key in the certificate will not match.

   Type the `display` command and press `ENTER`. Choose to encrypt the private key, and specify a password phrase. Make sure to remember the password phrase.

Comments? infodev@avaya.com

```
>> Certificate 1# display
Encrypt private key (yes/no) [yes]: <Press ENTER>
Enter export pass phrase:
Reconfirm export pass phrase:
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,27C89CBC65615F06

5cZBjjKAVoYRdtLYFa0zBpKQhK3yAJ+qSXxkrNCaRlSzuX2iClaAHtsSueGvJg7o
HNHcZVZCCxZtSLIsBTvDK0xY5ZomlqAU+JdWn0zc4hilf9KjLRBzk2p7azQUCMqW
jVJ5x9oFeuurfm3e6kqdCvnPweYJmZGp5A33Y7EV7TY5v30lZWnZrmD0tTfvljq7
rAfavlfWFgeBRG5kcdOgeb1hIHF2X16YMcp7YQUWGBccA1R7FvsVuvFuva9icCN1
++bF1GjfIMcSdpFt6Rkyq/CXBy3LVCAX0rfdPjaniO8G6sARa+qbkpnOvsA2eMc4
MXDHxc7+EavNBOIxAPL8PXunns53MYiWx5INWiQPh38gkjhi+n+75PJQi/J1Ab5p
iOpqHDUfcUBwdrkp/+3SKMAbc4VIaBnbGpfv2hNrr0Q/LyJilhjEPX+LIizkhWKo
QcdeqY3KyJGDugnqJBfybkNysKpPMDtd5Q7Yki5HdRe1RXenowDpiQlxToLlz9Bl
XDwFj2Ag7IfUk3Kwin2dn5KKSM35+a6Ateb4WjctIZGRlsi9JqQN8GOZf4uwj/Wg
nkzQeQ1rExpLbGTfiuRfVAstvo8bUIjm5xDY5HSmKx1FA2O2W2E/mB02Q9ZckG7I
hjB3ku2Wnvzv91qiCq6ljPN+hl4/zVmo6c/v2+pzubAxbOF5/NfQWwyogx0quCgN
4LaxsUXb0kpak4OLXNoqPVEDysYKD1zGCnrb3rgQ8hyhgoVHcRt6Rtsi4/6UzCkT
wtRtiyR96OEmVVA+x/8jsrU3LLCPYsswP0zje87mphh1PwiSRIMB6Q==
-----END RSA PRIVATE KEY-----
```

Copy the private key, including the

"-----BEGIN RSA PRIVATE KEY----- " and "-----END RSA PRIVATE KEY----- "

lines, and paste it into a text editor. Save the file with a .key extension. Preferably, use the same file name that you defined for the .csr file, so the connection between the two files becomes obvious. The name you define can indicate the server on which the certificate and the corresponding private key is to be used.

Note:

When using an ASA 310-FIPS, the private key is protected by the HSM card and cannot be exported.

After you have received the processed CSR from a CA, make sure to create a backup copy of the certificate as well.

6. Open and copy the CSR.

   In a text editor, open the .csr file you created in step 4 on page 84. It should appear similar to the following:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB+jCCAWMCAQAwgZQxCzAJBgNVBAYTAlNFMRIwEAYDVQQIEwlTdG9ja2hvbG0x
DjAMBgNVBAcTBUtpc3RhMREwDwYDVQQKEwhCbHVldGFpbDENMAsGA1UECxMERG9j
dTEZMBcGA1UEAxMQd3d3LmJsdWV0YWlsLmNvbTEkMCIGCSqGSIb3DQEJARYVdG9y
Ympvcm5AYmx1ZXRhaWwuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCX
2rSY81cgKJODuUreGF3ZnK7RvlRqSV/TIMS4UerqXPKpTjfMAWDjBG77hjIAOOZO
FQKFB5x/Zs9kNMBUmPBokA1/GXghomOvBhMIJBZBiUVtJNGmv2sjeqNXxsUg5XfJ
iwV2LjUvw65EzCLpq5dhq6ZPEx7tAgqB2Wgu8MolwQIDAQABoCUwIwYJKoZIhvcN
AQkHMRYTFEEgY2hhbGxlbmdlIHBhc3N3b3JkMA0GCSqGSIb3DQEBBAUAA4GBACem
SJr8Xuk9PQZPuIPV7iCDG+eWneU3HH3F3DigW3MILCLNqweljKw5pZdAr9HbDwU+
2iQGbTSH0nVeoqn4TJujq96XpIrbiAFdE1tR7Lmf6oGdrwG8ypfRpp3PmfId6lp+
HJ2fUGliPYyNtd/94AL6wW8un208+icCHq/S0yjz
-----END CERTIFICATE REQUEST-----
```

Copy the entire CSR, including the

```
"-----BEGIN CERTIFICATE REQUEST----- " and "-----END CERTIFICATE
REQUEST----- "
```

lines.

7. Submit the CSR to Verisign, Entrust, or any other CA.

   The process for submitting the CSR varies with each CA. Use your Web browser to access your CA's Web site and follow the online instructions. When prompted, paste the CSR into the space provided on the CA's online request process. If the CA requires that you specify a server software vendor whose software you supposedly used to generate the CSR, specify Apache.

   The CA will return the signed certificate for installation. The certificate is then ready to be added into the VPN Gateway.

Adding Certificates to the AVG

Using the encryption capabilities of the VPN Gateway requires adding a key and certificate that conforms to the X.509 standard to the VPN Gateway. If you have more than one VPN Gateway in a cluster, the key and certificate need only be added to one of the devices. As with configuration changes, the information is automatically propagated to all other devices in the cluster.

Note:

When using an ASA 310-FIPS running in FIPS mode, the private key associated with a certificate cannot be imported. All private keys must be generated on the HSM card itself due to the FIPS security requirements.

There are two ways to install a key and certificate into the VPN Gateway :

- Copy-and-paste the key/certificate.
- Download the key/certificate from a TFTP/FTP/SCP/SFTP server.

Comments? infodev@avaya.com

The VPN Gateway supports importing certificates and keys in these fomats:

- PEM
- NET
- DER
- PKCS7 (certificate only)
- PKCS8 (keys only, used in WebLogic)
- PKCS12 (also known as PFX)

Besides these formats, keys in the proprietary format used in MS IIS 4 can be imported by the VPN Gateway, as wells as keys from Netscape Enterprise Server or iPlanet Server. Importing keys from Netscape Enterprise Server or iPlanet Server however, require that you first use a conversion tool. For more information about the conversion tool, contact Avaya. See Customer service on page 11 for contact information.

When it comes to exporting certificates and keys from the VPN Gateway, you can specify to save in the PEM, NET, DER, or PKCS12 format when using the **`export`** command. If you choose to use the **`display`** command (which requires a copy-and-paste operation), you are restricted to saving certificates and keys in the PEM format only.

Note:

When performing a copy-and-paste operation to add a certificate or key, you must always use the PEM format.

Copy-and-Paste Certificates

The following steps demonstrate how to add a certificate using the copy-and-paste method.

Note:

If you connect to one of the VPN Gateways in the cluster by using a console connection,note that HyperTerminal under Microsoft Windows may be slow to complete copy-and-paste operations. If your security policy permits enabling Telnet or SSH access to the VPN Gateway, use a Telnet or SSH client and connect to the Management IP address instead.

1. Type the following command from the Main menu prompt to start adding a certificate.

```
>> Main#cfg/cert

Enter certificate number: (1-)<number of the certificate you want
to configure>

>> Certificate 1#cert

Paste the certificate, press Enter to create a new line, and then
type "..." (without the quotation marks) to terminate.

>
```

In most cases you should specify the same certificate number as the certificate number you used when generating the CSR. By doing so, you do not have to add the private key because this key remains connected to the certificate number that you used when you generated the CSR.

If you have obtained a key and a certificate by other means than generating a CSR using the **request** command on the VPN Gateway, specify a certificate number not used by a configured certificate before pasting the certificate. If the private key and the certificate are not in the same file, use the **key** or **import** command to add the corresponding private key.

To view basic information about configured certificates, use the **/info/certs** command. The information displayed lists all configured certificates by their main attributes.

2. Copy the contents of your certificate file.

   Open the certificate file you have received from a CA in a text editor and copy the entire contents. Make sure the selected text includes the

   ```
   " -----BEGIN CERTIFICATE----- "
   ```

   and

   ```
   " -----END CERTIFICATE----- "
   ```

   lines.

3. Paste the contents of the certificate file at the command prompt.

   Now, paste the certificate at the command line interface prompt, press ENTER to create a new empty line, and then type " ... " (without the quotation marks). Press ENTER again to complete the installation of the certificate.

   Your screen output should now resemble the following example:

Comments? infodev@avaya.com

```
>> Certificate 1# cert
Paste the certificate, press Enter to create a new line, and then
type "..." (without the quotation marks) to terminate.
> -----BEGIN CERTIFICATE-----
> MIIDTDCCArWgAwIBAgIBADANBgkqhkiG9w0BAQQFADB9MQswCQYDVQQGEwJzZTEO
> MAwGA1UECBMFa2lzdGExEjAQBgNVBAcTCXN0b2NraG9sbTEMMAoGA1UEChMDZG9j
> MQ0wCwYDVQQLEwRibHVlMRIwEAYDVQQDEwl3d3cuYS5jb20xGTAXBgkqhkiG9w0B
> CQEWCnR0dEBjY2MuZG4wHhcNMDAxMjIyMDkxOTI0WhcNMDExMjIyMDkxOTI0WjB9
> MQswCQYDVQQGEwJzZTEOMAwGA1UECBMFa2lzdGExEjAQBgNVBAcTCXN0b2NraG9s
> bTEMMAoGA1UEChMDZG9jMQ0wCwYDVQQLEwRibHVlMRIwEAYDVQQDEwl3d3cuYS5j
> b20xGTAXBgkqhkiG9w0BCQEWCnR0dEBjY2MuZG4wgZ8wDQYJKoZIhvcNAQEBBQAD
> gY0AMIGJAoGBALXym9cIVfHZUZFE1MFi+xefDviIEvilnJAQSSPITnZa69fzGcL3
> vpQv0NLxNffs1jEw4RPDMKu2rQ9N02EiiJcrCHnaSNZPdwGoX39IkEUkANzm3mh2
> DlP1RfW4ejpNKsG5Tme/e1vFYWXeXXI1oRtdPIaVGxK8pvqBEHDXCcJlAgMBAAGj
> gdswgdgwHQYDVR0OBBYEFJBM3K0KB03fpCOVrQCC34hovwM8MIGoBgNVHSMEgaAw
> gZ2AFJBM3K0KB03fpCOVrQCC34hovwM8oYGBpH8wfTELMAkGA1UEBhMCc2UxDjAM
> BgNVBAgTBWtpc3RhMRIwEAYDVQQHEwlzdG9ja2hvbG0xDDAKBgNVBAoTA2RvYzEN
> MAsGA1UECxMEYmx1ZTESMBAGA1UEAxMJd3d3LmEuY29tMRkwFwYJKoZIhvcNAQkB
> Fgp0dHRAY2NjLmRuggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEEBQADgYEA
> m/GKwEyDKCm2qdPt8+pz1znSGNaRTxfK1R0mjtnDGFb0qk+Bv7d9YlX+1QTZhxnZ
> Z4JXuWPJS36kAwiirVbOIaIforIVa+IUlo8HUjMvxzIqCYPiiDwBcBi3NsvjlFM7
> i24Q+lvDLE/Ko+x/YEnNukfp3SBXiJqZ8WZIvbTCyT4=
> -----END CERTIFICATE-----
> ...
Certificate added.
```

Note:

Depending on the type of certificate the CA generates (registered or chain), your certificate may appear substantially different from the one shown before. Be sure to copy and paste the entire contents of the certificate file.

4. Apply your changes.

```
>> Certificate 1#apply

Changes applied successfully.
```

If you have used the request command on the VPN Gateway to generate a CSR, and have specified the same certificate number as the CSR when pasting the contents of the certificate file, your certificate is now fully installed.

If you have obtained a certificate by other means, however, you must also add the corresponding private key.

Copy-and-Paste Private Key

1. Type the following command from the Main menu prompt to start adding a private key.

   Make sure you specify the same certificate number as when pasting the certificate.

   ```
   >> Main#cfg/cert

   Enter certificate number: (1-)<number of the certificate you want
   to configure>

   >> Certificate 1#key

   Paste the key, press Enter to create a new line, and then type
   "..."  (without the quotation marks) to terminate.
   >
   ```

2. Copy the contents of your private key file.

   Locate the file containing your private key. Make sure the key file corresponds with the certificate file you have received from a CA. The public key in the certificate works in concert with the related private key when handling SSL transactions.

   Open the key file in a text editor and copy the entire contents. Make sure the selected text includes the

   ```
   " -----BEGIN RSA PRIVATE KEY----- "
   ```

   and

   ```
   " -----END RSA PRIVATE KEY----- "
   ```

   lines.

3. Paste the contents of the key file at the command prompt.

   Now, paste the private key at the command line interface prompt. Press ENTER to create a new row, and then type " ... " (without the quotation marks). Press ENTER again to complete the installation of the key.

   You may be prompted for a password phrase after having completed the paste operation. The password phrase you are requested to type is the one you specified when creating (or exporting) the private key.

   Your screen output should now resemble the following example.

Comments? infodev@avaya.com

```
>> Certificate 1# key
Paste the key, press Enter to create a new line, and then type "..."
(without the quotation marks) to terminate.
> -----BEGIN RSA PRIVATE KEY-----
> Proc-Type: 4,ENCRYPTED
> DEK-Info: DES-EDE3-CBC,2C60C89FEB57A853
>
> MbbLDYlwdbNfXUGHFm10nfRlI+KTnx2Bdx750EaG8HSVV7KrtnsNF/Fsz1jFvO/j
> nKhZfs4zsVrsstrVlqfP1uatg19VyJSEug1ZcCamH59Dcy+UNocFWCzR56PHpyZK
> GXX66jS+6twYdiXQk58URIudkmGXGTYMvBRuVjV22ZRLyJk41Az5nA6HiDz6GGs6
> vkCaPFGm263KxmXjy/okNgSJl9QTqJfSq7Eh1cIslBReAE9HXGl0Eubb6gVJu+sR
> mGhS/yGx4vMx98wiMjL37gRtXBfDWlu6u0HOPeJxs6fH05fYzmnpwAHj592TDFds
> Ji5pmrY0NhAeXfuG8mF/T9nEz02ZA8iQGJsaUPfkeBxbZS+umY/R65Okwt1k2RN4
> RlFnmRWqvhHMrHzJuegez/806YazHBv74sOg3KgETRH92z5yvwbgFwmffgb+hai0
> RlRtZgQ4A5kSAFYW37KDq6eJBsZ/m3Que1buMbh8tRxdGpo54+bGqu5b12iLanLn
> Rk57ENQGTgzxOD/1RZIJHqObCY7VDLkK7WZM/LPa0k+bTeAysmZa7fu7gvELJF0i
> vszs3nzm7zT1y0mJ0QX9u9eoW8wpASCAdCC2r2LZt8o9+IWLSZWh5UCIr8qFKGiL
> rUIx8coIhxSpx/PqEV8KhSRV+0taq0N7pJa3TLmO3o80t5966VSFKc3Y35fx9Yk8
> G+RlSzo4CxooY4bCKsfchnJ957SJx5vUyh6jjztnuU4iAfeTVCUdF0LXd+NlQ7T7
> IMFsjjx9SZuuHPZTF0KD/WYLx7FfIFIBHDumu6scraYZOaWaJKI5Pw==
> -----END RSA PRIVATE KEY-----
> ...
Enter pass phrase:
Key added
```

4. Apply your changes.

```
>> Certificate 1#apply

Changes applied successfully.
```

Your certificate and private key is now fully installed and ready to be taken into use.

If the AVG software is used for SSL acceleration purposes, the certificate should be mapped to the virtual SSL server, using the **/cfg/ssl/server #/ssl/cert** command.

If the AVG software is used for deployment of a VPN solution, the certificate should be mapped to the portal server of the desired VPN, using the **/cfg/vpn #/ server/ssl /cert** command.

To view basic information about configured certificates, use the **/cfg/cur cert** command.

Using TFTP/FTP/SCP/SFTP to add Certificates and Keys

The following is an example of how to input a certificate into the VPN Gateway using TFTP, FTP, SCP, or SFTP.

1. Put the certificate file and key file on your TFTP/FTP/SCP/SFTP server.

   Note:

   You may arrange to include your private key in the certificate file. When the specified certificate file is retrieved from the TFTP/FTP/SCP/SFTP server, the AVG software will analyze the contents and automatically add the private key, if present (the screen output appears "Certificate added" and "Key added" in this case). If the private key is included, you do not have to perform step 5.

2. Initiate the process of adding a certificate using TFTP/FTP/SCP/SFTP.

   Type the command `/cfg/cert` and press `ENTER`. Specify an unused certificate index number, and then type the command `import`.

   Make sure to specify a certificate number not in use by an existing certificate. To view basic information about all configured certificates, use the **`/info/certs`** command.

```
>> Main#cfg/cert

Enter certificate number: (1-)<number of the certificate you want
to configure>

>> Certificate 1#import

Select protocol (tftp/ftp/scp/sftp) [tftp]:ftp

Enter host name or IP address of server:<server host name or IP
address>
```

3. Enter the desired file name.

```
Enter filename on server:<filename.crt>

Retrieving VIP_1.crt from 192.168.128.58
```

4. If you are importing the file from an FTP server you are prompted for a user name.

   Log in to the FTP server with your user name and password. For anonymous mode, the following string is used as the password (for logging purposes):

```
admin@hostname/IP.isd.
```


Comments? infodev@avaya.com

You may also be prompted for a password phrase (if specified when creating or exporting the private key)

```
FTP User (anonymous):<username or press ENTER for anonymous mode>

Password:<password or press ENTER for default password in
anonymous mode>

received 2392 bytes
Enter pass phrase:
```

Provided the operation was successful and the certificate file includes your private key, your screen output should resemble the following example:

```


Key added.
Certificate added.
Use 'apply' to activate changes.
```

5. Add your private key (if in a separate file).

   This step is only required if the certificate file does not include the private key. You may be prompted for a password phrase (if specified when creating or exporting the private key).

```
>> Certificate 1#import

Select protocol (tftp/ftp/scp/sftp) [tftp]:ftp

Enter host name or IP address of server:<server host name or IP
address>

Enter filename on server:<filename.key>

Retrieving VIP_1.key from 192.168.128.58

FTP User (anonymous):<username or press ENTER for anonymous mode>

Password:<password or press ENTER for default password in
anonymous mode>

received 392 bytes
Enter pass phrase:
Key added.
Use 'apply' to activate changes.
```

6. Apply your changes.

```
>> Certificate 1#apply

Changes applied successfully.
```

If the AVG software is used for SSL acceleration purposes, the certificate should be mapped to the virtual SSL server, using the **/cfg/ssl/server #/ssl/cert**command.

If the AVG software is used for deployment of a VPN solution, the certificate should be mapped to the portal server of the desired VPN, using the **/cfg/vpn #/server/ssl /cert** command.

To view basic information about configured certificates, use the **/cfg/cur cert** command.

Update Existing Certificate

Whenever you wish to substitute an existing certificate for a new certificate, you should keep the existing certificate until it is verified that the new certificate works as designed.

Create a New Certificate

1. Check the certificate numbers currently in use.

```
>> Main#cfg/cur cert
```

   If for example, two different certificates exist as Certificate 1 and Certificate 2, create Certificate 3 for your new certificate.

2. Add a certificate with a new certificate number.

```
>> Configuration#cert

Enter certificate number: (1-1500)3

Creating Certificate 3
```

3. Add the new certificate according to the instructions in Adding Certificates to the AVG on page 86.
4. Map the new certificate to the desired servers.

   The following example refers to a virtual SSL server used for SSL acceleration. To map the certificate to a portal server in a VPN, use the **/cfg/vpn #/server/ssl/cert** command.

Comments? infodev@avaya.com

```
>> Configuration#ssl/server

Enter virtual server number: (1-256)1

>> Server 1#ssl

>> SSL Settings#cert

Current value: 2
Enter certificate number: (1-1500)3
```

After you have tested that the new certificate works fine you may delete the old certificate(s).

Configure a Virtual SSL Server to Require a Client Certificate

This section describes how to configure client certificate authentication when the VPN Gateway is used for SSL acceleration.

Note:

For information about how to configure client certificate authentication in conjunction with VPN deployment, see the "Authentication Methods" chapter in the *Application Guide for VPN*.

As explained previously in this chapter, each virtual SSL server on the VPN Gateway should be configured to use a server certificate to authenticate itself towards the clients. Besides, the server can be configured to require client certificates to authenticate clients before granting access to the requested service.

When a server is set to require client certificates, a CertificateRequest message is sent from the server to the client during the SSL handshake. The client responds by sending its public key certificate in a Certificate message. After that, the client will send a CertificateVerify message to the server. The CertificateVerify message is signed by using the clients private key, and contains important information about the SSL session known to both the client and the server. Upon receiving the CertificateVerify message, the virtual SSL server will use the public key from the client certificate to authenticate the client's identity.

The virtual SSL server will also check if the certificate the client presents is signed by an accepted certificate authority (CA). Accepted certificate authorities are defined by the CA certificates you have listed on the virtual SSL server. The certificate you use for generating client certificates must therefore also be specified as a CA certificate on the virtual SSL server.

In addition, the virtual SSL server checks if the client certificate should be revoked, by comparing the serial number of the presented client certificate with entries in the certificate revocation list.

The following steps demonstrate how to configure a virtual SSL server to require client certificates for authentication purposes.

1. Display information about current virtual SSL servers.

   This command displays information about all virtual SSL servers on the VPN Gateway, including installed certificate. Based on the information displayed, decide which virtual SSL server to configure for client authentication.

```
>> Main#cfg/cur ssl
```

2. Configure the chosen virtual SSL server to require client certificates.

   The client must send its client certificate to the virtual SSL server during the SSL handshake. If the client does not have a certificate, the client will respond with a NoCertificateAlert message. At that point, the session will be terminated.

```
>> SSL#server 1

>> Server 1#ssl

>> SSL Settings#verify

Current value: none
Certificate verification (none/optional/require):require
```

3. Specify which CA certificates to use for client authentication.

   Specify which CA certificates you want the virtual SSL server to use for authenticating client certificates. Only those client certificates that are issued by a certificate authority whose CA certificate you specify, will be accepted. Note that the CA certificates you specify by index number must be available on the VPN Gateway itself.

   To authenticate client certificates issued within your own organization, the CA certificate used for generating the issued client certificates must be specified as a CA certificate.

```
>> SSL Settings#cacerts

Current value:""

Enter certificate numbers (separated by comma):<CA certificates
by index number>
```

   To view basic information about all certificates currently added to the VPN Gateway, use the **/info/certs** command.

4. Apply your settings.

Comments? infodev@avaya.com

```
>> SSL Settings#apply

Changes applied successfully.
```

Generating client certificates

Before issuing client certificates, you should establish the means of validating the identities of the users. The credentials users need to present to obtain a client certificate may vary, depending on the type of service, the size of your organization, and so on.

1. Specify a CA certificate by index number to use for generating a client certificate, and generate the client certificate.

   In this example certificate number 1 is specified for generating a client certificate. The private key corresponding with the public key in the certificate you specify is used for signing the client certificate.

```
>>  Main#cfg/cert

Enter certificate number: (1-)1

>>  Certificate 1#gensigned

Type of certificate (server/client) [client]:<press ENTER for
client certificate>

The combined length of the following parameters may not exceed
225 bytes.
Country Name (2 letter code):
State or Province Name (full name):
Locality Name (e.g., city):
Organization Name (e.g., company):
Organizational Unit Name (e.g., section):
Common Name (e.g., your name or your server's hostname):
Email Address:
Subject alternative name (blank or comma separated list of
URI:<uri>, DNS:<fqdn>, IP:<ip-address>, email:<email-address>):
```

   To view basic information about all available certificates, use the **/info/certs** command.

   Note:

   Only certificates having the basic constraint CA:TRUE can be used for generating client certificates. When generating a client certificate, the VPN Gateway automatically checks that the current certificate has this constraint. To perform this check yourself, use the **/cfg/cert #/show** command and look for lines containing the text

```
X509v3 Basic Constraints:CA:TRUE|FALSE
```

in the screen output.

2. When prompted, provide the following information to include in the client certificate:

   Note that you do not have to complete all fields. Only one of Common Name and E-mail Address is strictly required.

   - Country Name (2 letter code): The two-letter ISO code for the country in which the subject resides. With subject is meant the person for whom the client certificate is created. For current information about ISO country codes, visit for example http://www.iana.org/.
   - State or Province Name (full name): The full name of the state or province in which the subject resides.
   - Locality Name (for example, city): The name of the city or town where the subject resides.
   - Organization Name (for example., company): The registered name of the organization to which the subjects belongs. Do not abbreviate the organization name and do not use the following characters:

     `< > ~ ! @ # $ % ^ * / \ ( ) ?`
   - Organizational Unit Name (for example,, section): The unit name of the organization to which the subject belongs.
   - Common Name (for example,, the subject's name): The full name of the subject.
   - E-mail Address: The full e-mail address of the subject.
   - Subject alternative name: Comma-separated list of URI:<uri>, DNS:<fqdn>, IP:<ip address>, email:<e-mail address>. Example:

     `URI:http://www.example.com,email:john@example.com,IP:10.1.2.3`

3. Specify the validity period, key size, and serial number.

   After having provided information about the subject, you are now ready to specify information relating to the client certificate itself.

   Decide how many days the client certificate should be valid. By default, each new client certificate is set to be valid for 365 days. Also decide which key size should be used. The default key size is set to 512 bits, which is appropriate in most cases. Note that export versions of Internet Explorer 4.x (40-bit encryption) and Internet Explorer 5 (56-bit encryption) cannot import client certificates with a larger key size than 512.

   Assign a serial number to the client certificate, or accept the suggested number. When generating a new client certificate, the lowest available serial number is displayed in square brackets and will be used unless you specify a different number. As you generate more client certificates, the proposed serial number increments automatically.

```
>> Certificate 1#
Valid for days [365]:
```


Comments? infodev@avaya.com

```
Key size (512/1024) [512]:
Serial number of client certificate [1]:
```

4. Decide whether to save the client certificate and define a pass phrase for the private key.



```
>> Certificate 1#
Save signed certificate (yes/no) [yes]: (press ENTER to save the certificate)
Select cert no. to save to [2]: (press ENTER to accept the suggested certificate index
number)
Encrypt private key (yes/no) [yes]: (press ENTER to encrypt the private key)
Enter export pass phrase: (define a pass phrase to protect the encrypted private key)
Reconfirm export pass phrase:
Creating new cert 2
Use 'apply' to save signed key and certificate.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,5B2BFB939B4A9524

ErcHmgvzyLuaGn9WXrkZgn/EY6CcrgluO7d4fh/a3YuCBFPgiE8NKs7HtqJ6RPfb
K/Uinv7MaRSmRzIIbojOaOk6jZUsP1U7d+60Hy/kqfnMI7mI2cByHFvJ1IfZ5Dfs
SyJFmbMY5fG7MPtcbaUjuTedmBw5Vc5JnpmfYqndCuvMMI4H8HM6PgEHggJctBoJ
iaENDtCEbhaUX6B6+7qzXBpcUx6GJoQ3P8b07YrGhkfY9KNGT4Dg1KBHJiT4Wgua
+voUIIWPebSC5XCfR6bnIFykxNrFPWMV+2FwxNs6to6QPY2sARwym8/pK2CQFW5b
mojNTWtW9U9UObAvV1TUCSUauARy3aVANtY7bi7HX93Yypk5FXFVn75RoTMB7GIZ
jxwL3R7kZFsEmHe/NE4lkiLHRFd+IxbbRdNC1Zw47qu=
-----END RSA PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
MIIDyjCCAzOgAwIBAgIBATANBgkqhkiG9w0BAQQFADCBqjELMAkGA1UEBhMCVVMx
FDASBgNVBAgTC09ha2xhZm9ybmlhMRAwDgYDVQQHEwdUZXN0aW5nMRIwEAYDVQQK
EwlUZXN0IEluYy4xEjAQBgNVBAsTCXRlc3QgZGVwdDEgMB4GA1UEAxMXd3d3LmRl
bWl5c3NsdGVzdGluZy5jb20xKTAnBgkqhkiG9w0BCQEWGnRlc3RlckBkdWlteXNz
bHRlc3RpbmcuY29tMB4XDTAxMDIyNzEyMzAzMFoXDTAyMDIyNzEyMzAzMFowgZQx
CzAJBgNVBAYTAlNFMRIwEAYDVQQIEwlTdG9ja2hvbG0xDjAMBgNVBAcTBUtpe3Rh
MREwDwYDVQQKEwhCbHVldGFpbDENMAsGA1UECxMERG9jdTEZMBcGA1UEAxMQd3d3
LmJsdWV0YWlsLmNvbTEkMCIGCSqGSIb3DQEJARYVdG9yYmpvcm5AYmxlZXRhaWwu
Y29tMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALNjbwor//Gz3CsugRPJvcw36tml
O9BuZ8lg2NTahrXJKKotRb947c7YJgTIYFnlaOHV7tpRUnp5yASCzBHBt0MCAwEA
AaOCAVIwggFSMAkGA1UdEwQCMAAwEQYJYIZIAYb4QgEBAQDAgWgMAsGA1UdDwQE
AwIF4DAsBglghkgBhvhCAQ0EHxYdaVNELVNTTCBHZW5lcmF0ZWQgQ2VydGlmaWNh
dGUwHQYDVR0OBBYEFDdbxK9VEsti/nS/lcTxp9eMYVfdMIHXBgNVHSMEgc8wgcyA
FIZ96B3BhMl2d8GJ1/GrC+Shs5gtoYGwpIGtMIGqMQswCQYDVQQGEwJVUzEUMBIG
A1UECBMLT2FrbGFmb3JuaWExEDAOBgNVBAcTB1Rle3RpbmcxEjAQBgNVBAoTCVRl
c3QgSW5jLjESMBAGA1UECxMJdGVzdCBkZXB0MSAwHgYDVQQDExd3d3cuZHVtbXlz
c2x0ZXN0aW5nLmNvbTEpMCcGCSqGSIb3DQEJARYadGVzdGVyQGR1bW15c3NsdGVz
dGluZy5jb22CAQAwDQYJKoZIhvcNAQEEBQADgYEAlEIbixeNQqSUIiRJ26ty8vQW
TqpEP7B9dGGqPnGXTQQ8QqjHaaGppYDAUZAceFGWHG94fIS7OtRqX40zrsC05lbn
2kMMz/XVj78Z3/nr+mv4RmlZGXmAEhVo2XjvVFChOF74XcMyAzOQp3UVvTVsFULK
AlqnIZ0SWnc9T8xR0lU=
-----END CERTIFICATE-----
Use 'apply' to save incremented certificate serial number.
```

You should save the client certificate and assign a certificate index number to it. The lowest available index number available is displayed in square brackets and will be used unless you specify a different number.

By saving the certificate, you can later easily access the certificate by specifying the assigned index number at the

```
cert
```

prompt. After having specified the assigned index number, you can use the **`display`** or **`export`** command to prepare for the transfer of the client certificate to the subject. To view basic information about all saved certificates, use the **`/info/certs`** command.

If you choose to not save the client certificate, you will need to save the private key and the certificate to a file by performing a copy-and-paste operation to a text editor. The private key and the certificate are displayed on screen as soon as you reconfirm the chosen password phrase. The private key and the certificate are combined and saved in the PEM format when using a copy-and-paste operation.

The requested pass phrase is a word or code that you need to define. The pass phrase protects the encrypted key against illegitimate use. When the intended user installs the client certificate into a Web browser or e-mail client, the correct pass phrase (which you defined) is required to unlock the certificate.

5. Verify that the certificate you used for generating the client certificate is specified as a CA certificate for the appropriate virtual SSL server.

```
>> Main#cfg/ssl/server

Enter virtual server number: (1-)1

>> Server 1#ssl

>> SSL Settings#cacerts

Current value: 1
Enter certificate numbers (separated by comma):
```

To successfully validate the client certificate on authentication, you need to verify that the certificate you used for generating the client certificate is also specified as a CA certificate for the appropriate virtual SSL server. In the sample screen preceding output, the certificate has already been defined as a CA certificate. This is observable by the line

```
Current value: 1,
```

where number 1 is the index number of the certificate that was used when generating the client certificate. If the certificate index number representing the certificate you used when generating client certificates is not listed by

```
Current value:
```

, type the certificate index number and apply your changes.

If the correct certificate index number is already listed by

```
Current value:
```

, press ENTER and answer no to the question if you want to clear the list.

Export Client Certificate

Before you transfer the private key and client certificate to the subject, you should save the key and the certificate to a file using the **export** or **display** command on the Certificate menu. The **export** command (see following instruction) is recommended, as this provides

Comments? infodev@avaya.com

you with the option to select the PKCS12 file format (also known as PFX). Most Web browsers accept importing a combined key and certificate file in the PKCS12 format.

This is how to export the client certificate to a TFTP/FTP/SCP/SFTP server.

1. Specify the number of the certificate you wish to export.

   When you generated the client certificate you had the option to save it with a new certificate number. In the previous example (Step 4), the client certificate was saved as certificate number 2. Enter this certificate number when prompted, then use the `export` command to export the certificate as a file.

```
>> Main#cfg/cert

Enter certificate number: (1-)2

>> Certificate 1#export

Select protocol (tftp/ftp/scp/sftp) [tftp]:ftp

Enter hostname or IP address of server:ftp.example.com
```

2. Select the desired export format, enter a pass phrase and specify the name of the output file.

```
Enter export format (pem/der/net/pkcs12):pkcs12

Enter export pass phrase:<passphrase>

Reconfirm export pass phrase:<passphrase once again>

Enter name of combined key and certificate file on remote
host:cert.pfx

FTP User (anonymous):<FTP user name>

Password:<password>

sent 2392 bytes
```

Transmit Private Key and Certificate to User

Transmit the client certificate and the pass phrase protected private key to the user in a secure manner. Never send the password phrase in an e-mail message.

The user will then need to import the received client certificate into his or her Web browser or e-mail program. For more information about importing certificates, refer to the help system of the destination Web browser or e-mail program.

Managing Revocation of Client Certificates

Certificate revocation lists (CRLs) are maintained by certificate authorities to recall client certificates that are no longer considered trustworthy. The reasons for this can be that the client certificate may have been issued by mistake, or that the subject accidentally has revealed the private key.

By keeping a certificate revocation list on your SSL server, client certificates sent to the server are checked against the CRL. If a match is found, the SSL session is terminated. This mode of operation requires, first of all, that you have configured the virtual SSL server to always require client certificates. (For more information, see Configure a Virtual SSL Server to Require a Client Certificate on page 95). You must also regularly check with the certificate authorities you trust for their latest CRLs.

Moreover, if you take on the role of a certificate authority by issuing your own client certificates, you will also need to maintain your own certificate revocation lists. This can be done by listing the serial numbers of the client certificates you want to revoke in an ASCII file. You may also specify the serial number of a particular client certificate directly in the command line interface by using the add command in the Revocation menu.

Revoking Client Certificates Issued by an External CA

1. Specify the CA certificate, to which you want to add a CRL.

   The certificate you specify must be a CA certificate from the same certificate authority that published the CRL you are about to add. To view basic information about available certificates, use the **/info/certs** command.

   ```
   >> Main#cfg/cert

   Enter certificate number: (1-)1

   (example)

   >> Certificate 1#revoke
   ```

2. Download and add a CRL from a TFTP/FTP/SCP/SFTP server.

   Specify the host name or IP address of the TFTP/FTP/SCP/SFTP server, and provide the file name of the CRL. The CRL is retrieved and added to Certificate 1 (used as an example).

   ```
   >> Revocation#import
   ```


Comments? infodev@avaya.com

```
Select protocol (tftp/ftp/scp/sftp) [tftp]:ftp

Enter host or IP address of server:192.168.128.20

(example)

Enter name of file on server (PEM, DER or ASCII format):crl.der

Retrieving crl.der from 192.168.128.20

Received 12628 bytes in 0.1 seconds

Certificate revocation list found in der format
Revocation list added.
Use 'apply' to activate changes.
```

3. Apply your changes.

```
>> Revocation#apply

Changes applied successfully.
```

Revoking Client Certificates Issued within your Own Organization

1. Specify the CA certificate, to which you want to add a CRL.

   Specify the certificate number that represents the CA certificate of the certificate used for generating the client certificate you want to revoke. To view basic information about available certificates, use the **`/info/certs`** command.

```
>> Main#cfg/cert

Enter certificate number: (1-)1

(example)

>> Certificate 1#revoke
```

2. Add the serial number of a specific client certificate to revoke.

```
>> Revocation#add

Enter serial number to revoke:
```

   To add serial numbers in hexadecimal form, enter `addx` instead of `add`.

Repeat this step for each serial number you want to add. To display the serial number (along with subject information) for a saved client certificate, use the **/info/certs** command.

Or, download and add your own CRL in ASCII format from a remote machine.

```
>> Revocation#import

Select protocol (tftp/ftp/scp/sftp) [tftp]:ftp

Enter host or IP address of server:192.168.128.20

(example)

Enter name of file on server (PEM, DER or ASCII
format):crl.ascii

Retrieving crl.ascii from 192.168.128.20
Received 12628 bytes in 0.1 seconds


Certificate revocation list found in ascii format
Revocation list added.
Use 'apply' to activate changes.
```

If you have added serial numbers for particular client certificates by using the add command prior to using the `import` command, you will be asked if you want to merge those serial numbers to the CRL in ASCII format. If the CRL does not already include those serial numbers, choose to merge them. However, make sure that you update the original CRL with the merged serial numbers before the next download, as you will otherwise lose them. For more information about how to build your own CRL, see Creating Your Own Certificate Revocation List on page 104.

3. Verify that the serial numbers of the client certificates you want to revoke have been added.

```
>> Revocation#list

Revoked certificates:
```

4. Apply your changes.

```
>> Revocation#apply

Changes applied successfully.
```

Creating Your Own Certificate Revocation List

You can easily build and manage certificate revocation lists for client certificates issued within your own organization. The CRL can then be added by using TFTP/FTP/SCP/SFTP. For more

information about how to accomplish this, see Revoking Client Certificates Issued within your Own Organization on page 103.

1. Open a text editor and create a new file.
2. Decide if you want to add serial numbers in decimal form, or in hexadecimal form.

   If you choose to add serial numbers for client certificates to revoke in decimal form, add a paragraph in the text document that reads:

   ```
   ASCII revocation
   ```

   Or, if you choose to add serial numbers in hexadecimal form, add a paragraph in the text document that reads:

   ```
   HEX ASCII revocation
   ```

   Note:

   You can add comments to a CRL ASCII file by preceding your comments with the # character. Each new line of comments must begin with the # character. Comments can be used for providing information about the date of issue or last update, for example. You can cancel the revocation of a client certificate by inserting the # character at the beginning of the line containing the desired serial number.
3. Add the serial numbers of the client certificates you want to revoke.

   For a CRL in decimal format, simply list the serial numbers the ASCII revocation paragraph. For example:

   ```
   # CRL for CA certificate 1
   # Issued first: 2005-01-01
   # Last update: 2005-02-01
   ASCII revocation

   500
   501
   590
   ```

   Or, for a CRL in hexadecimal format, list the serial numbers by their hexadecimal values below the HEX ASCII revocation paragraph. For example:

```
# CRL for CA certificate 1

# Issued first: 2005-01-01

# Last update: 2005-02-01

HEX ASCII revocation

1F4

1F5

24E
```

4. Save the file, and upload it to a TFTP/FTP/SCP/SFTP server that can be accessed from your VPN Gateway(s).

Automatic CRL Retrieval

Automatic CRL retrieval is used for configuring access to a server containing CRLs (certificate revocation lists), and retrieving such lists at regular intervals to automate the task of keeping the CRL up-to-date.

Note:

When enabling automatic retrieval of certificate revocation lists, any existing revocation list is overwritten.

You can use LDAP, HTTP, or TFTP to retrieve CRLs from the appropriate server (for LDAP, the server must support LDAP v3). When using LDAP, a bind operation to the specified LDAP server is performed each time a CRL retrieval occurs. The bind operation uses the specified distinguished name and password. Directly after a successful bind operation, a search for the CRL attribute specified in the URL is performed on the LDAP server. For more information about the implementation details behind these operations, see RFC 2251.

1. Specify the URL from which the CRL list should be retrieved.

   This step sets the complete URL for retrieving a CRL using LDAP, HTTP, or TFTP. If you are not using the default TCP port of the respective protocol, the TCP port number must also be included in the URL.

   If you want to retrieve CRLs from an LDAP server, you need to provide the distinguished name of the specific object on the LDAP server, together with the attribute that holds the CRL (all in accordance with RFC 2255). Example:

   ```
   ldap://10.42.128.30:389/cn=VeriSign CRL,o=Your Organization?
   CertificateDiscHyphenRevocationList;binary
   ```


Comments? infodev@avaya.com

Note:

RFC 2255 states that entering host information is optional. The AVG software's implementation of the CRL retrieval feature however requires that host information is specified.

Using HTTP or TFTP, the URL you specify must include the specific file name you want to access. The recognized URL syntax is a subset of RFC 1738, and can be defined as:

```
<proto>://<host>[:<port>]/<path>.
```

Example:

```
http://10.42.128.30/server.crl
```

```
>> Main/cfg/cert 1/revoke/automatic

>> Automatic CRL#url

Current value:""

Enter URL to retrieve from:
```

2. Set the distinguished name used for binding and authenticating the initiated LDAP session on the specified LDAP server.

   Check your LDAP server documentation for details on binding, authentication, and access control. Example:

   ```
   cn=Bill Smith,o=Your Organization
   ```

   By setting the `/cfg/cert #/revoke/automatic/anonymous` command to `true`, you can enable anonymous binding for automatic CRL retrieval through LDAP. In this case, the **`authDN`** and **`passwd`** commands (see the following sections) can be set to anything, including an empty string.

   When using HTTP or TFTP to retrieve a CRL, you do not need to provide a distinguished name for binding and authentication.

   ```
   >> Automatic CRL#authDN

   Current value:""

   Enter DN:
   ```

3. Set the password used for binding and authenticating the initiated LDAP session on the specified LDAP server.

   Check your LDAP server documentation for details on binding, authentication, and access control.

When using HTTP or TFTP to retrieve a CRL, you don't need to provide a password for binding and authentication.

```
>> Automatic CRL#passwd

Current value:""

Enter password:
```

4. Set the time interval for retrieving CRLs from the resource you have specified using the **url** command.

   If you want to specify a time interval in minutes, hours or days, enter an integer directly followed by the letter m, h, or d.

   The default interval is 1 day (1d). The shortest time interval allowed is 601 seconds (10 minutes and 1 second).

```
>> Automatic CRL#interval

Current value: 1d
Enter refresh interval:
```

5. Specify which CA certificates are valid signers of the certificate revocation lists you retrieve.

   To get an overview over all available certificates, enter the **/info/certs** command.

   When specifying more than one certificate, use commas to separate the corresponding index numbers. Example: 1,2,5

   To clear all specified CA certificates, press ENTER when asked to enter certificate numbers, then answer yes to the question if you want to clear the list.

```
>> Automatic CRL#cacert

Current value:""

Enter certificate numbers (separated by comma):
```

6. Enable automatic retrieval of CRLs.

```
>> Automatic CRL#ena
```

   When using the **apply** command the first time after having enabled automatic retrieval of CRLs, a first retrieval is invoked immediately. After that, retrievals will

Comments? infodev@avaya.com

occur at the specified time interval (where the default value is once every 24 hours).

7. Apply the changes.

Client certificate support

Authentication with AVG server can be done through NDIC using client certificates.

Follow these steps to authenticate using client certificates:

1. Indicate whether client certificate authentication is needed for NDIC connection profile.

   If connection is required, then NDIC hides the user name and password fields and replaces it with a message indicating, client certificate is required to connect.
2. Click **Connect**.

   The MSCAPI window appears.
3. Select the certificate in the **MSCAPI** window.
4. If secondary authentication is not required, then you can connect using Net Direct.
5. If secondary authentication is required, then AVG extracts the user name. The user name will be based on ‘useroid’ in AVG.

   The NDIC login screen is displayed with disabled pre-filled user name.
6. Enter the password in the NDIC login screen.
7. Click **Connect**.

Signing CSRs

This feature is primarily used when you have configured the virtual SSL server to perform end to end encryption, and you want to sign a CSR (Certificate Signing Request) generated on a backend web server by using a CA certificate on the VPN Gateway.

1. Specify the CA certificate that you want to use for signing the CSR.

```
>> Main#cfg/cert 1

>> Certificate 1#sign
```

2. Paste the CSR.

   Open the CSR file in a text editor and copy the entire contents, including the text "-----BEGIN CERTIFICATE REQUEST-----" and "-----END CERTIFICATE

REQUEST-----". Having pasted the CSR, press ENTER to create a new line and type three periods (...). Finally press ENTER once again.

```
Paste the certificate request, press Enter to create a new line,
and then type "..."(without the quotation marks) to terminate.
> -----BEGIN CERTIFICATE REQUEST-----
> MIIBwzCCASwCAQAwgYIxCzAJBgNVBAYTAlNFMRAwDgYDVQQIEwdTdmVyaWdlMREw
> DmK//G/x4A0rSiWgosNldZKJTPWhgYqkgYcwgYQxCzAJBgNVBAYTAlNFMRAwDgYD
> W26ntiCyRgmaYjMCOV/n95qx3h57og0=
> -----END CERTIFICATE REQUEST-----
> ...
Valid for days [365]: <press ENTER to accept>
Serial number of signed certificate [1]: <press ENTER to accept>
Save signed certificate (yes/no) [yes]: <press ENTER to accept>
Select cert no. to save to [3]: <press ENTER to accept>
Created /cfg/cert 3
Use 'apply' to save signed key and certificate.
-----BEGIN CERTIFICATE-----
MIID4zCCA0ygAwIBAgIBAjANBgkqhkiG9w0BAQQFADCBhDELMAkGA1UEBhMCU0Ux
DmK//G/x4A0rSiWgosNldZKJTPWhgYqkgYcwgYQxCzAJBgNVBAYTAlNFMRAwDgYD
fT00vSLpvNHB199q1YV9+rJJz1ZIAT+bqiIvHNAOph0spPoZDUHc
-----END CERTIFICATE-----
Use 'apply' to save incremented certificate serial number.
```

3. Apply the changes.

   In the preceding example, the newly signed certificate is saved as certificate number 3. Use the **`export`** command to export the signed certificate to a file. The signed CSR can then be installed on the backend web server as a server certificate.

4. Specify the certificate you used for signing the CSR is specified as a CA certificate on the virtual SSL server.

```
>> Main#cfg/ssl/server #/adv/sslconnect/verify/cacerts

Current value:""

Enter certificate numbers (separated by comma):1
```

5. Apply the changes.

   The CSR is signed using the private key associated with the currently selected certificate.

Generate Test Certificate

If needed, you can generate a self-signed certificate and private key for testing purposes. After providing the requested information, the certificate and key are generated immediately.

1. Specify an unused certificate number.

Comments? infodev@avaya.com

If a certificate and key already exist for the current certificate index number, they are overwritten when you execute the **apply** command. You should therefore always choose an unused certificate index number before creating a test certificate.

```
>> Main#cfg/cert 4

Creating Certificate 4
>> Certificate 4#test
```

2. Provide the requested information.

   For a more detailed explanation of the requested information, see Generating and Submitting a CSR Using the CLI on page 81.

```
The combined length of the following parameters may not exceed 225
bytes.
Country Name (2 letter code):
State or Province Name (full name):
Locality Name (eg, city):
Organization Name (eg, company):
Organizational Unit Name (eg, section):
Common Name (eg, your name or your server's hostname):
Email Address:
Subject alternative name (blank or comma separated list of
URI:<uri>, DNS:<fqdn>, IP:<ip-address>, email:<email-address>):
Valid for days [365]:
Key size (512/1024/2048/4096) [1024]:
Test key and certificate added.
Use 'apply' to activate.
```

3. Apply the changes.

   The test certificate is now ready to be mapped to an SSL server.

   If the AVG software is used for SSL acceleration purposes, the certificate should be mapped to the virtual SSL server, using the **/cfg/ssl/server #/ssl/cert** command.

   If the AVG software is used for deployment of a VPN solution, the certificate should be mapped to the portal server of the desired VPN, using the **/cfg/vpn #/server/ssl /cert** command.

General Commands

This section includes examples on how to use some general Certificate menu commands.

Show Certificate Information

The **info** command is used to show brief information about the selected certificate.

```
>> Certificate 1#info

Serial number:   0 (0x0)
Expire:   Nov 29 12:42:17 2006 GMT
Certificate subject:
C=US
ST=Texas
L=Dallas
O=Avaya
OU=Switching
CN=John/emailAddress=john@avaya.com
```

Show Subject Information

The **subject** command is used to view the subject information adhering to the selected certificate. Parts of a client certificate's subject information can be used extract to user name and password. For usage examples, see the "Client Certificate Authentication" section in the "Authentication Methods" chapter in the *Avaya CLI/BBI Application Guide for VPN*.

```
>> Certificate 1#subject

Certificate subject:
C/countryName (2.5.4.6)                      = US
ST/stateOrProvinceName (2.5.4.8)               = Texas
L/localityName (2.5.4.7)                     = Dallas
O/organizationName (2.5.4.10)              = Avaya
OU/organizationalUnitName (2.5.4.11)       = Switching
CN/commonName (2.5.4.3)                      = John
emailAddress/emailAddress (1.2.840.113549.1.9.1) = john@avaya.com
```

Check if Key and Certificate Match

To check if the private key matches the public key in the selected certificate, use the following command:

```
>> Certificate 1#validate

Validate: key and certificate match.
```


Comments? infodev@avaya.com

Show Key Size

This command is used to show the size of the private key in the selected certificate:

```
>> Certificate 1#keysize

Key is of size 1024.
```

Show Key Information

This command provides information about how the private key associated to the currently selected certificate is protected.

For the VPN Gateways without the HSM card, private keys are protected by the cluster.

For the ASA FIPS, private keys are protected by the HSM card. However, when generating a client certificate, the associated private key is protected by the cluster and not by the HSM card. This is necessary to transfer both the certificate and the private key to the client using the **`export`** command.

```
>> Certificate 1#keyinfo

The key is protected by the iSD Cluster.
```

Comments? infodev@avaya.com

Chapter 9: Virtual Desktop

Symantec On-Demand Agent (SODA) provides a Virtual Desktop environment to secure Web-based applications and services. Therefore, you can access confidential information in a secure environment.

Running the Virtual Desktop on Client Computers

The Virtual Desktop runs on computers meeting the following specifications:

- Pentium 633MHz or faster
- 128 MB RAM
- 25 MB MINIMUM available hard disk space required for Agent to download

Note:

More space may be required for your system to run smoothly after Agent is downloaded, because user data files must be virtualized for successful launch of certain applications.

- Windows Server 2003, Windows 2000 Pro, Windows 2000 Server, Windows XP, Windows NT4 (SP6).
- Browser: Internet Explorer 5.0 or later, Netscape 6.0 or later, Opera 7.2 or later, FireFox 1.0 and later.
- Java Runtime Environment (JRE) version 1.4.2 or later, or Microsoft Java Virtual Machine (JVM) version 5.0 and later.

Licensing vdesktop

Your copy of Symantec On-Demand Manager is licensed with vdesktop. Following software bundles with vdesktop are available:

- Symantec™ On-Demand - Security Edition
- Symantec™ On-Demand - Protection Solution

To activate the virtual desktop feature, you need to paste the license key for the same.

1. Logon as `admin`.
2. Click on **Config** tab.
3. In the system tree view, select **Host(s)**.
4. Click on **SSL VPN Host name**.

System Information screen is displayed.

5. Click on **Licenses** tab.
6. Paste the contents of the license.
7. Click **Save**.

Launch Vdesktop from Portal

Follow these steps to launch virtual desktop from portal:

1. Open the internet explorer.
2. Enter the Protocol, IP address, and Port.

   For example: http://10.127.232.45:1234
3. Enter the user name and password.
4. Click on **Home**.
5. Click on the virtual desktop link.



6. Click on the virtual desktop link.

   The virtual desktop is launched.

Virtual Desktop Operations

Once the vdesktop license is installed, you can perform the following tasks:

- Print and copy information to removable USB media.
- Work only within the Virtual Desktop (Enable Automatic Switch).
- Work with copies of the files rather than the ‘real’ versions (Enable File Separation).

The vdesktop session may get terminated when the browser session is terminated to ensure that the Virtual Desktop session does not remain active indefinitely on halted or shared machines.

Note:

If you want to enable or disable some of the options in this, contact your system administrator.

Comments? infodev@avaya.com

Chapter 10: The Command Line Interface

This chapter explains how to access the Avaya VPN Gateway (AVG) through the command line interface (CLI).

The AVG software provides means for accessing, configuring, and viewing information and statistics about the AVG configuration. By using the built-in, text-based command line interface and menu system, you can access and configure the VPN Gateway or cluster either through a local console connection (using a computer running terminal emulation software), or through a remote session using either a Telnet client or an SSH client.

When using a Telnet client or SSH client to connect to a cluster of VPN Gateways, always connect to the IP address of the MIP (Management IP). Configuration changes are automatically propagated to all members of the cluster. However, when using the **`halt`**, **`reboot`**, or **`delete`** commands (available in the Boot menu), you should connect to the IP address of the particular VPN Gateway on which you want to perform these commands, or connect to that VPN Gateway through a console connection.

Connecting to the VPN Gateway

You can access the command line interface in two ways:

- Using a console connection through the console port
- Using a Telnet connection or SSH connection over the network.

Establishing a Console Connection

A console connection is required when performing the initial setup, and when reinstalling the AVG software as the boot user. When logging in as root user for advanced troubleshooting purposes, a console connection is also required.

Requirements

To establish a console connection with the VPN Gateway, you will need the following:

- An ASCII terminal or a computer running terminal emulation software set to the parameters shown in the following table:

Table 3: Console Configuration Parameters

Parameter	Value
Baud Rate	9600
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

- A serial cable with a female DB-9 connector. (For more specific information, see the "Connecting to the VPN Gateway " chapter in the *Hardware Installation Guide*.)

Procedure

1. Connect the terminal to the Console port using the correct serial cable.

   When connecting to a VPN Gateway, use a serial cable with a female DB-9 connector (shipped with the VPN Gateway).
2. Power on the terminal.
3. To establish the connection, press ENTER on your terminal.

   You will next be required to log in by entering a user name and a password. For more information about user accounts and default passwords, see Accessing the AVG Cluster on page 122.

Establishing a Telnet Connection

A Telnet connection offers the convenience of accessing the AVG cluster from any workstation connected to the network. Telnet access provides the same options for user access and administrator access as those available through the console port.

To configure the AVG cluster for Telnet access, you need to have a device with Telnet client software located on the same network as the VPN Gateway(s). The VPN Gateway must have an IP address and a Management IP address. If you have already performed the initial setup by selecting **new** or **join** in the Setup menu, the assignment of IP addresses is complete.

When making configuration changes to a cluster of AVGs through Telnet, it is recommended that you connect to the IP address of the MIP. However, if you want to halt or reboot a particular VPN Gateway in a cluster, or reset all configuration to the factory default settings, you must connect to the IP address of the particular VPN Gateway. This also applies when using an SSH connection instead of a Telnet connection. To view the IP addresses of all VPN Gateways in a cluster, use the **`/info/isdlist`** command.

Enabling and Restricting Telnet Access

Telnet access to the AVG cluster is disabled by default, for security reasons. However, depending on the severity of your security policy, you may want to enable Telnet access. You may also restrict Telnet access to one or more specific machines.

For more information about how to enable Telnet access, see the **`telnet`** command in the "Administrative Applications Configuration" section under Configuration Menu>System Configuration in the *Avaya Command Reference*. For more information about how to restrict Telnet access to one or more specific machines, see the **add** command in the "System Access Configuration " section in the same chapter.

Running Telnet

Once the IP parameters on the VPN Gateway are configured and Telnet access is enabled, you can access the CLI using a Telnet connection. To establish a Telnet connection with the VPN Gateway, run the Telnet program on your workstation and issue the Telnet command, followed by the VPN Gateway 's IP address.

```
telnet <IP address>
```

You will then be prompted to enter a valid user name and password. For more information about different user accounts and default passwords, see Accessing the AVG Cluster on page 122.

Establishing a Connection Using SSH (Secure Shell)

When accessing the VPN Gateway from a workstation connected to the network using a Telnet connection, it is important to keep in mind that the communication channel is not secure. All data flowing back and forth between the Telnet client and the VPN Gateway is sent unencrypted (including the password), and there is no server host authentication.

By using an SSH client to establish a connection over the network, the following benefits are achieved:

- Server host authentication
- Encryption of passwords for user authentication
- Encryption of all traffic that is transmitted over the network when configuring or collecting information from the VPN Gateway

Enabling and Restricting SSH Access

SSH access to the VPN Gateway is disabled by default. However, depending on the severity of your security policy, you may want to enable SSH access. You may also restrict SSH access to one or more specific machines.

For more information about how to enable SSH access, see the **ssh** command in the "Administrative Applications Configuration " section under Configuration Menu>System Configuration in the *Command Reference*. For more information about how to restrict SSH access to one or more specific machines, see the add command in the "System Access Configuration " section in the same chapter.

Running an SSH Client

Connecting to the VPN Gateway using a SSH client is similar to connecting through Telnet. As with Telnet, the IP parameters on the VPN Gateway need to be configured in advance and SSH access must be enabled. After providing a valid user name and password, the command line interface in the VPN Gateway is accessible the same way as when using a Telnet client. However, because a secured and encrypted communication channel is set up even before the user name and password is transmitted, all traffic sent over the network while configuring or collecting information from the VPN Gateway is encrypted. For information about different user accounts and default passwords, see Accessing the AVG Cluster on page 122.

During the initial setup of the VPN Gateway(s), you are provided with the choice to generate new SSH host keys. It is recommended that you do so, to maintain a high level of security when connecting to the VPN Gateway using a SSH client. If you fear that your SSH host keys have been compromised, you can create new host keys at any time by using the **/cfg/sys/adm/sshkeys/generate** command. When reconnecting to the VPN Gateway after having generated new host keys, your SSH client will display a warning that the host identification (or host keys) has been changed.

Accessing the AVG Cluster

To enable better AVG management and user accountability, five categories of users can access the AVG cluster:

- Operator is only granted read access to the menus and information appropriate to this user access level. The Operator cannot make any changes to the configuration.
- Administrator can make any changes to the AVG configuration. Thus, the Administrator has read and write access to all menus, information and configuration commands in the AVG software.
- A Certificate Administrator is a member of the certadmin group, and has sufficient user rights to manage certificates and private keys. By default, only the Administrator user is

Comments? infodev@avaya.com

a member of the certadmin group. To separate the Certificate Administrator user role from the Administrator user role, the Administrator user can add a new user account to the system, assign the new user to the certadmin group, and then remove himself or herself from the certadmin group. For more information, see Adding a New User on page 69.

- Boot user can only perform a reinstallation. For security reasons, it is only possible to log in as the Boot user through the console port using terminal emulation software. The Boot user password cannot be changed from the default ForgetMe.
- Root user is granted full access to the underlying Linux operating system. For security reasons, it is only possible to log in as the Root user through the console port using terminal emulation software. Root user access should mainly be reserved for advanced troubleshooting purposes, under guidance from Avaya customer support.

  For more information, see Customer service on page 11.

Access to the AVG command line interface and settings is controlled through the use of four predefined user accounts and passwords. Once you are connected to the VPN Gateway through a console connection or remote connection (Telnet or SSH), you are prompted to enter a user account name and the corresponding password. The default user accounts and passwords for each access level are listed in Table 4: User Access Levels on page 123.

Note:

The default Administrator user password can be changed during the initial configuration. For the Operator user, the Boot user, and the Root user however, the default passwords are used even after the initial configuration. It is therefore recommended that you change the default AVG passwords soon after the initial configuration, and as regularly as required under your network security policies.

For more information about how to change a user account password, see Changing a Users Password on page 75.

Table 4: User Access Levels

User Account	User Group	Access Level Description	Default Password
oper	oper	The Operator is allowed read access to some of the menus and information available in the CLI.	`oper`
admin	admin oper certadmin	The Administrator is allowed both read and write access to all menus, information and configuration commands. The Administrator can add users to all groups in which the Administrator himself or herself is a member. The Administrator can delete a user from any of the three built-in groups.	`admin`
	certadmin	By default, only the Administrator is a member of the certadmin group. Certadmin group rights are sufficient for administrating certificates and keys on the VPN Gateway. A certificate administrator user has no access to the SSL Server menu, and only limited access to the System menu.	

User Account	User Group	Access Level Description	Default Password
boot		The boot user can only perform a reinstallation of the software, and only through a console connection.	`ForgetMe`
root		The root user has full access to the underlying Linux operating system, but only through a console connection.	`ForgetMe`

CLI vs. Setup

Once the Administrator user password is verified, you are given complete access to the VPN Gateway. If the VPN Gateway is still set to its factory default configuration, the system will run Setup (see Installing an AVG in a New Cluster on page 36), a utility designed to help you through the first-time configuration process. If the VPN Gateway has already been configured, the Main menu of the CLI is displayed instead.

The following figure shows the Main menu with administrator privileges.

```
[Main Menu]
      info       - Information menu
      stats      - Statistics menu
      cfg        - Configuration menu
      boot       - Boot menu
      maint      - Maintenance menu
      diff       - Show pending config changes   [global command]
      apply      - Apply pending config changes  [global command]
      revert     - Revert pending config changes [global command]
      paste      - Restore saved config with key [global command]
      help       - Show command help             [global command]
      exit       - Exit  [global command, always available]
```

Command Line History and Editing

For a description of global commands, shortcuts, and command line editing functions, see the *Command Reference*.

Idle Timeout

The VPN Gateway will disconnect your local console connection or remote connection (Telnet or SSH) after 10 minutes of inactivity. This value can be changed to a maximum value of 1 hour using the **`/cfg/sys/adm/clitimeout`** command.

Comments? infodev@avaya.com

If you have unapplied configuration changes when automatically disconnected after the specified idle timeout value, the unapplied configuration changes will be lost. Therefore, make sure to save your configuration changes regularly by using the global **`apply`** command.

If you have unapplied configuration changes when using the global **`exit`** command to log out from the command line interface, you will be prompted to view the pending configuration changes by using the global **`diff`** command. After verifying the pending configuration changes, you can either remove the changes or apply them. For more information about pending configuration changes, see the "Viewing, Applying and Removing Changes " section under Configuration Menu in the *Command Reference*.

Comments? infodev@avaya.com

Chapter 11: Troubleshooting the AVG

This chapter provides troubleshooting tips for the following problems:

- Cannot connect to the Avaya VPN Gateway (AVG) through Telnet or SSH, on Cannot Connect to VPN Gateway through Telnet or SSH on page 127.
- Cannot add the VPN Gateway to an existing cluster, on Cannot Add an AVG to a Cluster on page 130.
- Cannot contact the Management IP Address (MIP) on Cannot Contact the MIP on page 130.
- The VPN Gateway stops responding, on The AVG Stops Responding on page 131.
- A user password is lost, on .
- An ASA 310-FIPS does not process any SSL traffic, on A User Password is Lost on page 132.
- Resetting the HSM cards on the ASA 310-FIPS, on An ASA 310-FIPS Stops Processing Traffic on page 133.
- An AVG cluster configuration needs to be reconstructed onto new devices, on An ASA 310-FIPS Cluster Must be Reconstructed onto New Devices on page 137.
- User fails to connect to the VPN, on A User Fails to Connect to the VPN on page 141.
- User unable to connect to the VPN Gateway through the Net Direct client, on User Unable to Connect to the VPN Gateway through the Net Direct Client on page 146.
- Unable to download Net Direct from VPN server.
- Cannot download the Net Direct Zipped file from client PC.

The chapter also provides a section on performing system diagnostics, on System Diagnostics on page 148.

Cannot Connect to VPN Gateway through Telnet or SSH

Note:

The Disable new IPSec logins feature may have been enacted to allow maintenance of the gateway. Contact your system administrator to determine the status of this feature.

Verify the Current Configuration

Connect through a console connection and check that Telnet or SSH access to the VPN Gateway is enabled. By default, remote connections to the AVG are disabled for security

reasons. Type the command `/cfg/sys/adm/cur` to see whether remote access through Telnet or SSH is enabled.

```
>> #/cfg/sys/adm/cur

 Collecting data, please wait...
Administrative Applications:
CLI idle timeout = 1h
Telnet CLI access = off
SSH CLI access = off
```

Enable Telnet or SSH Access

If your security policy affords enabling remote connections to the VPN Gateway, type the command `/cfg/sys/adm/telnet` to enable Telnet access, or the command `/cfg/sys/adm/ssh` to enable SSH access. Apply your configuration changes.

```
>> #/cfg/sys/adm/ssh

Current value: off
Allow SSH CLI access (on/off):on

>> Administrative Applications#apply

Changes applied successfully.
```

Check the Access List

If you find that Telnet or SSH access is enabled but you still can't connect to the VPN Gateway using a Telnet or SSH client, check whether any hosts have been added to the Access List. Type the command `/cfg/sys/accesslist/list` to view the current Access List.

```
>> #/cfg/sys/accesslist/list

1: 192.168.128.78, 255.255.255.0
```

When Telnet or SSH access is enabled, only those hosts listed in the Access List are allowed to access the VPN Gateway over the network. If no hosts have been added to the Access List, this means that any host is allowed to access the VPN Gateway over the network (assuming that Telnet or SSH access is enabled).

Check the IP Address Configuration

If your host is allowed to access the VPN Gateway over the network according to the Access List, check that you have configured the correct IP addresses on the VPN Gateway. Make sure you ping the host IP address of the VPN Gateway, and not the Management IP (MIP) of the cluster in which the VPN Gateway is a member. Type the command `/cfg/cur sys` to view IP address information for all VPN Gateways in the cluster.

```
>> # /cfg/cur sys
System:
  Management IP (MIP) address = 192.168.128.211

    iSD Host 1:
      Type of the iSD = master
      IP address = 10.1.82.145
      License =
        IPSEC user sessions: 10
        TPS: unlimited
        SSL user sessions: 10
      Default gateway address = 10.1.82.2
      Ports = 1 : 2
      Hardware platform = 200

        Host Routes:
          No items configured

        Host Interface 1:
          IP address = 192.168.128.210
          Network mask = 255.255.255.0
          VLAN tag id = 0
          Mode = failover
          Primary port = 0

            Interface Ports:
               1

        Host Port 1:
```

If the IP address assigned to the VPN Gateway seems to be correct, you may have a routing problem. Try to run **`traceroute`** (a global command available at any menu prompt) or the **`tcpdump`** command (or some other network analysis tool) to locate the problem. For more information about the **`tcpdump`** command, see the *"Network Traffic Dump Commands"* section under *Configuration Menu>SSL Configuration Menu* in the *Avaya Command Reference*.

If this does not help you to solve the problem, contact Avaya for technical support. See Customer service on page 11.

Cannot Add an AVG to a Cluster

When trying to add a VPN Gateway to a cluster by selecting

```
join
```

in the Setup menu, you may receive an error message stating that the system is running an incompatible software version. The incompatible software version referred to in the error message is the software that is running on the AVG device you are trying to add to the cluster. This error message is displayed whenever the AVG you are trying to add has a different software version from the AVG(s) already in the cluster. In this situation you need to do one of the following:

- Adjust the software version on the AVG device you are trying to add to the cluster, to synchronize it with the software version running on the AVG(s) already in the cluster. You can verify software versions by typing the command **`/boot/software/cur`**, where the active version is indicated as

  ```
  permanent
  ```

  . Adjusting the software version on the AVG device you want to add to the cluster implies either upgrading to a newer software version, or reverting to an older software version. In either case you will need to perform the steps described in Reinstalling the Software on page 60. After having adjusted the software version, log in as the Administrator user and select **`join`** from the Setup menu.
- Upgrade the software version running on the AVG(s) in the cluster to the same version as running on the VPN Gateway you want to add to the cluster. Perform the steps described in Performing Minor/Major Release Upgrades on page 63. Then add the AVG device by selecting **`join`** from the Setup menu.

Cannot Contact the MIP

When trying to add a VPN Gateway to a cluster by selecting **join** in the Setup menu, you may receive an error message stating that the system is unable to contact the Management IP address (MIP).

This could be the case if you are trying to join a VPN Gateway to a cluster and there are existing entries in the Access list. Typically, the Access list contains valid IP addresses for Telnet or SSH management. If the Access list contains entries, you have to add the Interface 1 IP addresses of both VPN Gateways and the Management IP address (MIP) to the Access list before joining the VPN Gateway.

If the Access list is empty, communication should be working fine.

Comments? infodev@avaya.com

Check the Access List

On the master VPN Gateway, check if there are entries in the Access list. Type the command `/cfg/sys/accesslist/list` to view the current Access list.

```
>> #/cfg/sys/accesslist/list

1: 192.168.128.78, 255.255.255.0
```

Add Interface 1 IP Addresses and MIP to Access List

Use the **`/cfg/sys/cluster/cur`** command to view the Host Interface 1 IP address for the existing VPN Gateway. Then add this IP address, the intranet IP address you had in mind for the new VPN Gateway and the Management IP address (MIP) to the Access list.

To add the IP addresses to the Access list, type the command `/cfg/sys/accesslist/add`.

```
>> #/cfg/sys/accesslist/add

Enter network address:<IP address>

Enter netmask:<network mask>
```

Try adding the VPN Gateway to the cluster using the **`join`** command in the Setup menu.

If a software version earlier than 2.0.11.16 is running in the cluster, and software version 3.1 or later is installed on the VPN Gateway you want to join, perform the steps described in Reinstalling the Software on page 60. If there is still a difference in software version after this, you need to adjust the software version on the VPN Gateway you want to add as well. After having upgraded the software version in the cluster, log in to the VPN Gateway you want to add as the Administrator user and select **join** from the Setup menu.

The AVG Stops Responding

Telnet or SSH Connection to the Management IP Address

When you are connected to a cluster of VPN Gateways through a Telnet or SSH connection to the Management IP address, your connection to the cluster can be maintained as long as

at least one master VPN Gateway in the cluster is up and running. However, if the particular VPN Gateway that currently is in control of the Management IP stops responding while you are connected, you need to close down your Telnet or SSH connection and reconnect to the Management IP address.

After doing so, you can view the operational status of all VPN Gateways in the cluster by typing the command **`/info/isdlist`**. If you find that one of the AVG's operational status is indicated as, you should reboot that machine. On the VPN Gateway, press the Power button on the back panel to turn the machine off, wait until the fan comes to a standstill, and then press the Power button again to turn the machine on.

Log in as the Administrator user when the login prompt appears and check the operational status again.

Console Connection

If you are connected to a particular VPN Gateway through a console connection, and that AVG stops responding, you should first try pressing the key combination CTRL+ ^ and press ENTER. This will take you back to the login prompt. Log in as the Administrator user and check the operational status of the VPN Gateway. Type the command **`/info/isdlist`** and see if the operational status is indicated as up. If the operational status is indicated as up, the VPN Gateway should continue to process SSL traffic without the need of a reboot.

If the operational status of the VPN Gateway is indicated as down, try rebooting the device by typing the command **`/boot/reboot`**. You will be asked to confirm your action before the actual reboot is performed. Log in as the Administrator user and check if the operational status of the VPN Gateway is now up.

If the operational status of the VPN Gateway still is down, reboot the machine. On the device, press the Power button on the back panel to turn the machine off, wait until the fan comes to a standstill, and then press the Power button again to turn the machine on. Log in as the Administrator user when the login prompt appears.

A User Password is Lost

Administrator User Password

If you have lost the Administrator user password there is only one way to regain access to the VPN Gateway as the Administrator user: reinstalling the software through a console connection as the Boot user.

For more information, see Reinstalling the Software on page 60.

Comments? infodev@avaya.com

Operator User Password

If you have lost the Operator user password, log in as the Administrator user and define a new Operator user password. Only the Administrator user can change the Operator user password.

For more information, see the **`edit`** command in the "User Access Configuration " section under Configuration Menu>System Configuration in the *Command Reference*.

Root User Password

If you have lost the Root user password, log in as the Administrator user and define a new Root user password. Only the Administrator user can change the Root user password. For more information, see the **`edit`** command in the "User Access Configuration " section under Configuration Menu>System Configuration in the *Command Reference*.

Boot User Password

The default Boot user password cannot be changed, and can therefore never really be "lost". If you have forgotten the Boot user password, see Accessing the AVG Cluster on page 122.

If the Boot user password could be changed and you have lost both the Administrator password and the Boot user password, the VPN Gateway be rendered completely inaccessible to all users except the Operator, whose access level does not permit any changes being made to the configuration of the AVG.

The fact that the Boot user password cannot be changed should not imply a security issue, because the Boot user can only access the VPN Gateway through a console connection using a serial cable, and the VPN Gateway presumably is set up in a server room with restricted access.

An ASA 310-FIPS Stops Processing Traffic

Whenever an ASA 310-FIPS has undergone a reboot (whether intentionally invoked by the user, or due to a power failure), the device stops processing SSL traffic. This behavior is perfectly normal, and is due to the high security demands placed on the ASA 310-FIPS.

To make an ASA 310-FIPS start processing SSL traffic again, log in to the HSM cards using the HSM-USER iKey associated to each card. Logging in to the HSM cards will clear the alarms that were set during the reboot, and the ASA 310-FIPS will accept SSL traffic again.

Follow these steps to log in to the HSM cards:

1. Log in to the specific ASA 310-FIPS that has undergone a reboot as the admin or oper user.

```
login:admin

Password:<enter the admin user password>

Alteon iSD SSL
Software version 8.0
```

   When connecting to the ASA 310-FIPS, you can use a console connection, or a remote connection (Telnet or SSH, if enabled in the system configuration).

   Note:

   It is important that you log in to the particular ASA 310-FIPS on which a reboot has occurred, and not to the Management IP address (MIP) of the cluster.

2. Log in to each HSM card consecutively by inserting the correct HSM-USER iKey and providing the associated password.

   Remember that each HSM card requires inserting the specific HSM-USER iKey that was used when initializing that particular HSM card. This holds true even if you use the same password for both HSM-USER iKeys.

```
>> Main#maint/hsm/login

Verify that HSM-USER iKey (blue) is inserted in card 0 (with
flashing LED).
Hit enter when done.
Enter the current HSM-USER password for card 0:<enter the
password associated with the HSM-USER iKey for card 0>

Successful login on card 0.
Verify that HSM-USER iKey (blue) is inserted in card 1 (with
flashing LED).
Hit enter when done.
Enter the current HSM-USER password for card 1:<enter the
password associated with the HSM-USER iKey for card 1>

Successful login on card 1

.
```

   Note:

   If you enter the wrong password for the HSM-USER fifteen (15) times in a row, the HSM-USER iKey will be rendered unusable. This is due to the strict security specifications placed on the ASA 310-FIPS.

3. Verify that the alarms that caused the ASA 310-FIPS to stop processing SSL traffic have been cleared.

```
>> #/info/events/alarms

** (alarm) Active Alarm List
************************************
```

The hsm_not_logged_in alarms that were triggered during the reboot should now be cleared from the active alarm list, after the successful login to both HSM cards. The ASA 310-FIPS is now ready to process SSL traffic again.

Resetting HSM Cards on the ASA 310-FIPS

When removing an ASA 310-FIPS device from a cluster, you have the option to reset (or de-initialize) the HSM cards.

When an ASA 310-FIPS device that has been removed from a cluster is installed in a new cluster, or added to an existing cluster, the cards will be initialized again. This is done by performing a series of steps as part of the setup procedure of the ASA 310-FIPS device itself. If the Setup utility detects that the cards have not been reset, you will be prompted to reset the HSM cards at that time. The HSM cards must be reset before they can be initialized. You may therefore choose to reset the cards already when removing the ASA 310-FIPS device from the cluster. Resetting the HSM cards will clear all sensitive cryptographic information stored on the cards. Until the cards are initialized again, they will remain in that state.

To reset the HSM cards, you need the following:

- The two pairs of HSM-SO and HSM-USER iKeys, where each pair is associated with a particular HSM card on the ASA 310-FIPS device you want to delete from the cluster
- The HSM-SO password associated with each HSM-SO iKey
- Log in as the admin user to the particular ASA 310-FIPS device you want to delete

If the ASA 310-FIPS device will be used in a different department or organization after it has been deleted from the cluster, you may want to change the current password for the HSM-SO iKey and the HSM-USER iKey before you reset the HSM cards. The user who performs the initial setup of the ASA 310-FIPS device must then provide the "transient" passwords known by both parties when initializing the HSM cards, but can directly change to new HSM-SO and HSM-USER passwords within the normal initialization procedure.

To change the current password for the HSM-SO iKey before resetting the HSM cards, use the **`/maint/hsm/changepass`** command. For more information about this command, see the "HSM Menu " section under Maintenance Menu in the *Command Reference*.

Note:

When moving the ASA 310-FIPS device to a different location, make sure to maintain the connection between each pair of HSM-SO and HSM-USER iKeys and the particular HSM card to which they are associated. To initialize the HSM cards when installing or adding the device in a cluster, the correct HSM-SO and HSM-USER iKeys are required, as well as the corresponding HSM-SO and HSM-USER passwords.

1. Log in to the ASA 310-FIPS ASA 310-FIPS that you want to delete from the cluster.

   In this step it is important that you connect to the particular ASA 310-FIPS ASA 310-FIPS that you want to delete from the cluster. To do that, you can use either a console connection, or a remote connection (through Telnet or SSH) using the IP address assigned to the specific ASA 310-FIPS ASA 310-FIPS device. Do not connect through a remote connection using the Management IP (MIP) address of the ASA cluster. To view the IP addresses assigned to each ASA 310-FIPS device in the cluster, use the **`/info/isdlist`** command.

   ```
   login:admin

   Password:<enter the admin user password>

   Alteon iSD SSL
   Software version 8.0
   ```

2. Delete the ASA 310-FIPS ASA 310-FIPS (iSD) and choose to reset the HSM cards.

   ```
   >> Main#/boot/delete

   Are you sure you want delete the iSD? (y/n)y

   Do you want to clear the HSM card(s) as well? (y/n) [y]:
   ```

   (press ENTER to accept resetting the HSM cards)

3. Insert the HSM-SO iKey associated with HSM card 0 in the card with flashing LED and provide the correct password.

   Remember that each HSM card requires inserting the specific HSM-SO iKey that was used when initializing that particular HSM card. This holds true even if you use the same password for both HSM-SO iKeys that are used on one ASA 310-FIPS device.

   (continued)

   ```
   Verify that HSM-SO iKey (purple) is inserted in card 0 (with
   flashing LED).
   Hit enter when done.
   Enter the current HSM-SO password for card 0:
   ```

4. Insert the HSM-SO iKey associated with HSM card 1 in the card with flashing LED and provide the correct password.

   Again, make sure that you insert the correct HSM-SO iKey, as each HSM card requires the specific iKey that was used when the card was first initialized.

   (continued)

Comments? infodev@avaya.com

```
Verify that HSM-SO iKey (purple) is inserted in card 1 (with
flashing LED).
Hit enter when done.
Enter the current HSM-SO password for card 1:


iSD 192.168.128.185 deleted. Logging out.
```

The ASA 310-FIPS device is now removed from the cluster and reset to its factory default settings. Both HSM cards are also reset, which means that all sensitive cryptographic information stored on the cards is deleted. The next time a user turns on the ASA 310-FIPS device, the Setup menu will be displayed after having logged in as the admin user through a console connection.

When selecting `new` or `join` in the Setup menu, you will be prompted to insert the HSM-SO iKey and HSM-USER iKey associated with each HSM card, and provide the current password stored on the respective iKey. This is required to initialize the HSM card anew. After you have provided the correct password for the iKey being requested by the Setup utility, a new passwords can be defined for that iKey.

For more information about installing and adding ASA 310-FIPS device in a cluster, see Installing an ASA 310-FIPS on page 50.

An ASA 310-FIPS Cluster Must be Reconstructed onto New Devices

If your cluster of ASA 310-FIPS devices has been damaged beyond repair (by fire, for example) you can reconstruct the complete cluster, including certificates, private keys, and wrap keys. However, this requires that you have access to the following:

- A new set of ASA 310-FIPS devices, replacing the cluster of damaged devices.
- A backup configuration file, saved to an FTP/TFTP/SCP/SFTP server as a precautionary measure by using the **`/cfg/ptcfg`** command in the former cluster. For more information about the **`ptcfg`** command, see the "Configuration Menu " chapter in the *Command Reference*.
- The black CODE-SO and CODE-USER iKeys that were used when the now damaged cluster of ASA 310-FIPS devices was first created. The black CODE iKeys are needed to transfer the wrap key used in the former cluster onto the HSM cards in the new ASA 310-FIPS devices, as well as for decrypting private key information in the backup configuration file.
- The secret passphrase that was defined in the former cluster when first initialized (Provided your former cluster was running in FIPS mode).

To reconstruct the cluster configuration, certificates, private keys, and wrap keys used in the former cluster onto a new set of ASA 310-FIPS ASA 310-FIPS devices, follow these steps:

1. Install the first ASA 310-FIPS in a new cluster by following the instructions on Installing an ASA 310-FIPS on page 50 up to and including step 5 on page 138.

   Note:

   When asked to use FIPS or Extended Security Mode, select the same mode that was used in the former cluster.

2. When both HSM cards have been initialized, you will be asked if you want to use new or existing HSM-CODE iKeys. Type `existing` and press ENTER.

```
(new setup, continued)

Card 1 successfully initialized.
Should new or existing CODE iKeys be used? (new/existing)
[new]:existing
```

3. Transfer the cluster wrap key from the existing CODE-SO and CODE-USER iKeys to card 0.

   Make sure you use the same pair of CODE-SO and CODE-USER iKeys that were used in the former cluster of ASA 310-FIPS devices.

```
(new setup, continued)

Verify that CODE-SO iKey (black) is inserted in card 0 (with
flashing LED).
Hit enter when done.
Verify that HSM-USER iKey (blue) is inserted in card 0 (with
flashing LED).
Hit enter when done.
Verify that CODE-USER iKey (black) is inserted in card 0 (with
flashing LED).
Hit enter when done.
Wrap key successfully combined to card 0.
```

4. Transfer the cluster wrap key from the CODE-SO and CODE-USER iKeys to card 1.

```
(new setup, continued)

Verify that CODE-SO iKey (black) is inserted in card 1 (with
flashing LED).
Hit enter when done.
Verify that HSM-USER iKey (blue) is inserted in card 1 (with
flashing LED).
Hit enter when done.
Verify that CODE-USER iKey (black) is inserted in card 1 (with
flashing LED).
Hit enter when done.
Wrap key successfully split combined to card 1.
```

5. If you selected FIPS mode as the security mode, specify the passphrase.

   Enter the same secret passphrase as was defined in the former cluster running in FIPS mode. This step only appears if you selected FIPS mode when initializing the HSM cards.

```
(new setup, continued)

Enter the old secret passphrase (it is used during addition of
new iSDs to the cluster):<Enter the same secret passphrase as was
used in the former cluster.>

Re-enter to confirm:
```

6. Wait for the initial setup of the first ASA 310-FIPS in the cluster to finish.

```
(new setup, continued)

Initializing system......ok
Setup successful. Relogin to configure.


login:
```

7. Add an additional ASA 310-FIPS to the newly created cluster by following the instructions on pageAdding an ASA 310-FIPS to an Existing Cluster on page 55 up to and including step 4 on page 138.
8. Transfer the cluster wrap key from the CODE-SO and CODE-USER iKeys to card 0.

   When asked to insert the CODE-SO and the CODE-USER iKeys, make sure to use the same CODE iKeys as you did in step 3 on page 138 and step 4 on page 138.

```
(join setup, continued)

Verify that CODE-SO iKey (black) is inserted in card 0 (with
flashing LED).
Hit enter when done.
Verify that HSM-USER iKey (blue) is inserted in card 0 (with
flashing LED).
Hit enter when done.
Verify that CODE-USER iKey (black) is inserted in card 0 (with
flashing LED).
Hit enter when done.
Wrap key successfully combined to card 0.
```

9. Transfer the cluster wrap key to card 1.

```
(join setup, continued)


Verify that CODE-SO iKey (black) is inserted in card 1 (with
flashing LED).
Hit enter when done.
Verify that HSM-USER iKey (blue) is inserted in card 1 (with
flashing LED).
Hit enter when done.
Verify that CODE-USER iKey (black) is inserted in card 1 (with
flashing LED).
Hit enter when done.
Wrap key successfully split combined to card 1.
```

10. If you selected FIPS mode as the security mode, specify the secret passphrase.

Enter the same secret passphrase as you specified in step 5 on page 138. This step only appears if you selected FIPS mode when initializing the HSM cards.

```
(join setup, continued)

Enter the secret passphrase (as given during initialization of
the first iSD in the cluster):<Enter the same secret passphrase
as was used in the former cluster.>
```

If you chose FIPS mode when initializing the first HSM card in the cluster, you will be asked to enter the secret passphrase. Enter the same secret passphrase as when initializing the first HSM card in the cluster.

11. Wait for the setup of the added ASA 310-FIPS to finish.

```
(join setup, continued)

Setup successful.


login:
```

12. Log in to the ASA 310-FIPS ASA 310-FIPS that you are currently connected to and restore the configuration file of the former cluster from an FTP/TFTP/SCP/SFTP server.

```
login:admin

Password:
Alteon iSD SSL
Software version 8.0

>> Main#cfg/gtcfg

Select protocol (tftp/ftp/scp/sftp) [tftp]:ftp

Enter hostname or IP address of server:<server IP address>

Enter name of file on server:<name of saved configuration file>

FTP User (anonymous):<press ENTER if anonymous mode is supported>

Password:
Received 4960 bytes in 0.1 seconds
Password for importing private keys in cfg:<password as defined
when saving the configuration file to an FTP/TFTP/SCP/SFTP server>

Configuration loaded.


>> Configuration#
```

The configuration information is now automatically propagated and applied to all ASA 310-FIPS devices in the cluster. The information includes certificates and encrypted private keys.

Comments? infodev@avaya.com

A User Fails to Connect to the VPN

There can be different reasons for why a user is having difficulty authenticating to the VPN or why a client connection cannot be established: the user name or password is wrong, the configured authentication server cannot be reached, the group name retrieved from the authentication server does not exist on the VPN Gateway and so on.

Note:

The Disable new IPSec Logins feature may have been enacted to allow maintenance of the gateway. Contact your system administrator to determine the status of this feature.

To trace the different steps involved in a specific process, for example, authorization, enter the following command.

```
>> Main#maint/starttrace

Enter tags (list of all,aaa,dns,ike,ipsec,ippool,ssl,tg,pptp,upref,
ftp,smb,netdirect,netdirect_packet) [all]:aaa,ssl

Enter VPN (or 0 for all VPNs) [0]:
Output mode (interactive/tftp/ftp/sftp) [interactive]:
```

Enter the desired tag(s) separated by comma, for example, `aaa,ssl` to trace the user authorization and SSL handshake processes, or press ENTER to trace all processes. To limit tracing to a specific VPN, enter the desired VPN ID, or press ENTER to view trace information for all domains.

Select the desired output mode.

- interactive. The result is displayed directly in the CLI.
- tftp/ftp/sftp. The result is exported as a file to the specified TFTP/FTP/SFTP server.

When starttrace is on, different steps in the selected process (tag) is logged. For sample outputs, see aaa on page 141.

To disable tracing, press ENTER to display the prompt, then enter `stoptrace`.

```
>> Maintenance#stoptrace
```

aaa

The **aaa** tag logs authentication method, user name, timeouts, group and profile (base or extended).

```
>> Maintenance#
12:54:08.875111: Trace started
12:54:28.834571 10.1.82.145 (1) aaa: "local user db Accept 1:john
with groups ["trusted"]"
12:54:28.835144 10.1.82.145 (1) aaa: "final groups for user: john
groups: trusted:<base> "
12:54:29.917926 10.1.82.145 (1) aaa: "TTL for user: john idle: 15m
session: infinity"
```

The output first shows groups received from configured authentication databases. In the preceding example the

`trusted`

group is returned from the local user database. If an external authentication database is used, all groups returned from that database will be shown.

Final groups for the user are all groups where a match is found between groups returned from configured authentication databases and groups configured on the VPN Gateway. Matching groups are listed in the order they are configured on the VPN Gateway. This is also the order in which the groups will be applied. <base> implies that the group's base profile will be used.

TTL for user shows the idle timeout (15m (15 minutes) in the preceding example) and the maximum session length (infinity in the example).

For detailed information about groups, profiles and so on, see the chapter "Groups, Access Rules and Profiles" in the *CLI/BBI Application Guide for VPN*.

dns

The **dns** tag logs failed DNS lookups made during a VPN session.

```
>> Maintenance#
13:00:09.868682 10.1.82.145 (1) dns: "Failed to lookup www.exam-
ple.com in DNS (DNS domain name does not exist)"
```

ike

The **ike** tag logs any output that is produced by the IKE daemon, e.g. all messages related to actual ISAKMP negotiations between the client and the IKE daemon.

```
>> Maintenance#
13:03:47.692954 10.1.82.145 (0) ike: "ISAKMP SA Established with
john (192.168.128.19)" 13:03:47.885492 10.1.82.145 (0) ike: "IPSec
SA Established with john (192.168.128.19), IPComp N/A, inbound CPI
0x0"
```


Comments? infodev@avaya.com

ipsec

The **ipsec** tag logs any AAA-related output concerning the establishment of an IPsec tunnel.

```
>> Maintenance#
14:05:22.866730 10.1.82.145 (1) ipsec: "Creating isakmp tunnel ses-
sion for user <john>"
14:05:22.869265 10.1.82.145 (1) ipsec: "Replying to ike that isakmp
sess is created sid=3, tp="vpn_1_1", u=john"
14:05:22.870305 10.1.82.145 (1) ipsec: "Deleting session 3 ,Ike
explicitly deleted it"
14:05:23.717120 10.1.82.145 (1) ipsec: "Creating isakmp tunnel ses-
sion for user <john>"
14:05:23.717673 10.1.82.145 (1) ipsec: "Replying to ike that isakmp
sess is created sid=4, tp="vpn_1_1", u=john"
14:05:23.782443 10.1.82.145 (1) ipsec: "Allocated Tunnel IP
10.1.82.149"
14:05:23.782961 10.1.82.145 (1) ipsec: "Setting primNbns=0.0.0.0,
primdns=10.1.0.10, domainname=example.com"
```

ippool

The **ippool** tag logs messages related to the allocation of IP addresses from the IP pool (applies to Net Direct and IPsec).

```
>> Maintenance#
14:02:28.145414: Trace started
14:02:59.013407 10.1.82.145 (1) ippool: "Adding arp entry for
10.1.82.148 on interface 1 (device eth1)"
14:02:59.014058 10.1.82.145 (1) ippool: "Alloc ip 10.1.82.148 on
behalf of "netdirect""
```

ssl

The **ssl** tag logs information related to the SSL handshake procedure, e.g. used cipher.

```
>> Maintenance#
13:15:55.985432: Trace started
13:16:26.808831 10.1.82.145 (1) ssl: "SSL accept done, cipher is
RC4-MD5"
13:16:28.802199 10.1.82.145 (1) ssl: "SSL accept done, cipher is
RC4-MD5"
13:16:29.012856 10.1.82.145 (1) ssl: "SSL accept done, cipher is
RC4-MD5"
```

tg

The **tg** tag logs information related to a Tunnel Guard check, e.g. access method, user name, user source IP, Tunnel Guard session status and SRS rule check result.

```
>> Maintenance#
13:27:50.715545: Trace started
13:27:54.976137 10.1.82.145 (1) tg: "ssl user john[192.168.128.19] -
starting tunnelguard ssl session"
13:28:17.204049 10.1.82.145 (1) tg: "ssl user john[192.168.128.19] -
agent authentication ok"
13:28:18.807447 10.1.82.145 (1) tg: "user john[192.168.128.19] - SRS
checks ok, open session"
```

upref

The **upref** tag shows information related to retrieval and storage of user preferences, e.g. Portal bookmarks. For more information about how to enable this feature, see the section "The Tools tab, Edit Bookmarks" in the chapter "The Portal from an End-User Perspective" in the *CLI/BBI Application Guide for VPN*.

```
>> Maintenance#
12:55:34.093948 127.0.0.1 (1) upref: "userpref found for
user="john""
12:56:18.702323 127.0.0.1 (1) upref: "added userpref
entry="www.cnn.com", user="john""
12:56:36.890725 127.0.0.1 (1) upref: "LDAP connect succeeded for
john"
12:56:36.893461 127.0.0.1 (1) upref: "bind succeeded for: john"
12:56:37.153940 127.0.0.1 (1) upref: "userpref saved for user="john"
```

smb

The **smb** tag shows information related to SMB (Windows file share) sessions initiated through the Portal's Files tab.

Comments? infodev@avaya.com

```
>> Maintenance#
15:43:56.427933: Trace started
15:44:10.877107 10.1.82.145 (1) smb: "user: john connected to SMB
server: 192.168.128.1"
15:44:10.885579 10.1.82.145 (1) smb: "user: john is authenticated
(unicode=false smbsign=false ssn=0)"
15:44:10.888012 10.1.82.145 (1) smb: "user: john connected to:
\\192.168.128.1\JOHN (ssn=0 charset=iso-8859-1) "
15:44:10.915649 10.1.82.145 (1) smb: "user: john list_dir successful
(ssn=0)"
```

ftp

The **`ftp`** tag shows information related to FTP sessions initiated through the Portal's Files tab.

```
>> Maintenance#
15:50:16.362765 10.1.82.145 (1) ftp: "user: john connected to FTP
server: 192.168.128.1"
15:50:16.372000 10.1.82.145 (1) ftp: "user: john is authenticated"
15:50:16.373548 10.1.82.145 (1) ftp: "user: john pwd succeeded"
15:50:16.375014 10.1.82.145 (1) ftp: "user: john set binary"
15:50:16.424280 10.1.82.145 (1) ftp: "user: john 'dir' successful
(redirected to home directory)"
15:50:16.443105 10.1.82.145 (1) ftp: "user: john 'dir' started, cli-
cset=iso-8859-1 be-cset=ASCII"
15:50:16.501245 10.1.82.145 (1) ftp: "user: john 'dir' successful"
```

netdirect

The **`netdirect`** tag logs information pertaining to the Net Direct client connection, e.g. that a connection has been requested and that it has been accepted or rejected.

```
>> Maintenance#
13:31:42.654216 10.1.82.145 (1) netdirect: "Netdirect client connec-
tion requested (session 61)"
13:31:42.684871 10.1.82.145 (1) netdirect: "Netdirect client connec-
tion accepted (session 61)"
```

netdirect_packet

The **`netdirect_packet`** tag logs information about packets being sent and received when the user has initiated a connection to a host.

```
>> Maintenance#
14:11:38.799781 10.1.82.145 (1) netdirect_packet: "Netdirect packet
from server to 10.1.82.149, size 40, sending over SSL (session 7)"
14:11:38.808303 10.1.82.145 (1) netdirect_packet: "Netdirect packet
from client to 192.168.128.1, size 40, sending over SSL (session 7)"
14:11:40.946930 10.1.82.145 (1) netdirect_packet: "Netdirect packet
from client to 192.168.128.1, size 40, sending over SSL (session 7)"
14:11:52.730401 10.1.82.145 (1) netdirect_packet: "Netdirect packet
from client to 10.1.82.255, size 237, sending over SSL (session 7)"
```

Because of the large amount of information, we recommend logging to a TFTP/FTP/SFTP server.

User Unable to Connect to the VPN Gateway through the Net Direct Client

Start by verifying on your own PC that Net Direct works towards the same VPN Gateway as the end-user's device.

Then check the following in the specified order:

1. Is the user logged in to the Portal? Check in the CLI.

   You can choose to limit the output of logged in users to a particular VPN by providing the VPN number as a modifier to the **users** command. To limit the output further, you can also provide one or more initial letters of a user name, directly followed by an asterisk (*).

   ```
   >> Information#users 1 s*
   ```

   If the user is not logged in, make sure the user can log into the Portal at all. See A User Fails to Connect to the VPN on page 141.

2. Is Net Direct enabled and configured correctly?

   See the "Net Direct" chapter in the *Avaya Application Guide for VPN* for instructions on how to enable Net Direct and how to configure an IP pool.

3. Is the Net Direct link visible to the end-user on the Portal's Home tab?

   If not, the user may belong to a group that does not have access to the linkset where the Net Direct link is included. See the "Net Direct" chapter in the *Avaya Application Guide for VPN* for instructions on how to configure a Net Direct link and map the linkset to the desired group.

4. For Windows, is the Net Direct ActiveX control present on the end-user's PC?

   Let the end-user check the following: In Internet Explorer, on the **Tools** menu, select **Internet options**. On the **General** tab, under **Temporary Internet Files**, click

Settings. Click **View objects**. Verify that the Net Direct control is installed and that the version corresponds to the VPN Gateway 's version.

If the ActiveX control cannot be started, Net Direct tries to start the Java applet instead.

For Linux and Mac (and Windows), is the Java applet window displayed properly?

If an X is displayed in the Java applet window, check the Java Console Window (select **Java Console** on the **Tools** menu).

5. Let the end-user log into the Portal again.
6. Make sure that the end-user allows ActiveX controls and scripting of ActiveX controls (Windows only).

   The warning dialogue might be hidden in the IE info field in XP SP2.
7. When the end user has logged in and clicked on a Net Direct link, is the Net Direct splash screen (progress bar) shown?

   Notice any error message in the splash screen (progress bar) and act accordingly.
8. On Windows, is the Avaya Net Direct icon visible on the system tray (next to the clock bottom right)?

   If the end user is using Windows, make sure Windows XP or Windows 2000 and Internet Explorer 5.0 or later is used.

   On Linux and Mac, is the message "Net Direct started" displayed in the Net Direct Java applet window?
9. Verify that the maximum number of users for the license currently loaded to the VPN Gateway has not been reached.

   If required, user's can be logged out from the VPN through the **`/info/kick`** command. To accommodate more users in the VPN, you may have to purchase a license valid for a larger number of users.
10. Ask the end-user to send (e.g. through e-mail) the Net Direct error log file for inspection.

    An error log file is written to the root of the System Drive if Net Direct cannot be activated. On Windows, the usual location/name is `C:\Documents and Settings\<user>\Local Settings\Temp\NetDirectError.log`. On Linux and Macintosh, the NetDirectError.log file is created under `/tmp` on the client machine.
11. On Windows, when the end user double-clicks the Net Direct icon in the system tray, what settings are shown?

    Verify that the settings shown corresponds to the settings you have made in the CLI/BBI. For example, the IP address used should be from the IP pool.

    On Linux and Mac, click the Advanced button in the Net Direct Java applet window.

Verify that the settings shown corresponds to the settings you have made in the CLI/BBI. For example, the IP address used should be from the IP pool.

12. On Windows, when the end user starts a new instance of Internet Explorer from the Start menu and points to a site you know should be tunneled – does the Net Direct icon on the system tray blink green?

    Does it ever blink green? Check (using **`/maint/starttrace`** and the **`netdirect_packet`** tag) that traffic is flowing from and to the client machine. If no traffic flows, verify on your own machine that Net Direct works. For more information about the **`starttrace`** command see the section A User Fails to Connect to the VPN on page 141.

    On Linux and Mac, are sent and received bytes displayed in the Net Direct Java applet window?

Cannot download the Net Direct Zipped file from client PC

Follow these steps to download the Net Direct_Zip file:

1. Download the NetDirect_Setup.zip file using the portal.

   `https://vpn-ip/avaya_cacheable/NetDirect_Setup.zip.`

2. Customize the Netdirect_setup file and save as `SetDirect_Setup_Custom.zip`.

3. Place the NetDirect_Setup_Custom.zip file in a folder named avaya_cacheable and zip the avaya_cacheable folder

   This is because after imported into the AVG the top directory will be unzipped in the AVG.

4. Import the customized file (avaya_cacheable.zip) into the AVG through BBI/CLI.

   `cfg/vpn #/portal/content/import`

5. Login as root and we can find the imported file in the path `/config/isd/user_content/docroot`.

   You can access <https://vpn-ip/avaya_cacheable/NetDirect_Setup_Custom.zip>.

System Diagnostics

A few system diagnostics can be performed on the VPN Gateway.

Installed Certificates and Virtual SSL Servers

To view the currently installed certificates, type the following command:

```
>> # /info/certs
```

To view detailed information about a specific certificate, access the Certificate menu and specify the desired certificate by its index number:

```
>> #/cfg/cert
Enter certificate number: (1-)<certificate number by index>
>> Certificate 1#show
```

To view the configured virtual SSL servers, type the following command:

```
>> #/info/servers
```

The screen output provides information about which certificate (indicated by certificate index number) is used by each configured SSL server.

Network Diagnostics

To check if the VPN Gateway is able to contact configured gateways, routes, DNS servers, authentication servers, and IP addresses/domain names specified in group links, use the following command:

```
>> #/maint/chkcfg
```

The screen output provides information about each configured item (For example, gateway and DNS server) and shows whether the network test was successful or not. Besides checking the connection, the method (For example, ping) for checking each item is displayed.

To check various network settings for a specific VPN Gateway, access the iSD Host menu by typing the following commands:

```
>> #/cfg/sys/host
Enter iSD host number: (1-)<iSD host by index number>
```

```
>> iSD Host 1#cur
```

The screen output provides information about the type of iSD (master or slave), IP address, network mask, and gateway address for the VPN Gateway you have specified (by host number).

To check general network settings related to the cluster to which you have connected, type the following command:

```
>> #/cfg/sys/cur
```

The screen output provides information about the management IP address (MIP) of the AVG cluster, DNS servers, iSD hosts in the cluster, Syslog servers, and NTP servers.

To check if the VPN Gateway(s) is getting network traffic, type the following command:

```
>> #/stats/dump
```

The screen output provides information about currently active request sessions, total completed request sessions, as well as SSL statistics for configured virtual SSL servers.

To check statistics for the local Ethernet network interface card, type the following command:

```
>> #/info/ethernet
```

The screen output provides information about the total number of received and transmitted packets, the number of errors when receiving and transmitting packets, as well as the type of error such as dropped packets, overrun packets, malformed packets, packet collisions, and lack of carrier.

To check if a virtual server (on the Application Switch) is working, type the following command at any menu prompt:

```
>> #ping <IP address of virtual server>
```

To capture and analyze TCP traffic sent from a virtual SSL server to the backend server, type the following command (where you replace "#" with the index number of the desired virtual SSL server):

```
>> #/cfg/ssl/server #/trace/tcpdump
```


Comments? infodev@avaya.com

To capture and analyze decrypted SSL traffic sent between a client and a virtual SSL server, type the following command (where you replace "#" with the index number of the desired virtual SSL server):

```
>> #/cfg/ssl/server #/trace/ssldump
```

Active Alarms and the Events Log File

To view an alarm that has been triggered and is active, type the following command:

```
>> #/info/events/alarms
```

In the current software version of the AVG, an alarm is only triggered when a hardware failure in an SSL accelerator card is detected.

To save the events log file to an FTP/TFTP/SFTP server, type the following command:

```
>> #/info/events/download
```

You need to provide the IP address or host name of the FTP/TFTP/SFTP server, as well as a file name. After the events log file has been saved, connect to the FTP/TFTP/SFTP server and examine the contents of the file.

Error Log Files

Provided you have configured the VPN Gateway to use a Syslog server, the VPN Gateway will send log messages to the specified Syslog server. For more information about how to configure a UNIX Syslog daemon, see the Syslog manpages under UNIX. For more information about how to configure the VPN Gateway to use a Syslog server, see the "Syslog Servers Configuration " section under Configuration Menu>System Configuration in the *Avaya Command Reference*.

Another option is to use the **`/maint/dumplogs`** command. It collects system log file information from the VPN Gateway you are connected to (or optionally, all AVGs in the cluster) and sends the information to a file in the gzip compressed tar format on the TFTP/FTP/SFTP server you have specified. The information can then be used for technical support purposes. The file sent to the TFTP/FTP/SFTP server does not contain any sensitive information related to the system configuration, such as certificates, private keys, and so on.

Unable to download Net Direct from VPN server

After installing Net Direct v1.0.2.3+ as a result of upgrading to code releases v5.1.3.4 or higher and subsequently downgrading the portal software to v5.1.3.3 or earlier, the Net Direct client fails to load and produces an error.

To use the Net Direct with v5.1.3.4 or earlier release, you need to manually remove the Net Direct and relaunch the portal and earlier Net Direct. To remove the Net Direct, follow these steps:

1. Open Windows Explorer to `C:\WINNT\Downloaded Program Files`.
2. Right click on NetDirect.OCX ActiveX control.
3. Select **Remove**.

   Net Direct is uninstalled.

Comments? infodev@avaya.com

Appendix A: Supported Ciphers

The Avaya VPN Gateway (AVG) supports SSL version 2.0, SSL version 3.0, and TLS version 1.0. All ciphers covered in these versions of SSL are supported, except the IDEA and FORTEZZA ciphers and ciphers using DH or DSS authentication.

Table 5: Supported Ciphers

Cipher Name	SSL Protocol	Key Exchange Algorithm, Authentication	Encryption Algorithm	MAC Digest Algorithm
DHE-RSA-AES256-SHA	SSLv3	DH, RSA	AES (256)	SHA1
AES256-SHA	SSLv3	RSA, RSA	AES (256)	SHA1
EDH-RSA-DES-CBC3- SHA	SSLv3	DH, RSA	3DES (168)	SHA1
DES-CBC3-SHA	SSLv3	RSA, RSA	3DES (168)	SHA1
DES-CBC3-MD5	SSLv2	RSA, RSA	3DES (168)	MD5
DHE-RSA-AES128-SHA	SSLv3	DH, RSA	AES (128)	SHA1
AES128-SHA	SSLv3	RSA, RSA	AES (128)	SHA1
RC4-SHA	SSLv3	RSA, RSA	RC4 (128)	SHA1
RC4-MD5	SSLv3	RSA, RSA	RC4 (128)	MD5
RC2-CBC-MD5	SSLv2	RSA, RSA	RC2 (128)	MD5
RC4-MD5	SSLv2	RSA, RSA	RC4 (128)	MD5
RC4-64-MD5	SSLv2	RSA, RSA	RC4 (64)	MD5
EXP1024-RC4-SHA	SSLv3	RSA(1024), RSA	RC4 (56)	SHA1 EXPORT
EXP1024-DES-CBC-SHA	SSLv3	RSA (1024), RSA	DES (56)	SHA1 EXPORT
EXP1024-RC2-CBC-MD5	SSLv3	RSA (1024), RSA	RC2 (56)	MD5 EXPORT
EXP1024-RC4-MD5	SSLv3	RSA (1024), RSA	RC4 (56)	MD5 EXPORT
EDH-RSA-DES-CBC-SHA	SSLv3	DH, RSA	DES (56)	SHA1
DES-CBC-SHA	SSLv3	RSA, RSA	DES (56)	SHA1
DES-CBC-MD5	SSLv2	RSA, RSA	DES (56)	MD5
EXP-EDH-RSA-DES-CBC-SHA	SSLv3	DH (512), RSA	DES (40)	SHA1 EXPORT
EXP-DES-CBC-SHA	SSLv3	RSA (512), RSA	DES (40)	SHA1 EXPORT

Cipher Name	SSL Protocol	Key Exchange Algorithm, Authentication	Encryption Algorithm	MAC Digest Algorithm
EXP-RC2-CBC-MD5	SSLv3	RSA (512), RSA	RC2 (40)	MD5 EXPORT
EXP-RC4-MD5	SSLv3	RSA (512), RSA	RC4 (40)	MD5 EXPORT
EXP-RC2-CBC-MD5	SSLv2	RSA (512), RSA	RC2 (40)	MD5 EXPORT
EXP-RC4-MD5	SSLv2	RSA (512), RSA	RC4 (40)	MD5 EXPORT
ADH-AES256-SHA	SSLv3	DH, NONE	AES (256)	SHA1
ADH-DES-CBC3-SHA	SSLv3	DH, NONE	3DES (168)	SHA1
ADH-AES128-SHA	SSLv3	DH, NONE	AES (128)	SHA1
ADH-RC4-MD5	SSLv3	DH, None	RC4 (128)	MD5
ADH-DES-CBC-SHA	SSLv3	DH, NONE	DES (56)	SHA1
EXP-ADH-DES-CBC-SHA	SSLv3	DH (512), None	DES (40)	SHA1 EXPORT
EXP-ADH-RC4-MD5	SSLv3	DH (512), None	RC4 (40)	MD5 EXPORT

Cipher List Formats

The cipher list you specify for a virtual SSL server consists of one or more cipher strings separated by colons (e.g. RC4:+RSA:+ALL:!NULL:!DH:!EXPORT@STRENGTH). Lists of ciphers can be combined using a logical and operation (+) (e.g. SHA1+DES represents all cipher suites containing the SHA1 and the DES algorithms).

In the colon-separated list, any cipher string can be preceded by the characters !, - or +. These characters serve as modifiers, with the following meanings:

- ! permanently deletes the ciphers from the list (e.g. !RSA).
- - deletes the ciphers from the list, but the ciphers can be added again by later options.
- + moves the ciphers to the end of the list. This option doesn't add any new ciphers it just moves matching existing ones.
- `@STRENGTH`

  is placed at the end of the cipher list, and sorts the list in order of encryption algorithm key length.

The default cipher list used for all virtual SSL servers on the VPN Gateway is

```
ALL@STRENGTH.
```

A cipher list consisting of the string

```
RC4:ALL:!DH
```


Comments? infodev@avaya.com

translates into a preferred list of ciphers that begins with all ciphers using RC4 as the encryption algorithm, followed by all cipher suites except the eNULL ciphers (ALL). The final

```
!DH
```

string means that all cipher suites containing the DH (Diffie-Hellman) cipher are removed from the list. (Few of the major web browsers support these ciphers.)

Modifying a Cipher List

Starting from the

```
RC4:ALL:!DH
```

cipher list, an example of a slightly modified cipher list can be:

```
RC4:ALL:!EXPORT:!DH
```

This example will remove all EXPORT ciphers, besides the DH related cipher suites. Removing the EXPORT ciphers means that all ciphers using either 40 or 56 bits symmetric ciphers are removed from the list. This means that browsers running export controlled crypto software cannot access the server.

Using the OpenSSL command line tool (on a UNIX machine), it is possible to check which cipher suites a particular cipher list corresponds to. The preceding example yields the following output:

```
# openssl ciphers -v 'RC4:ALL:!EXPORT:!DH
RC4-SHA          SSLv3 Kx=RSA    Au=RSA   Enc=RC4(128)    Mac=SHA1
RC4-MD5          SSLv3 Kx=RSA    Au=RSA   Enc=RC4(128)    Mac=MD5
RC4-64-MD5       SSLv2 Kx=RSA    Au=RSA   Enc=RC4(64)     Mac=MD5
RC4-MD5          SSLv2 Kx=RSA    Au=RSA   Enc=RC4(128)    Mac=MD5
DES-CBC3-SHA     SSLv3 Kx=RSA    Au=RSA   Enc=3DES(168)   Mac=SHA1
DES-CBC-SHA      SSLv3 Kx=RSA    Au=RSA   Enc=DES(56)     Mac=SHA1
DES-CBC3-MD5     SSLv2 Kx=RSA    Au=RSA   Enc=3DES(168)   Mac=MD5
DES-CBC-MD5      SSLv2 Kx=RSA    Au=RSA   Enc=DES(56)     Mac=MD5
RC2-CBC-MD5      SSLv2 Kx=RSA    Au=RSA   Enc=RC2(128)    Mac=MD5
```

Supported Cipher Strings and Meanings

The following table lists each supported cipher string alias and its significance.

Table 6: Cipher Strings and Meanings

Cipher String Aliases	Meaning
DEFAULT	The default cipher list, which corresponds to

Cipher String Aliases	Meaning
	`ALL@STRENGTH` .
ALL	All cipher suites except the eNULL ciphers, which must be explicitly enabled.
HIGH	Cipher suites with key lengths larger than 128 bits.
MEDIUM	Cipher suites using 128 bit encryption.
LOW	Includes cipher suites using 64 or 56 bit encryption, but excludes export cipher suites.
EXPORT	Includes cipher suites using 40 and 56 bit encryption.
EXPORT40	Cipher suites using 40 bit export encryption only.
EXPORT56	Cipher suites using 56 bit export encryption only.
eNULL, NULL	Cipher suites that do not offer any encryption at all. Because the use of such ciphers pose a security threat, they are disabled unless explicitly included.
aNULL	Cipher suites that do not offer authentication, like anonymous DH algorithms. The use of such cipher suites is not recommended, because they facilitate man-in-the-middle attacks.
kRSA, RSA	Cipher suites using RSA key exchange.
kEDH	Cipher suites using ephemeral Diffie-Hellman key agreement.
aRSA	Cipher suites using RSA authentication, which implies that the certificates carry RSA keys.
SSLv3, SSLv2	SSL version 3.0 and SSL version 2.0 cipher suites, respectively.
DH	Cipher suites using DH encryption algorithms, including anonymous DH.
ADH	Cipher suites using anonymous DH encryption algorithms.
AES	Cipher suites using AES encryption algorithms.
3DES	Cipher suites using triple DES encryption algorithms.
Cipher String Aliases	Meaning
DES	Cipher suites using DES encryption algorithms, but not triple DES.
RC4	Cipher suites using RC4 encryption algorithms.

Comments? infodev@avaya.com

Cipher String Aliases	Meaning
RC2	Cipher suites using RC2 encryption algorithms.
MD5	Cipher suites using MD5 encryption algorithms.
SHA1, SHA	Cipher suites using SHA1 encryption algorithms.

Comments? infodev@avaya.com

Appendix B: The SNMP Agent

There is one SNMP agent on each Avaya VPN Gateway (AVG), and the agent listens to the IP address of that particular device. On the VPN Gateway that currently holds the cluster's Management IP address (MIP), the SNMP agent also listens to the MIP.

The SNMP agent supports SNMP version 1, version 2c and version 3. Notification targets (the SNMP managers receiving trap messages sent by the agent) can be configured to use either SNMP v1, v2c and v3 (with the default being SNMP v2c). Users may specify any number of notification targets on the VPN Gateway.

For more information about the commands used to configure the SNMP agent in a cluster, see the "*SNMP Management Configuration* " section under *Configuration Menu>System Configuration* in the *Avaya Command Reference*.

For detailed information about the MIB (Management Information Base) definitions that are currently implemented for the SNMP agent, do one of the following:

- Go to http://www.avaya.com. In the left pane, select Downloads. In the Product dialog box, type VPN Gateway 3050 or VPN Gateway 3070. Select the release number you want from the pull-down list, and then select the download package you want. Click the Downloads tab. Search on the resulting page for the mib file you want.
- Connect to the Browser-Based Management Interface (BBI) In the System tree view, expand **Administration** and **SNMP**. Finally select the **MIBs** form.

The file ALTEON-SSL-CAP.mib contains an AGENT-CAPABILITIES statement, which formally specifies which MIBs are implemented.

Supported MIBs

The VPN Gateway supports the following MIBs:

- SNMPv2-MIB
- SNMP-MPD-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-TARGET-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-VIEW-BASED-ACM-MIB
- SNMP-USER-BASED-SM-MIB
- SYNOPTICS-ROOT-MIB

- S5-TCS-MIB
- S5-ROOT-MIB
- S5-ETH-MULTISEG-TOPOLOGY-MIB
- IF-MIB
- IP-MIB
- IP-FORWARD-MIB
- ENTITY-MIB
- DISMAN-EVENT-MIB
- ALTEON-ISD-PLATFORM-MIB
- ALTEON-ISD-SSL-MIB
- ALTEON-SSL-VPN-MIB
- ALTEON-ROOT-MIB
- IANAifType-MIB

SNMPv2-MIB

The SNMPv2-MIB is a standard MIB implemented by all agents. The following groups are implemented:

- snmpGroup
- snmpSetGroup
- systemGroup
- snmpBasicNotificationsGroup
- snmpCommunityGroup

Comments? infodev@avaya.com

SNMP-MPD-MIB

The following group is implemented:

- snmpMPDGroup

SNMP-FRAMEWORK-MIB

The following group is implemented:

- snmpEngineGroup

The SNMP-TARGET MIB

The SNMP-TARGET-MIB contains information about where to send traps. This is also configurable/viewable from the CLI, using the **`/cfg/sys/adm/snmp/target`** command.

The following groups are implemented:

- snmpTargetCommandResponderGroup
- snmpTargetBasicGroup
- snmpTargetResponseGroup

Write access to snmpTargetParamsTable is turned off in VACM.

SNMP-NOTIFICATION-MIB

The following group is implemented:

- snmpNotifyGroup

Write access to all objects in this MIB is turned off in VACM.

SNMP-VIEW-BASED-ACM-MIB

The following group is implemented:

- vacmBasicGroup

Write access to all objects in this MIB is turned off in VACM.

SNMP-USER-BASED-SM-MIB

The following group is implemented:

- usmMIBBasicGroup

Write access to all objects in this MIB is turned off in VACM.

S5-ETH-MULTISEG-TOPOLOGY-MIB

This MIB is used when the AVG participates in SONMP. The following groups are implemented:

- s5EnMsTopInfo
- s5EnMsTopNmm
- s5EnMsTopBdg
- s5EnMsSrcMac

SYNOPTICS-ROOT-MIB

This MIB provides product IDs and descriptions for SONMP-aware products. It is required by the S5-ETH-MULTISEG-TOPOLOGY-MIB MIB.

S5-TCS-MIB

This MIB is used when the AVG participates in SONMP. It is required by the S5-ETH-MULTISEG-TOPOLOGY-MIB MIB.

S5-ROOT-MIB

This MIB is used when the AVG participates in SONMP. It is required by the S5-ETH-MULTISEG-TOPOLOGY-MIB MIB.

IF-MIB

The following groups are implemented:

- ifPacketGroup
- ifStackGroup

Limitations

The agent does not implement the following objects:

- ifType
- ifSpeed
- ifLastChange
- ifInUnknownProtos
- ifOutNUnicast

IP-MIB

The following groups are implemented:

- ipGroup
- icmpGroup

IP-FORWARD-MIB

The following group is implemented:

- ipCidrRouteGroup

ENTITY-MIB

The following groups are implemented:

- entityPhysicalGroup
- entityPhysical2Group
- entityGeneralGroup
- entityNotificationsGroup

Write access to snmpTargetParamsTable is turned off in VACM.

DISMAN-EVENT-MIB

The DISMAN-EVENT-MIB is a MIB module for defining event triggers and actions for network management purposes. See the **`/cfg/sys/adm/snmp/event`** command in the *Command Reference* for instructions on how to add a monitor as defined in this MIB.

The following groups are implemented:

- dismanEventResourceGroup
- dismanEventTriggerGroup
- dismanEventObjectsGroup
- dismanEventEventGroup
- dismanEventNotificationObjectGroup
- dismanEventNotificationGroup

ALTEON-ISD-PLATFORM-MIB

The ALTEON-ISD-PLATFORM-MIB contains the following groups and objects:

- isdClusterGroup
- isdResourceGroup
- isdAlarmGroup
- isdBasicNotificatioObjectsGroup
- isdEventNotificationGroup
- isdAlarmNotificationGroup

ALTEON-ISD-SSL-MIB

The ALTEON-ISD-SSL-MIB contains objects for monitoring the SSL gateways. The following groups are implemented:

- sslBasicGroup
- sslEventGroup

Comments? infodev@avaya.com

ALTEON-SSL-VPN-MIB

The ALTEON-SSL-VPN-MIB contains SSL/IPsec user statistics and SSL/IPsec license information for all VPNs. It also contains authentication server statistics. The following groups are implemented:

- vpnBasicGroup
- vpnEventGroup

IANAifType-MIB

Defines the IANAifType Textual Convention, and thus the enumerated values of the ifType object defined in MIB-II's ifTable.

Supported Traps

The following SNMP traps are supported by the VPN Gateway:

Table 7: Traps Supported by the VPN Gateway

Trap Name	Description
alteonISDSSLHsmNotLoggedIn	Signifies that login to the HSM card is required. Only for the ASA 310 FIPS model.
alteonISDSSLHsmTamperedWith	Signifies that the HSM card has been tampered with. Only for the ASA 310 FIPS model.
alteonISDSSLHwFail	Signifies that the SSL accelerator hardware failed. The VPN Gateway will continue to handle traffic, but with severely degraded performance.
authenticationFailure	Sent when the SNMP agent receives an SNMP message which is not properly authenticated. This trap is disabled by default. To enable the trap through SNMP, set `snmpEnableAuthenTraps` to enabled or use the CLI command **`/cfg/sys/adm/snmp/snmpv2-mib/snmpenable`**. Defined in SNMPv2-MIB.
coldStart	Sent when the VPN Gateway reboots. Defined in SNMPv2-MIB.
isdAlarmCleared	Sent when an alarm is cleared.

Trap Name	Description
isdDown	Signifies that a VPN Gateway in the cluster is down and out of service.
isdLicense	Sent when the VPN Gateways in the cluster have different licenses and when a demo license has 7 days left before expiration. Defined in ALTEON-ISD-PLATFORM-MIB.
isdLicenseExpired	Sent when a license has expired.
isdMipMigration	Signals that the master IP has migrated to another VPN Gateway.
isdSingleMaster	Signifies that only one master VPN Gateway in the cluster is up and operational. Only having one master in a cluster means that the fault tolerance level is severely degraded—if the last master fails, the system cannot be reconfigured. This trap is only sent if more than two VPN Gateways in the cluster are defined as masters.
linkDown	Sent when the agent detects that one of the links (interfaces) has gone down. Defined in IF-MIB.
linkUp	Sent when the agent detects that one of the links (interfaces) has gone up. Defined in IF-MIB.
vpnLicenseExhausted	Sent when the VPN has run out of SSL or IPsec user licenses. No more than one event per hour is sent for one VPN. Defined in ALTEON-SSL-VPN-MIB.

Comments? infodev@avaya.com

Appendix C: Syslog Messages

This appendix contains a list of the syslog messages that are sent from the Avaya VPN Gateway (AVG) to a Syslog server (when added to the system configuration). All the syslog messages follow common specifications. These messages are compliant with the SYSLOG SRD specifications. They can be stored locally on the hard disk or in a memory buffer. Syslog servers are added to the system configuration by using the menu options in the Syslog Servers menu. To view the menu options, see the "*Syslog Servers Configuration*" section under *Configuration Menu>System Configuration* in the *Avaya Command Reference*.

List of Syslog Messages

This section lists the Syslog messages that can be sent from a VPN Gateway to a configured Syslog server. The messages are divided into the following message types:

- Operating system (OS)
- System control
- Traffic processing
- Startup
- Configuration reload
- AAA
- IPsec

To view a list of syslog messages in alphabetical order, see the section Syslog Messages in Alphabetical Order on page 185.

Operating System (OS) Messages

The OS system messages are divided into three categories:

- EMERG
- CRITICAL
- ERROR

EMERG

- Root filesystem corrupt

  The system cannot boot, but stops with a single-user prompt. fsck failed. Reinstall to recover.

- Config filesystem corrupt beyond repair

  The system cannot boot, but stops with a single-user prompt. Reinstall to recover.

- Failed to write to config filesystem

  Probable hardware error. Reinstall.

CRITICAL

- Config filesystem re-initialized - reinstall required

  Reinstall.

- Application filesystem corrupt - reinstall required

  Reinstall.

ERROR

- Config filesystem corrupt

  Possible loss of configuration. Followed by the message Config filesystem re-initialized - reinstall required or Config filesystem restored from backup.

- Missing files in config filesystem

  Possible loss of configuration. Followed by the message Config filesystem re-initialized - reinstall required or Config filesystem restored from backup.

- Logs filesystem re-initialized

  Loss of logs.

- Root filesystem repaired - rebooting

  fsck found and fixed errors. Probably OK.

- Config filesystem restored from backup

  Loss of recent configuration changes.

- Rebooting to revert to permanent OS version

Comments? infodev@avaya.com

Happens after Config filesystem re-initialized - reinstall required or Config filesystem restored from backup if software upgrade is in progress (that is, if failure at first boot on new OS version).

System Control Process Messages

The System Control Process messages are divided into three categories:

- INFO
- ALARM
- EVENT

Both events and alarms are stored in the event log file, which can be accessed by typing the **`/info/events/download`** command. Active alarms can be viewed by typing the **`/info/events/alarms`** command.

INFO

System started [isdssl-<version>]

Sent whenever the system control process has been (re)started.

ALARM

Alarms are sent at a syslog level corresponding to the alarm severity as shown in the following table:

Alarm Severity	Syslog Level
CRITICAL	ALERT
MAJOR	CRITICAL
MINOR	ERROR
WARNING	WARNING
*	ERROR

Alarms are formatted according to the following pattern:

Id: <alarm sequence number> Severity: <severity> Name: <name of alarm> Time. <date and time of the alarm> Sender: <sender, e.g. system or the VPN Gateway 's IP address> Cause: <cause of the alarm> Extra: <additional information about the alarm>

To simplify finding the desired alarm messages, this section lists alarms with the name parameter on top.

- Name: isd_down Sender: <IP> Cause: down Extra: Severity: critical

  A member of the AVG cluster is down. This alarm is only sent if the cluster contains more than one VPN Gateway.

- Name: single_master Sender: system Cause: down Extra: Severity: warning

  Only one master VPN Gateway in the cluster is up and running.

- Name: log_open_failed Sender: <IP>, event Cause and Extra are explanations of the fault. Severity: major

  The event log (where all events and alarms are stored) could not be opened.

- Name: make_software_release_permanent_failed Sender: <IP> Cause: file_error | not_installed Extra: "Detailed info" Severity: critical

  Failed to make a new software release permanent after being activated. The system will automatically revert to the previous version.

- Name: copy_software_release_failed Sender: <IP> Cause: copy_failed | bad_release_package | no_release_package | unpack_failed Extra: "Detailed info" Severity: critical

  A VPN Gateway failed to install a software release while trying to install the same version as all other VPN Gateways in the cluster. The failing VPN Gateway tries to catch up with the other cluster members as it was not up and running when the new software version was installed.

- Name: license Sender: license_server Cause: license_not_loaded Extra: "All iSDs do not have the same license loaded " Severity: warning

  All VPN Gateways in the cluster do not have a license containing the same set of licensed features. Check loaded licenses using the **`/cfg/sys/cur`** command.

- Name: license Sender: <IP> Cause: license_expire_soon Extra: "Expires: <TIME> " Severity: warning

  The (demo) license loaded to the local VPN Gateway expires within 7 days. Check loaded licenses using the **`/cfg/sys/cur`** command.

- Name: ssl_hw_fail Sender: <IP> Cause: find_error |init_error Extra: Severity: major

  The SSL hardware acceleration card could not be found or initiated. This will cause the VPN Gateway to run with degraded performance.

- Name: hsm_not_logged_in Sender: <IP>, <Token> Cause: reboot Extra: "Card<Token> " Severity: critical

  After a reboot, login to the HSM card is required.

Comments? infodev@avaya.com

- Name: hsm_tampered_with Sender: <IP>, <Token> Cause: hsm_detected Extra: "Card<Token> " Severity: critical
- Name: slave_not_starting Sender: <IP>, <SlaveNo> Cause: start_error | connect_timeout | fdsend | nothidden | name_resolv | nodename_occupied Extra:" Severity: warning

  The portal handling subsystem cannot be started.

When an alarm is cleared, one of the following messages are sent:

Alarm Cleared Name="<Name>" Id="<ID>" Sender="<Sender>" Alarm Cleared Id="<ID>"

EVENT

Events are sent at the NOTICE syslog level. They are formatted according to the following pattern:

Name: <Name> Sender: <Sender> Extra: <Extra>

- Name: partitioned_network Sender and Extra is lower level information.

  Sent to indicate that a VPN Gateway is recovering from a partitioned network situation.
- Name: ssi_mipishere Sender: ssi Extra: <IP>

  Tells that the MIP (management IP address) is now located at the VPN Gateway with the <IP> host IP address.
- Name: license_expire_soon Sender: <IP>

  Indicates that the loaded (demo) license at the <IP> VPN Gateway expires within 7 days.
- Name: aaa_license_exhausted Sender: <IP>:<VPNIndex> Extra: ssl | IPsec

  This event is sent when the VPN has run out of SSL or IPsec user licenses. A hysteris mechanism is used so that no more than one event per hour is sent for one VPN.

  If <VPNIndex> is 0, the globally shared license was exhausted.
- Name: software_configuration_changed Sender: system Extra: software release version <VSN> <Status> Indicates that release <VSN> (version) has been <Status> (unpacked/ installed/permanent).
- Name: software_release_copying Sender: <IP> Extra: copy software release <VSN> from other cluster member

  Indicates that <IP> is copying the release <VSN> from another cluster member.
- Name: software_release_rebooting Sender: <IP> Extra: reboot with release version <VSN>

Indicates that a VPN Gateway (<IP>) is rebooting on a new release (that is, a VPN Gateway that was not up and running during the normal installation is now catching up).

- Name: license_expired Sender = <IP>

  Indicates that the demo license loaded at host <IP> has expired. Check the loaded licenses with **`/cfg/sys/cur`**.

- Name: audit Sender: CLI Extra: Start <session> <details> Update <session> <details> Stop <session> <details>

  Sent when a CLI system administrator enters, exits or updates the CLI if audit logging is enabled using the **`/cfg/sys/adm/audit/ena`** command.

Traffic Processing Messages

The Traffic Processing Subsystem messages are divided into these categories:

- CRITICAL
- ERROR
- WARNING
- INFO

CRITICAL

- DNS alarm: all dns servers are DOWN

All DNS servers are down. The VPN Gateway cannot perform any DNS lookups.

ERROR

- internal error: <no>

  An internal error occurred. Contact support with as much information as possible to reproduce this message.

- javascript error: <reason> for: <host><path>

  JavaScript parsing error encountered when parsing content from <host><path>. This could be a problem in the AVG JavaScript parser, but most likely a syntactical error in the JavaScript on that page.

- vbscript error: <reason> for: <host><path>

Comments? infodev@avaya.com

VBScript parsing error encountered when parsing content from <host><path>. This could be a problem in the AVG VBScript parser, but most likely a syntactical error in the VBScript on that page.

- jscript.encode error: <reason>

  Problem encountered when parsing an encoded JavaScript. It may be a problem with the JavaScript parser in the AVG or it could be a problem on the processed page.

- css error: <reason>

  Problem encountered when parsing an style sheet. It may be a problem with the css parser in the AVG or it could be a problem on the processed page.

- Failed to syslog traffic :<reason> -- disabling traf log

  Problem occurred when the AVG tried to send traffic logging syslog messages. Traffic syslogging was disabled as a result.

- www_authenticate: bad credentials

  The browser sent a malformed WWW-Authenticate: credentials header. Most likely a broken client.

- http error: <reason>, Request="<method> <host><path>"

  A problem was encountered when parsing the HTTP traffic. This is either an indication of a non-standard client/server or an indication that the AVG's HTTP parser has gotten out of sync due to an earlier non-standard transaction from the client or server on this TCP stream.

- http header warning cli: <reason> (<header>)

  The client sent a bad HTTP header.

- http header warning srv: <reason> (<header>)

  The server sent a bad HTTP header.

- unknown WWW-Authenticate method, closing

  Backend server sent unknown HTTP authentication method.

- failed to parse Set-Cookie <header>

  The AVG got a malformed Set-Cookie header from the backend web server.

- failed to locate corresponding portal for portal authenticated http server

  Portal authentication has been configured for an http server, but no portal using the same VPN can be found. Make sure that there is a portal running using the same VPN id.

- Bad IP:PORT data <line> in hc script

  Bad ip:port found in health check script. Reconfigure the health script. This should normally be captured earlier by the CLI.

- Bad regexp (<expr>) in health check

Bad regular expression found in health check script. Reconfigure. This should normally be captured earlier by the CLI.

- Bad script op found <script op>

  Bad script operation found in health check script. Reconfigure. This should normally be captured earlier by the CLI.

- Bad string found <string>

  Bad load balancing string encountered. This is normally verified by the CLI.

- Unable to use the certificate for <server nr>

  Unsuitable certificate configured for server #.

- The private key and certificate don't match for <server nr>

  Key and certificate does not match for server #. The certificate has to be changed.

- Unable to use client private key for <server #>

  Key for doing sslconnect is not valid. Reconfigure.

- Unable to find client private key for <server #>

  Key for doing sslconnect is not valid. Reconfigure.

- Unable to use client certificate for <server #>

  Certificate for doing sslconnect is not valid. Reconfigure.

- Failed to initialize SSL hardware

  Problem initializing SSL acceleration hardware. This will cause the VPN Gateway to run with degraded performance.

- Could not find SSL hardware.

  Failed to detect SSL acceleration hardware.

- Connect failed: <reason>

  Connect to backend server failed with <reason>

- SSL connect failed: <reason>

  SSL connect to backend server failed with <reason>

- html error: <reason>

  Error encountered when parsing HTML. Probably non-standard HTML.

- socks error: <reason>

  Error encountered when parsing the socks traffic from the client. Probably a non-standard socks client.

- socks request: socks version <version> rejected

Comments? infodev@avaya.com

Socks request of version <version> received and rejected. Most likely a non-standard socks client.

- Failed to log to CLI:<reason> -- disabling CLI log

  Failed to send troubleshooting log to CLI. Disabling CLI troubleshooting log.

- Can't bind to local address: <ip>:<port>: <reason>

  Problem encountered when trying to set up virtual server on <ip>:<port>.

- Ignoring DNS packet was not from any of the defined namesserver <ip>:<port>

  AVG received reply for non-configured DNS server.

- Proxy connect host name too long: <host>

  The host name is too long to perform proxy connect. Make the host name shorter or remove the domain from the proxy connect mapping.

- Certificate CRL handling errors:

  - failed to start auto-crl handling
  - <Cert#>: syntax error when parsing the CRL-URL
  - <Cert#>: automatic retrieval of HTTP-CRL failed - lookup failure <Host>
  - <Cert#>: automatic retrieval of HTTP-CRL failed - parse error
  - <Cert#>: auto-crl over HTTP failed, reason: <Reason>
  - <Cert#>: automatic retrieval of HTTP-CRL failed
  - <Cert#>: failed to create TFTP-CRL temp file
  - <Cert#>: parsing of TPFP-CRL URL failed
  - <Cert#>: automatic retrieval of TFTP-CRL failed - lookup failure <Host>
  - <Cert#>: failed to read TFTP-CRL temp file
  - <Cert#>: automatic retrieval of TFTP-CRL failed
  - <Cert#>: automatic retrieval of LDAP-CRL failed - lookup failure <Host>
  - <Cert#>: failed to contact LDAP server at <Host>
  - <Cert#>: no CRL (1) found at LDAP server
  - <Cert#>: CRL authentication failed
  - <Cert#>: no CRL (2) found at LDAP server
  - <Cert#>: no CRL (3) found at LDAP server
  - <Cert#>: no CRL passwd found
  - <Cert#>: no CRL filter was found
  - <Cert#>: no CRL interval found for cert

- <Cert#>: CRL revocation failed - <Reason>

WARNING

- TPS license limit (<limit>) exceeded

  The transactions per second (TPS) limit has been exceeded.

- No PortalGuard license loaded: VPN <id> *will* use portal authentication

  The PortalGuard license has not been loaded on the VPN Gateway but **`/cfg/vpn # /server/portal/authenticate`** is set to

  `off`

  .

- No Secure Service Partitioning loaded: server <id> *will not* use interface <n>

  The Secure Service Partitioning license has not been loaded on the VPN Gateway but the server is configured to use a specific interface.

- License expired

  The loaded (demo) license on the VPN Gateway has expired. The VPN Gateway now uses the default license.

- Server <id> uses default interface (interface <n> not configured)

  A specific interface is configured to be used by the server but this interface is not configured on the VPN Gateway.

- IPSEC server <id> uses default interface (interface <n> not configured)

  A specific interface is configured to be used by the IPsec server but this interface is not configured on the VPN Gateway.

- Certificate CRL handling warnings:

  - <Cert#>: no CRL-URL specified
  - invalid escape sequence in DN, ignoring...
  - <Cert#>: Ambiguous CRL configuration, all usage of certificate <Cert> does not bind to the same interface and/or DNS environment - using gateway <Gateway> settings

INFO

- gzip error: <reason>

  Problem encountered when processing compressed content.

- gzip warning: <reason>

Comments? infodev@avaya.com

Problem encountered when processing compressed content.

- accept() turned off (<nr>) too many fds

  The VPN Gateway has temporarily stopped accepting new connections. This will happen when the VPN Gateway is overloaded. It will start accepting connections once it has finished processing its current sessions.

- No cert supplied by backend server

  No certificate supplied by backend server when doing SSL connect. Session terminated to backend server.

- No CN supplied in server cert <subject>

  No CN found in the subject of the certificate supplied by the backend server.

- Bad CN supplied in server cert <subject>

  Malformed CN found in subject of the certificate supplied by the backend server.

- Shutting sslproxy down.

  Traffic subsystem has been stopped.

- Restarting proxy due to <reason>

  Traffic subsystem restarted due to <reason>

- DNS alarm: dns server(s) are UP

  At least one DNS server is now up.

- HC: backend <ip>:<port> is down

  Backend health check detected backend <ip>:<port> to be down.

- HC: backend <ip>:<port> is up again

  Backend health check detected backend <ip>:<port> to be up.

Startup Messages

The Traffic Processing Subsystem Startup messages only include the INFO category.

INFO

- HSM mode: <mode>

  Hardware Security Mode <mode>.

- Disabling transparent proxy, non-compatible with pooling

Transparent proxy mode is disabled due to pooling being enabled (startup message).

- Set CSWIFT as default

  Using CSWIFT SSL hardware acceleration. (startup message).

- Using <hwtype> hardware

  Using <hwtype> hardware for SSL acceleration. (startup message)

- Loaded <ip>:<port>

  Initializing virtual server <ip>:<port>.

- Because we use clicerts, force adjust totalcache size to: <size> per server that use clicerts

  Generated if the size of the SSL session cache has been modified.

- No more than <nr> backend supported

  Generated when more than the maximum allowed backend servers have been configured.

- TPS license limit: <limit>

  TPS limit set to <limit>

- No TPS license limit

  Unlimited TPS license used.

- Started ssl-proxy

  Traffic subsystem started.

- Found <size> meg of phys mem

  Amount of physical memory found on system.

Configuration Reload Messages

The Traffic Subsystem Configuration Reload messages only include the INFO category.

INFO

- reload cert config start

  Starting reloading of certificates.

- reload cert config done

  Certificate reloading done.

- reload configuration start

Comments? infodev@avaya.com

Virtual server configuration reloading start.

- reload configuration network down

  Accepting new sessions are temporarily put on hold.

- reload configuration network up

  Resuming accepting new sessions after loading new configuration.

- reload configuration done

  Virtual server configuration reloading done.

AAA Subsystem Messages

The AAA (Authentication, Authorization and Accounting) subsystem messages are divided into these categories:

- ERROR
- WARNING
- INFO

ERROR

LDAP backend(s) unreachable Vpn=\"<id>\" AuthId=\"<authid>\"

In case LDAP server(s) cannot be reached when a user tries to login to the Portal.

WARNING

Host <host ip> has been down too long: is no longer accounted for in the license pool.

The host has been down too long (more than 30 days) and is no longer accounted for in the license pool.

INFO

Host <host ip> is up: accounted for in the license pool.

A host that has been down too long is up again and is now sharing its licenses in the license pool.

Log functionality

Messages listed are generated if the CLI command **`/cfg/vpn #/adv/log`** is enabled.

If the log value contains

`login`

, the following messages can be displayed:

- VPN LoginSucceeded Vpn="<id>" Method=<"ssl"|"ipsec"> SrcIp="<ip>" User="<user>" Groups="<groups>"
- VPN LoginSucceeded Vpn="<id>" Method=<"ssl"|"ipsec"> SrcIp="<ip>" User="<user>" Groups="<groups>" TunIP="<inner tunnel ip>"
- VPN AddressAssigned Vpn="<id>" Method=<"ssl"|"ipsec"> SrcIp="<ip>" User="<user>" TunIP="<inner tunnel ip>"
- VPN LoginFailed Vpn="<id>" Method=<"ssl"|"ipsec"> SrcIp="<ip>" [User="<user>"] Error=<error>
- VPN Logout Vpn="<id>" SrcIp="<ip>" User="<user>"

If the log value contains

`portal`

, the following messages can be displayed:

- PORTAL Vpn="<id>" User="<user>" Proto="<proto>" Host="<host>" Share="<share>" Path="<path>"

If the log value contains

`http`

, the following messages can be displayed:

- HTTP Vpn="<id>" Host="<host>" User="<user>" SrcIP="<ip>" Request="<method> <host> <path>"
- HTTP NotLoggedIn Vpn="<id>" Host="<host>" SrcIP="<ip>" Request="<method> <host> <path>"

If the log value contains

`socks`

, the following messages can be displayed:

- SOCKS Vpn="<id>" User="<user>" SrcIP="<ip>" Request="<request>"

  This message refers to the features on the Portal's Advanced tab.

If the log value contains

`reject`

Comments? infodev@avaya.com

, the following messages can be displayed:

- HTTP Rejected Vpn="<id>" Host="<host>" User="<user>" SrcIP="<ip>" Request="<method> <host> <path>"
- PORTAL Rejected Vpn="<id>" User="<user>" Proto="<proto>" Host="<host>" Share="<share>" Path="<path>"
- SOCKS Rejected Vpn="<id>" User="<user>" SrcIP="<ip>" Request="<request>"

IPsec Subsystem Messages

The IPsec subsystem messages are divided into these categories:

- ERROR
- WARNING
- NOTICE
- INFO

ERROR

There are several ERROR messages that may get sent from the IPsec subsystem. They all indicate internal errors and thus provide no meaningful information for troubleshooting.

WARNING

- CreateSession Failed with sessionId 0

  AAA returned failure for creating session.
- Can't find new IKE Profile %s received in Auth Reply

  AAA provided new IKE profile as received from RADIUS, but IKE does not have it.
- Log off notif for non-existing session id %u

  AAA notified about log-off for a non-existing session.
- Quick mode initiation to %s failed, error - %s

  Quickmode initiation failed.
- All credits are exhausted for Isakmp SA

  Maximum number of outstanding ISAKMP SA create requests have exceeded the limit.
- All credits are exhausted for IPsec SA

Maximum number of outstanding IPsec SA create requests have exceeded the limit.

- Ignoring unauthenticated informational message from %s

  Dropping message without the authentication hash.

- Dropping unprotected notify message %s from %s

  Dropping the clear-text notify message.

- IPsec Mobility is disabled. Roaming request denied.

  Dropping the roaming request. Mobility is disabled in the configuration.

- Malformed ADDRESS_CHANGE notify message received from %s

  Dropping invalid ADDRESS_CHANGE (Mobility) request.

- Message from %s dropped because SPI is not found

  Dropping message because SPI is not found.

- Ignoring request to roam from %s to %s due to invalid source. Expecting %s

  Dropping roam request message because mismatch in source in payload and header.

- Ignoring request to roam from %s to %s

  Dropping roam request because old and new source IP are same.

- Error in Diffie-Hellman Setup, group=%u

  Error in DH Setup.

- No IPsec encryption type selected for %s - terminating connection attempt

  IPsec encryption does not match with the configured value.

- Diffie-Hellman group mismatch for %s - terminating connection attempt

  Configured Diffie-Hellman Group does not match with the one that the peer requested.

- PFS is required but not provided by %s

  PFS (Perfect Forward Secrecy) is configured locally, but the peer does not provide it.

- No Secure Service Partitioning license loaded IPSEC server ~s *will not* use interface ~p

  Secure Service Partitioning license not loaded.

- IPsec server ~s uses default interface (interface ~p not configured)

  This indicates possible badly configured default gateways on some Secure Service Partitioning interface.

- Failed to allocate IP addr from empty pool

Comments? infodev@avaya.com

The IP address pool is empty and a login attempt was rejected due to not being able to allocate an IP address from the pool. Note that Net Direct clients also use IPs from the IP pool.

NOTICE

- Failed to decode client cert

  A client sent a bad client certificate which could not decoded/parsed.

- Bad clicert, Can't find issuer in clicert

  A client sent a bad client certificate which did not contain an issuer.

- Error while decoding certificate DER Id

  A client sent a certificate where the X509 Name portion could not be extracted from the certificate.

- Client cert %d revoked

  The client certificate with serial number %d was revoked and thus login failed.

- Ike not started due: No license

  If no licence can be found (such as on old ASA 310), IKE is not started.

INFO

- Using new IKE. IKE Profile %s received in Auth Reply.

  Received new IKE profile from AAA (received from RADIUS).

- ISAKMP SA Established with %s

  ISAKMP SA Established.

- IPsec SA Established with %s, IPComp %s, inbound CPI 0x%x

  IPsec SA Established.

- Closing earlier opened UDP Encap Socket for port : %d

  UDP Encap port number changed.

- Creating UDP Encap Socket for %d.%d.%d.%d/%d

  UDP Encap port number changed.

- Received Delete ISAKMP SA message from %s

  Received Delete ISAKMP SA message.

- Received Delete IPSEC SA message from %s

Received Delete IPsec SA message.

- Client %s rejected IPsec SA Proposal, so deleting ISAKMP SA

  Client rejected the IPsec SA proposal.

- Deleting the QM replaced by new rekeyed QM

  Deleting the old IPsec SA which has been replaced with the new rekeyed one.

- No response from %s for maximum retransmission attempts %d

  Maximum number of retransmission attempts reached.

- ike Connected successfully to erlang

  IKE daemon has started and connected to the registry database.

- revocation byte length: %d

  Loading certificate revocation list of length %d.

- Loaded ca certificate %s

  Loaded CA certificate with name %s. This certificate is used to verify client certificates.

- Loaded server cert %s

  Loaded server certificate with name %s. This certificate must be signed by a trusted CA in the client.

- Creating Ike Profile %s

  Creating/Loading a new IKE profile called %s.

- Updating Ike profile %s

  A CLI/BBI change in IKE profile %s forces an update of the profile.

- Deleting ike profile %s

  IKE profile %s has been deleted in the CLI or BBI.

- Creating tunnel profile %s

  Updating tunnel profile %s.

- Deleting tunnel profile %s

  Deleting tunnel profile %s.

- Bad clientcert, no matching ca cert found

  A client tried to login with a client certificate when the corresponding CA certificate was not loaded in IKE.

- failed rsa private encrypt

  Failure to encrypt data while signing with the CA certificate.

Comments? infodev@avaya.com

- Failed to certificate der encode

  Failed to der encode the CA certificate.

- Allocated IP .....

  An IP address was allocated from the IP pool.

- Returned IP .....

  An IP address was returned to the IP address pool.

Syslog Messages in Alphabetical Order

This section lists the syslog messages in alphabetical order.

Table 8: Syslog Messages in Alphabetical Order

Message	Severity	Type	Explanation
aaa_license_exhausted	EVENT	System Control	This event is sent when the VPN has run out of SSL or IPsec user licenses. A hysteris mechanism is used so that no more than one event per hour is sent for one VPN. If <VPNIndex> is 0, the globally shared license was exhausted.
accept() turned off (<nr>) too many fds	INFO	Traffic Processing	The VPN Gateway has temporarily stopped accepting new connections. This will happen when the VPN Gateway is overloaded. It will start accepting connections once it has finished processing its current sessions.

Message	Severity	Type	Explanation
All credits are exhausted for IPsec SA	WARNING	IPsec	Maximum number of outstanding IPsec SA create requests have exceeded the limit.
All credits are exhausted for Isakmp SA	WARNING	IPsec	Maximum number of outstanding ISAKMP SA create requests have exceeded the limit.
Allocated IP	INFO	IPsec	An IP address was allocated from the IP pool.
Application filesystem corrupt - reinstall required	CRITICAL	OS	Reinstall.
audit	EVENT	System Control	Sent when a CLI system administrator enters, enters, exits or updates the CLI if audit logging is enabled using the **`/cfg/sys/adm/audit /ena`** command.
Bad clicert, Can't find issuer in clicert	NOTICE	IPsec	A client sent a bad client certificate which did not contain an issuer.
Bad clientcert, no matching ca cert found	INFO	IPsec	A client tried to login with a client certificate when the corresponding CA certificate was not loaded in IKE.
Bad CN supplied in server cert <subject>	INFO	Traffic Processing	Malformed CN found in subject of the certificate supplied by the backend server.

Comments? infodev@avaya.com

Message	Severity	Type	Explanation
Bad IP:PORT data <line> in hc script	ERROR	Traffic Processing	Bad ip:port found in health check script. Reconfigure the health script. This should normally be captured earlier by the CLI.
Bad regexp (<expr>) in health check	ERROR	Traffic Processing	Bad regular expression found in health check script. Reconfigure. This should normally be captured earlier by the CLI.
Bad script op found <script op>	ERROR	Traffic Processing	Bad script operation found in health check script. Reconfigure. This should normally be captured earlier by the CLI.
Bad string found <string>	ERROR	Traffic Processing	Bad load balancing string encountered. This is normally verified by the CLI.
Can't bind to local address: <ip>:<port>: <reason>	ERROR	Traffic Processing	Problem encountered when trying to set up virtual server on <ip>:<port>.
Can't find new IKE Profile %s received in Auth Reply	WARNING	IPsec	AAA provided new IKE profile as received from RADIUS, but IKE does not have it.
Client %s rejected IPsec SA Proposal, so deleting ISAKMP SA	INFO	IPsec	Client rejected the IPsec SA proposal.

Message	Severity	Type	Explanation
Client cert %d revoked	NOTICE	IPsec	The client certificate with serial number %d was revoked and thus login failed.
Closing earlier opened UDP Encap Socket for port: %d	INFO	IPsec	UDP Encap port number changed.
Config filesystem corrupt	ERROR	OS	Possible loss of configuration. Followed by the message Config filesystem re-initialized - reinstall required or Config filesystem restored from backup.
Config filesystem corrupt beyond repair	EMERG	OS	The system cannot boot, but stops with a single-user prompt. Reinstall to recover.
Config filesystem re-initialized - reinstall required	CRITICAL	OS	Reinstall.
Config filesystem restored from backup	ERROR	OS	Loss of recent configuration changes.
Connect failed: <reason>	ERROR	Traffic Processing	Connect to backend server failed with <reason>.
copy_software_release_failed	ALARM (CRITICAL)	System Control	A VPN Gateway failed to install a software release while trying to install the same version as all other VPN Gateway(s) in the cluster. The failing

Comments? infodev@avaya.com

Message	Severity	Type	Explanation
			VPN Gateway tries to catch up with the other cluster members as it was not up and running when the new software version was installed.
Could not find SSL hardware.	ERROR	Traffic Processing	Failed to detect SSL acceleration hardware.
CreateSession Failed with sessionId 0	WARNING	IPsec	AAA returned failure for creating session.
Creating Ike Profile %s	INFO	IPsec	Creating/Loading a new IKE profile called %s.
Creating tunnel profile %s	INFO	IPsec	Updating tunnel profile %s.
Creating UDP Encap Socket for %d.%d.%d.%d/%d	INFO	IPsec	UDP Encap port number changed.
css error: <reason>	ERROR	Traffic Processing	Problem encountered when parsing an style sheet. It may be a problem with the css parser in the AVG or it could be a problem on the processed page.
Deleting ike profile %s	INFO	IPsec	IKE profile %s has been deleted in the CLI or BBI.
Deleting the QM replaced by new rekeyed QM	INFO	IPsec	Deleting the old IPsec SA which has been replaced with the new rekeyed one.
Deleting tunnel profile %s	INFO	IPsec	Deleting tunnel profile %s.

Message	Severity	Type	Explanation
Diffie-Hellman group mismatch for %s - terminating connection attempt	WARNING	IPsec	Configured DH Group does not match with the one that the peer requested.
Disabling transparent proxy, non-compatible with pooling	INFO	Startup	Transparent proxy mode is disabled due to pooling being enabled.
DNS alarm: all dns servers are DOWN	CRITICAL	Traffic Processing	All DNS servers are down. The VPN Gateway cannot perform any DNS lookups.
DNS alarm: dns server(s) are UP	INFO	Traffic Processing	At least one DNS server is now up.
Dropping unprotected notify message %s from %s	WARNING	IPsec	Dropping the clear-text notify message.
Error in Diffie-Hellman Setup, group=%u	WARNING	IPsec	Error in DH Setup.
Error while decoding certificate DER Id	NOTICE	IPsec	A client sent a certificate where the X509 Name portion could not be extracted from the certificate.
failed rsa private encrypt	INFO	IPsec	Failure to encrypt data while signing with the CA certificate.
Failed to allocate IP addr from empty pool	WARNING	IPsec	The IP address pool is empty and a login attempt was rejected due to not being able to allocate an IP address from the pool. Note that Net Direct clients

Comments? infodev@avaya.com

Message	Severity	Type	Explanation
			also use IPs from the IP pool.
Failed to decode client cert	NOTICE	IPsec	A client sent a bad client certificate which could not decoded/parsed.
Failed to der encode certificate	INFO	IPsec	Failed to DER encode the CA certificate.
Failed to initialize SSL hardware	ERROR	Traffic Processing	Problem initializing SSL acceleration hardware. This will cause the VPN Gateway to run with degraded performance.
failed to locate corresponding portal for portal authenticated http server	ERROR	Traffic Processing	Portal authentication has been configured for an http server, but no portal using the same VPN id can be found. Make sure that there is a portal running using the same VPN id.
Failed to log to CLI:<reason> -- disabling CLI log	ERROR	Traffic Processing	Failed to send troubleshooting log to CLI. Disabling CLI troubleshooting log.
failed to parse Set-Cookie <header>	ERROR	Traffic Processing	The AVG got a malformed Set-Cookie header from the backend web server.
Failed to syslog traffic:<reason> -- disabling traf log	ERROR	Traffic Processing	Problem occurred when the AVG tried to send traffic logging syslog messages. Traffic

Message	Severity	Type	Explanation
			syslogging was disabled as a result.
Failed to write to config filesystem	EMERG	OS	Probable hardware error. Reinstall.
Found <size> meg of phys mem	INFO	Startup	Amount of physical memory found on system.
gzip error: <reason>	INFO	Traffic Processing	Problem encountered when processing compressed content.
gzip warning: <reason>	INFO	Traffic Processing	Problem encountered when processing compressed content.
HC: backend <ip>:<port> is down	INFO	Traffic Processing	Backend health check detected backend <ip>:<port> to be down.
HC: backend <ip>:<port> is up again	INFO	Traffic Processing	Backend health check detected backend <ip>:<port> to be up.
Host <host ip> has been down too long: is no longer accounted for in the license pool.	WARNING	AAA	The host has been down too long (more than 30 days) and is no longer accounted for in the license pool.
Host <host ip> is up: accounted for in the license pool.	INFO	AAA	A host that has been down too long is up again and is now sharing its licenses in the license pool.

Comments? infodev@avaya.com

Message	Severity	Type	Explanation
HSM mode: <mode>	INFO	Startup	Hardware Security Mode <mode>.
hsm_not_logged_in	ALARM (CRITICAL)	System Control	After a reboot, login to the HSM card is required.
hsm_tampered_with	ALARM (CRITICAL)	System Control	The HSM card has been tampered with.
html error: <reason>	ERROR	Traffic Processing	Error encountered when parsing HTML. Probably non-standard HTML.
http error: <reason>, Request="<method> <host><path>"	ERROR	Traffic Processing	A problem was encountered when parsing the HTTP traffic. This is either an indication of a non-standard client/server or an indication that the AVG 's HTTP parser has gotten out of sync due to an earlier non-standard transaction from the client or server on this TCP stream.
http header warning cli: <reason> (<header>)	ERROR	Traffic Processing	The client sent a bad HTTP header.
http header warning srv: <reason> (<header>)	ERROR	Traffic Processing	The server sent a bad HTTP header.
HTTP NotLoggedIn Vpn="<id>" Host="<host>" SrcIP="<ip>"	INFO	AAA	The remote user was not logged in to the specified web server

Message	Severity	Type	Explanation
Request="<method> <host> <path>"			requested from the Portal.
HTTP Rejected Vpn="<id>" Host="<host>" User="<user>" SrcIP="<ip>" Request="<method> <host> <path>"	INFO	AAA	The remote user failed to access the specified web server requested from the Portal.
HTTP Vpn="<id>" Host="<host>" User="<user>" SrcIP="<ip>" Request="<method> <host> <path>"	INFO	AAA	The remote user has successfully accessed the specified web server requested from the Portal.
Ignoring DNS packet was not from any of the defined namesserver <ip>:<port>	ERROR	Traffic Processing	AVG received reply for non-configured DNS server.
Ignoring request to roam from %s to %s	WARNING	IPsec	Dropping roam request because old and new source IP are same.
Ignoring request to roam from %s to %s due to invalid source. Expecting %s	WARNING	IPsec	Dropping roam request message because mismatch in source in payload and header.
Ignoring unauthenticated informational message from %s	WARNING	IPsec	Dropping message without the authentication hash.
ike Connected successfully to erlang	INFO	IPsec	IKE daemon has started and connected to the registry database.

Comments? infodev@avaya.com

Message	Severity	Type	Explanation
Ike not started due: No license	NOTICE	IPsec	If no licence can be found (such as on old ASA 310), IKE is not started.
internal error: <no>	ERROR	Traffic Processing	An internal error occurred. Contact support with as much information as possible to reproduce this message.
IPsec Mobility is disabled. Roaming request denied.	WARNING	IPsec	Dropping the roaming request, the Mobility is disabled in configuration.
IPsec SA Established with %s, IPComp %s, inbound CPI 0x %x	INFO	IPsec	IPsec SA Established.
IPSEC server ~s uses default interface (interface ~p not configured)	WARNING	IPsec	This indicates possible badly configured default gateways on some Secure Service Partitioning interface.
IPSEC server <id> uses default interface (interface <n> not configured)	WARNING	Traffic Processing	A specific interface is configured to be used by the IPsec server but this interface is not configured on the VPN Gateway.
ISAKMP SA Established with %s	INFO	IPsec	ISAKMP SA Established.
isd_down	ALARM (CRITICAL)	System Control	A member of the AVG cluster is down. This alarm is only sent if the cluster contains

Message	Severity	Type	Explanation
			more than one VPN Gateway.
javascript error: <reason> for: <host><path>	ERROR	Traffic Processing	JavaScript parsing error encountered when parsing content from <host><path>. This could be a problem in the AVG JavaScript parser, but most likely a syntactical error in the JavaScript on that page.
jscript.encode error: <reason>	ERROR	Traffic Processing	Problem encountered when parsing an encoded JavaScript. It may be a problem with the JavaScript parser in the AVG or it could be a problem on the processed page.
LDAP backend(s) unreachable Vpn=\"<id>\" AuthId= \"<authid>\"	ERROR	AAA	Shown if LDAP server(s) cannot be reached when a user tries to login to the Portal.
license	ALARM (WARNING)	System Control	One or several VPN Gateways in the cluster do not have the same SSL VPN license (with reference to number of concurrent users).
license	ALARM (WARNING)	System Control	The (demo) license loaded to the local VPN Gateway expires

Comments? infodev@avaya.com

Message	Severity	Type	Explanation
			within 7 days. Check loaded licenses using the **/cfg/sys/cur** command.
license_expire_soon	EVENT	System Control	Indicates that the loaded (demo) license at the <IP> VPN Gateway expires within 7 days.
license_expired	EVENT	System Control	Indicates that the the demo license at host <IP> has expired. Check the loaded licenses with **/cfg/sys/cur**.
License expired	WARNING	Traffic Processing	The loaded (demo) license on the VPN Gateway has expired. The VPN Gateway now uses the default license.
Loaded <ip>:<port>	INFO	Startup	Initializing virtual server <ip>:<port>.
Loaded ca certificate %s	INFO	IPsec	Loaded CA certificate with name %s. This certificate is used to verify client certificates.
Loaded server cert %s	INFO	IPsec	Loaded server certificate with name %s. This certificate must be signed by a trusted CA in the client.
Log off notif for non-existing session id %u	WARNING	IPsec	AAA notified about log-off for a non-existing session.

Message	Severity	Type	Explanation
log_open_failed	ALARM (MAJOR)	System Control	The event log (where all events and alarms are stored) could not be opened.
Logs filesystem re-initialized	ERROR	OS	Loss of logs.
make_software_release_permanent_failed	ALARM (CRITICAL)	System Control	Failed to make a new software release permanent after being activated. The system will automatically revert to the previous version.
Malformed ADDRESS_CHANGE notify message received from %s	WARNING	IPsec	Dropping invalid ADDRESS_CHANGE (Mobility) request.
Message from %s dropped because SPI is not found	WARNING	IPsec	Dropping message because SPI is not found.
Missing files in config filesystem	ERROR	OS	Possible loss of configuration. Followed by the message "Config filesystem re-initialized - reinstall required" or "Config filesystem restored from backup".
No cert supplied by backend server	INFO	Traffic Processing	No certificate supplied by backend server when doing SSL connect. Session terminated to backend server.

Comments? infodev@avaya.com

Message	Severity	Type	Explanation
No CN supplied in server cert <subject>	INFO	Traffic Processing	No CN found in the subject of the certificate supplied by the backend server.
No IPsec encryption type selected for %s - terminating connection attempt	WARNING	IPsec	IPsec encryption does not match with the configured value.
No more than <nr> backend supported	INFO	Startup	Generated when more than the maximum allowed backend servers have been configured.

No PortalGuard license loaded: VPN <id> *will* use portal authentication	WARNING	Traffic Processing	The PortalGuard license has not been loaded on the VPN Gateway but
			`/cfg/vpn # / server/portal/ authenticate`
			is set to
			`off`
			.

No response from %s for maximum retransmission attempts %d	INFO	IPsec	Maximum number of retransmission attempts reached.
No Secure Service Partitioning license loaded IPSEC server ~s *will not* use interface ~p	WARNING	IPsec	Secure Service Partitioning licence not loaded.
No Secure Service Partitioning loaded: server	WARNING	Traffic Processing	The Secure Service Partitioning license has not been loaded on

Message	Severity	Type	Explanation
<id> *will not* use interface <n>			the VPN Gateway but the server is configured to use a specific interface.
No TPS license limit	INFO	Startup	Unlimited TPS license used.
partitioned_network	EVENT	System Control	Sent to indicate that a VPN Gateway is recovering from a partitioned network situation.
PFS is required but not provided by %s	WARNING	IPsec	PFS (Perfect Forward Secrecy) is configured locally, but the peer does not provide it.
PORTAL Rejected Vpn="<id>" User="<user>" Proto="<proto>" Host="<host>" Share="<share>" Path="<path>"	INFO	AAA	The remote user failed to access the specified folder/directory on the specified file server requested from the Portal's Files tab.
PORTAL Vpn="<id>" User="<user>" Proto="<proto>" Host="<host>" Share="<share>" Path="<path>"	INFO	AAA	The remote user has successfully accessed the specified folder/ directory on the specified file server requested from the Portal's Files tab.
Proxy connect host name too long: <host>	ERROR	Traffic Processing	The host name is too long to perform proxy connect. Make the host name shorter or remove the domain from the proxy connect mapping.

Comments? infodev@avaya.com

Message	Severity	Type	Explanation
Quick mode initiation to %s failed, error - %s	WARNING	IPsec	Quickmode initiation failed.
Rebooting to revert to permanent OS version	ERROR	OS	Happens after "Config filesystem re-initialized - reinstall required" or "Config filesystem restored from backup" if software upgrade is in progress (i.e. if failure at first boot on new OS version).
Received Delete IPSEC SA message from %s	INFO	IPsec	Received Delete IPsec SA message.
Received Delete ISAKMP SA message from %s	INFO	IPsec	Received Delete ISAKMP SA message.
reload cert config done	INFO	Config Reload	Certificate reloading done.
reload cert config start	INFO	Config Reload	Starting reloading of certificates.
reload configuration done	INFO	Config Reload	Virtual server configuration reloading done.
reload configuration network down	INFO	Config Reload	Accepting new sessions are temporarily put on hold.
reload configuration network up	INFO	Config Reload	Resuming accepting new sessions after loading new configuration.
reload configuration start	INFO	Config Reload	Virtual server configuration reloading start.

Message	Severity	Type	Explanation
Restarting proxy due to <reason>	INFO	Traffic Processing	Traffic subsystem restarted due to <reason>.
Returned IP	INFO	IPsec	An IP address was returned to the IP address pool.
revocation byte length: %d	INFO	IPsec	Loading certificate revocation list of length %d.
Root filesystem corrupt	EMERG	OS	The system cannot boot, but stops with a single-user prompt. fsck failed. Reinstall to recover.
Root filesystem repaired - rebooting	ERROR	OS	fsck found and fixed errors. Probably OK.
Server <id> uses default interface (interface <n> not configured)	WARNING	Traffic Processing	A specific interface is configured to be used by the server but this interface is not configured on the VPN Gateway.
Set CSWIFT as default	INFO	Startup	Using CSWIFT SSL hardware acceleration.
Shutting sslproxy down.	INFO	Traffic Processing	Traffic subsystem has been stopped.
Because we use clicerts, force adjust totalcache size to : <size> per server that use clicerts	INFO	Startup	Generated if the size of the SSL session cache has been modified.
single_master	ALARM (WARNING)	System Control	Only one master VPN Gateway in

Comments? infodev@avaya.com

Message	Severity	Type	Explanation
			the cluster is up and running.
slave_not_starting	ALARM (WARNING)	System Control	The portal handling subsystem cannot be started.
socks error: <reason>	ERROR	Traffic Processing	Error encountered when parsing the socks traffic from the client. Probably a non-standard socks client.
SOCKS Rejected Vpn="<id>" User="<user>" SrcIP="<ip>" Request="<request>"	INFO	AAA	The remote user failed to perform an operation by using one of the features available under the Portal's Advanced tab.
socks request: socks version <version> rejected	ERROR	Traffic Processing	Socks request of version <version> received and rejected. Most likely a non-standard socks client.
	INFO	AAA	The remote user has successfully performed an operation by using one of the features available under the Portal's Advanced tab.
software_configuration_changed	EVENT	System Control	Indicates that release <VSN> (version) has been <Status> (unpacked/ installed/ permanent).
software_release_copying	EVENT	System Control	Indicates that <IP> is copying the release

Message	Severity	Type	Explanation
			<VSN> from another cluster member.
software_release_rebooting	EVENT	System Control	Indicates that a VPN Gateway (<IP>) is rebooting on a new release (i.e. a VPN Gateway that was not up and running during the normal installation is now catching up).
ssi_mipishere	EVENT	System Control	Tells that the MIP (management IP address) is now located at the VPN Gateway with the <IP> host IP address.
SSL connect failed: <reason>	ERROR	Traffic Processing	SSL connect to backend server failed with <reason>.
ssl_hw_fail	ALARM (MAJOR)	System Control	The SSL hardware acceleration card could not be found or initiated. This will cause the VPN Gateway to run with degraded performance.
Started ssl-proxy	INFO	Startup	Traffic subsystem started.
System started [isdssl-<version>]	INFO	System Control	Sent whenever the system control process has been (re)started.
The private key and certificate don't match for <server nr>	ERROR	Traffic Processing	Key and certificate does not match for server #. The

Comments? infodev@avaya.com

Message	Severity	Type	Explanation
			certificate has to be changed.
TPS license limit (<limit>) exceeded	WARNING	Traffic Processing	The transactions per second (TPS) limit has been exceeded.
TPS license limit: <limit>	INFO	Startup	TPS limit set to <limit>.
Unable to find client private key for <server #>	ERROR	Traffic Processing	Key for doing sslconnect is not valid. Reconfigure.
Unable to use client certificate for <server #>	ERROR	Traffic Processing	Certificate for doing sslconnect is not valid. Reconfigure.
Unable to use client private key for <server #>	ERROR	Traffic Processing	Key for doing sslconnect is not valid. Reconfigure.
Unable to use the certificate for <server nr>	ERROR	Traffic Processing	Unsuitable certificate configured for server #.
unknown WWW-Authenticate method, closing	ERROR	Traffic Processing	Backend server sent unknown HTTP authentication method.
Updating Ike profile %s	INFO	IPsec	A CLI/BBI change in IKE profile %s forces an update of the profile.
Using <hwtype> hardware	INFO	Startup	Using <hwtype> hardware for SSL acceleration.
Using new IKE. IKE Profile %s received in Auth Reply.	INFO	IPsec	Received new IKE profile from AAA (received from RADIUS).
vbscript error: <reason> for: <host><path>	ERROR	Traffic Processing	VBScript parsing error encountered when parsing

Message	Severity	Type	Explanation
			content from <host><path>. This could be a problem in the AVG VBScript parser, but most likely a syntactical error in the VBScript on that page.
VPN AddressAssigned Vpn="<id>" Method=<"ssl"|"ipsec"> SrcIp="<ip>" User="<user>" TunIP="<inner tunnel ip>"	INFO	AAA	Source IP address for the connection between the VPN Gateway and the destination address (inner tunnel) has been allocated.
VPN LoginFailed Vpn="<id>" Method=<"ssl"|"ipsec"> SrcIp="<ip>" [User="<user>"] Error=<error>	INFO	AAA	Login to the VPN failed. The remote user's access method, client IP address and user name is shown.
VPN LoginSucceeded Vpn="<id>" Method=<"ssl"|"ipsec"> SrcIp="<ip>" User="<user>" Groups="<groups>"	INFO	AAA	Login to the VPN succeeded. The remote user's access method, client IP address, user name and group membership is shown.
VPN LoginSucceeded Vpn="<id>" Method=<"ssl"|"ipsec"> SrcIp="<ip>" User="<user>" Groups="<groups>" TunIP="<inner tunnel ip>"	INFO	AAA	Login to the VPN succeeded. The remote user's access method, client IP address, user name and group membership is shown as well as the IP address allocated to the connection

Comments? infodev@avaya.com

Message	Severity	Type	Explanation
			between the VPN Gateway and the destination address (inner tunnel).
VPN Logout Vpn="<id>" SrcIp="<ip>" User="<user>"	INFO	AAA	Remote user has logged out from the VPN.
www_authenticate: bad credentials	ERROR	Traffic Processing	The browser sent a malformed WWW-Authenticate: credentials header. Most likely a broken client.

Comments? infodev@avaya.com

Appendix D: License Information

OpenSSL License Issues

The OpenSSL toolkit stays under a dual license, that is, both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See the following for the actual license texts. Both licenses are actually BSD-style Open Source licenses. In case of any license issues related to OpenSSL contact openssl-core@openssl.org.

OpenSSL License Copyright© 1998-1999 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the preceding copyright notice, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the preceding copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright© 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved. This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape SSL. This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, and so on., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com). Copyright remains Eric Young's, and as such, any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted, provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the preceding copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)". The word "cryptographic" can be left out if the routines from the library being used are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code), you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. That is, this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

GNU General Public License

Version 2, June 1991

Copyright© 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work that contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The following Program , refers to any such program or work. A "work based on the Program" means either the Program or any derivative work under copyright law: that is, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification.") Each licensee is addressed as "you."

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1, preceding, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish in whole or in part that contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it (when started running for such interactive use in the most ordinary way) to print or display an announcement, including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty), and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: If the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to the work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2, preceding, provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 preceding on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party (for a charge no more than your cost of physically performing source distribution) a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2, preceding, on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accordance with Subsection b, preceding.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, because you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute, or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment, or allegation of patent infringement, or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable

under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system. It is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version," you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs in which distribution conditions are different, write to the author for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING, THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION.

12. IN NO EVENT, UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING, WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS.

Apache Software License, Version 1.1

Copyright (c) 2000 The Apache Software Foundation. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the preceding copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the preceding copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: "This product includes software developed by the Apache Software Foundation (http://www.apache.org/)". Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.

4. The names "Apache" and "Apache Software Foundation" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, contact apache@apache.org.

5. Products derived from this software may not be called "Apache", nor may "Apache" appear in their name, without prior written permission of the Apache Software Foundation.

THIS SOFTWARE IS PROVIDED "QAS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABIL>ITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information about the Apache Software Foundation, see http://www.apache.org/.

Portions of this software are based upon public domain software originally written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign.

Appendix E: HSM Security Policy

All information in this Appendix is Copyright 2001 Rainbow Technologies.

Rainbow Technologies CryptoSwift® HSM Cryptographic Accelerator

FIPS 140-1 Non-Proprietary Cryptographic Module Security Policy Hardware P/N 107316 Firmware version 5.6.27 Ver 25 7/29/01for Level 3 Overall Level 4 for Self-Test Validation

Scope

This document describes the security policy for the HSM cryptographic accelerator. It is to be used for the FIPS 140-1 validation process. The board is designed to attain a level 3 overall validation and a level 4 validation in the area of Self-Test. The following table describes the compliance level for each section of the FIPS 140-1 specification:

Cryptographic Modules:	Level 3
Module Interfaces:	Level 3
Roles and Services:	Level 3
Finite State Machine Model:	Level 3
Physical Security:	Level 3
Software Security:	Level 3
Operating System Security:	Level N/a
Cryptographic Key Management:	Level 3
Cryptographic Algorithms:	Level 3
EMI/EMC:	Level 3
Self-Tests:	Level 4

If changes are made to the design of the HSM, this document should be updated to incorporate the changes and reviewed by an NVLAP-accredited CMT lab.

2.0 Applicable Documents

FIPS PUB 140-1 Federal Information Processing Standard, Security Requirements for Cryptographic Modules. January, 11, 1994, U.S. Department of Commerce, National Institute of Standards and Technology

Derived Test Requirements for FIPS PUB 140-1, Security Requirements for Cryptographic Modules. FINAL, March 1995, Mitre for NIST Contract 50SBNIC6732

FIPS PUB 46-3 and FIPS PUB 81, for information about the Data Encryption Standard (DES), and Triple DES algorithm. U.S. Department of Commerce, National Institute of Standards and Technology

FIPS PUB 180-1, Secure Hash Algorithm (SHA-1), U.S. Department of Commerce, National Institute of Standards and Technology. ANSI Standard X9.17-1995, Financial Institution Key Management (Wholesale), American Banking Association, X9 Financial Services, American National Standards Institute

PKCS #1 RSA Cryptography Standard, Version 2.0, http://www.rsasecurity.com/ RSA Security .Inc

3.0 Overview

The HSM is a cryptographic module which is used to accelerate cryptographic processing for network based electronic commerce and other network based applications. The board has two modes. These are the non-FIPS140-1 mode and the FIPS140-1 mode. In the FIPS140-1 mode, the board can be used in servers to improve the performance associated with high rate signing operations. In the non-FIPS140-1 mode, the board can be used to accelerate RSA operations for SSL connections on web servers. Other uses are limited only by the creativity of applications developers who can write to standard API's such as Cryptoki (PKCS#11). The HSM is a PCI card. It has a serial port, a Universal Serial Bus (USB) port, and an LED. The board is shipped with four tokens. These tokens plug into the USB port. The first token is used for authenticating the Security Officer to the HSM. The second token is used to for authenticating the User. The third and fourth tokens are called "code tokens." One of these is held (controlled) by the Security Officer. The other held by the User. The code keys are used to move key parts (also known as "key shares") between two HSM boards. Key parts transferred by this mechanism are combined within the destination boards so that a shared secret can exist on one or more boards without having existed in plaintext outside of a family of HSM boards. The shared secret is a Key-Wrapping-Key. When two or more boards contain the same Key-Wrapping-Key, they are said to be in the same family. The Key-Wrapping-Key is used to encrypt other keys. These encrypted keys can then be transmitted between boards over untrusted paths under the control

of a Rainbow Technologies key management utility. This allows boards to share keys as be appropriate for load distribution or redundancy needs.

The key wrapping key also makes it possible for keys to be stored in encrypted form on backup tapes or hard drives for archival purposes. The keys encrypted with the Key-Wrapping-Key need never exist in plaintext form outside of an HSM. When an operator uses an HSM, he will be assisted by a key management utility. This utility will prompt the operator when it is time to plug a particular token into a particular HSM. A particular host system may contain one or more HSM's. So that there is no confusion, the key management utility will control an LED on each HSM to alert the operator to know where to insert a particular token. 1. The HSM can detect attempts to penetrate its cryptographic envelope. If it detects a tamper attempt, the HSM will erase all of the critical security parameters that it contains. The HSM is controlled through its PCI interface. Commands are entered through the PCI bus, and status is read from the PCI bus. Also, both plaintext and encrypted data is transmitted over the PCI interface. The serial port is disabled in the production version of the HSM. A primary function of the HSM is to securely generate, store, and use private keys (particularly for signing operations).

4.0 Capabilities

The HSM is capable of performing a wide variety of cryptographic calculations including DES, SHA-1, DSA, 3DES, RSA exponentiation, RC4 and HMAC. When in the FIPS 140-1 mode, the board can perform DES, 3DES, RSA Signatures, RSA Signature Verifications and SHA-1 functions. When in the non-FIPS 140-1 mode, the board can also perform the RSA exponentiation, RC4, MD5, HMAC (SHA-1 and MD5) and DSA. The RSA signature and verification implementation is compliant with the PKCS #1 standard. The following table describes how each cryptographic algorithm is used by our module while operating in the FIPS 140-1 Mode:

Algorithm	How it is used by the HSM module	Used in FIPS 140-1 Mode?
DES	The module provides services for encryption/decryption. As currently implemented, the plaintext key must be input through the PCI interface. Therefore, this algorithm is not accessible in the FIPS 140-1 Mode. The self-tests perform a known answer test on this algorithm in FIPS 140-1 Mode.	No
3DES	Used to generate Pseudo-random numbers using the X9.17 Appendix C PRNG algorithm for the purposes of key generation of RSA and 3DES keys. Encryption/decryption of every key stored in persistence storage within the module using the Master Key. Wrapping (encryption) of Private RSA Keys using the Key-Wrapping-Key for archival purposes. Unwrapping (decryption) of Private RSA Keys using the Key-Wrapping-Key for the purpose of restoring an archived key. Note: The 3DES	Yes

Algorithm	How it is used by the HSM module	Used in FIPS 140-1 Mode?
	Encrypt and Decrypt services are not available for this algorithm in FIPS mode because keys are entered in plaintext.	
RSA Signature/ Verification	Generation and verification of digital signatures using the RSA algorithm, in accordance with the PKCS #1 specification. Keys pairs of modulus size in the range 192 through 1024 bits, in 64 bit increments. Note: The message digest operation of the digital signature and verification function is performed outside of the cryptographic boundary for performance reasons. After the digest is computed outside the module, the module formats and pads the message digest according to the PKCS #1 standard and then uses the RSA algorithm to compute the digital signature.	Yes
SHA-1	Hashing of host-provided data. Hashing for the purpose of verifying the RSA digital signature of a firmware image. Hashing a 3DES key for the purpose of checking its integrity after it is split and then the corresponding shares combined.	Yes
MD5	The module provides services to compute an MD5 message digest. As this algorithm is not FIPS-approved, the corresponding services are not available in the FIPS 140-1 Mode.	No
HMAC (SHA-1)	The module provides a service to compute HMAC using SHA-1. As currently implemented, the service requires the MAC key to be input unencrypted through the PCI interface, and therefore this service is not available in the FIPS 140-1 Mode.	No
HMAC (MD5)	The module provides a service to compute HMAC using MD5. Because MD5 is not a FIPS-approved algorithm, this service is not available in the FIPS 140-1 Mode.	No
RC4	The module provides services for encryption/decryption with RC4. Because RC4 is not a FIPS-approved algorithm, the corresponding services are not available in the FIPS 140-1 Mode.	No
DSA	The module provides services for generating and verifying DSA signatures. As currently implemented, the private key for signature generation must be input through the PCI interface. Therefore, this algorithm is not available in the FIPS 140-1 Mode. Keys pairs of modulus size in the range 512 through 1024 bits, in 64 bit increments.	No

Comments? infodev@avaya.com

5.0 Physical Security

The board is designed to detect tampering attempts and will zeroize critical security parameters under a variety of prescribed circumstances. These circumstances include penetration of the module's cryptographic envelope. The cryptographic envelope consists of an opaque tamper resistant lid and circuit board, and will provide clear visual evidence of tampering. The lid and circuit board are joined to form a contiguous perimeter. This perimeter encloses module components responsible for the creation, storage and processing of critical security parameters. The boundary contains intricate serpentine patterns that are used to detect tamper attempts associated with a breach of the cryptographic envelope by drilling, sawing or removal of the tamper lid.

7.1 Module Interfaces

6.1 USB (Universal Serial Bus) Interface

This is the trusted interface of the HSM. It is used for communicating with iKey1000 tokens. Four tokens are shipped with each HSM. One will contain a pin used to authenticate the Security Officer. One will contain a pin used to authenticate the User. One will contain a key-part to be controlled by the Security Officer. One will contain a key-part to be controlled by the user. No secrets, key-parts or critical security parameters are contained within any of the tokens or within the HSM when these items are shipped from Rainbow Technologies.

6.2 Status LED (Light Emitting Diode) Interface

The LED can be in four possible states. These are off, green, orange and red. The meaning associated with each LED state is as follows:

LED State	Meaning
Off	Power off
Green	Board is on but idle
Orange	Board is in the self-test state or performing a crypto function
Red	Board is in the error state

The true state of the HSM will be obtainable from the status register which is read by the host over the PCI interface.

6.3 Serial Interface

The serial interface is disabled in the production version of the HSM board.

6.4 PCI Interface

This interface is used to provide data and commands to the HSM board. It is also used to read data and status from the HSM.

6.5 Backup Battery Interface

The Backup Battery Interface is used to provide backup power to the HSM. This gives the HSM the capability to maintain and protect secrets should PCI power become unavailable. The battery is continuously monitored by the HSM for a voltage low condition. This makes it possible to alert an operator. The operator may then replace the battery. This can be done without loss of critical security parameters as long as the battery is replaced when PCI power is present. If the battery is removed while PCI power is absent, all critical security parameters contained within the HSM will be erased.

6.6 PCI Power Interface

The PCI Power Interface will provide the power necessary to perform all other HSM functions.

7.1 Components

7.1 Bulk Crypto

This component performs cryptographic hashing and symmetric cryptographic operations.

Comments? infodev@avaya.com

7.2 Power Management and Tamper Detect

This component monitors battery voltage and the security envelope to detect conditions that will result in the zeroization of critical security parameters. Battery voltage is also monitored to determine when it is necessary to replace the battery.

7.3 FastMap Processor

This component contains a processor and internal SRAM. The processor executes the software that initially resides in Flash memory and is eventually loaded into the external SRAM (external to the FastMap Processor yet still within the cryptographic boundary). The FastMap Processor also contains large accumulators and a random number generator. The accumulators are necessary for the acceleration of public key cryptographic operations. The random number generator generates truly random numbers through a stochastic process. The output of this random number generator is used only for seeding the FIPS-approved ANSI X9.17 Appendix C pseudo-random number generator (PRNG). The output of the PRNG is used for generating 3DES and RSA keys, as well as outputting random numbers requested through the Generate Random Number service.

7.4 Flash

This component is non-volatile memory. The contents of Flash will maintain its state after PCI power and Battery power have been removed. The Flash contains the firmware that controls processing within the HSM. It also contains public keys and other information that are not considered dangerous if exposed (certificates, public keys, encrypted data, encrypted keys and hash values used for authentication).

7.5 SRAM

SRAM is Static Random Access Memory. This memory will be used to store plaintext data, ciphertext data, symmetric keys, asymmetric keys, intermediate values, and firmware after it has been loaded from Flash.

7.6 Real Time Clock/Battery Powered RAM (RTC/BBRAM)

This component is used to store values that are to be retained when PCI power is removed. This includes the master key (MK) that can be used to decrypt encrypted private keys and symmetric keys stored in Flash. The RTC is used to provide input to the key generation process so that it is consistent with FIPS 140-1 key generation requirements.

7.7 Programmable Logic Device (PLD)

This component embodies all additional logic necessary to interface components contained within the security envelope.

7.8 USB (Universal Serial Bus) Controller

This component allows the board to communicate with an iKey. The iKey is used to store a Personal Identification Number PIN that allows for user authentication, or to store key parts for moving keys from one HSM to another HSM.

7.9 Universal Asynchronous Receiver Transmitter (UART)

This component is disabled in the production version of the HSM board.

7.10 33MHz Clock

This circuitry generates a square wave to provide the primary system clock and to synchronize the various components of the HSM with the operation of the FastMap chip.

8.0 Definition of Security Relevant Data Items

The following are the security relevant data items in this module: Master Key (MK) = The 3DES3KEY key which encrypts all non-volatile critical security parameters that are stored within the module (in the flash). The master key is stored in the BBRAM, and is destroyed when power is removed from both the PCI interface and the battery, and by the tamper detection circuitry whenever tampering is detected. The master key is randomly generated when the board is initialized (the Security Officer role is created). Security Officer role PIN (SOPIN) = The SO role PIN is generated randomly when the board is initialized. It is written to an iKey token through the trusted USB interface. Refer to following section 9.2 for a description of how this PIN is used for authentication. User Role PIN (UserPIN) = The User Role PIN is generated randomly when the SO invokes the Create User service. It is written to an iKey token through the trusted USB interface. Refer to following section 9.2 for a description of how this PIN is used for authentication. Key-Wrapping-Key (KWK) = A 3DES3KEY key created by either the SO or User role for the purpose of wrapping private RSA keys. The Key-Wrapping-Key may be randomly generated using the Generate Key service, or may be entered into the module using the Combine Key service, which combines two key shares entered through the trusted USB interface. In the non-FIPS 140-1 mode, the Key-Wrapping-Key may also be created

through the Derive Key service. PRNG3DES Key (PRNGKey)= This 3DES2Key is used for seeding the X9.17 Pseudo-random Number Generator (PRNG). The PRNG 3DES Key is generated randomly using the hardware random number generator (RNG) within the FastMap processor. This key is generated every time a random number is needed for key generation or as a direct request through the Generate Random Number service. The PRNG 3DES EDE Key is destroyed after each PRNG is generated. RSA Public and Private Key Pair (SPK, VPK)= This RSA key pair is generated by either the SO or User role for the purpose generating RSA digital signatures through the RSA Sign service, or for verifying the same through the RSA Verify service. A key pair which is designated by the user who created it cannot be used for any other purpose such as key exchanges or encryption/decryption of data. The user may specify through Boolean attributes whether the private key may be used for Signature Generation and/or Data Decryption, and whether the public key may be used for Signature Verification and/or Data Encryption. Hence, a given key pair may be used for both signatures/verifications as well as data encryption/decryption. In FIPS 140-1 Mode, data encryption/decryption is not available. RSA Encryption/Decryption Public and Private Key Pair (EPK, DPK)= This key pair is generated by either the SO or User role for the purpose of encrypting and decrypting data. When creating this key pair, the user may specify through Boolean attributes whether the private key may be used for Signature Generation and/or Data Decryption, and whether the public key may be used for Signature Verification and/or Data Encryption. Hence, a given key pair may be used for both signatures/verifications as well as data encryption/decryption. Note that in the FIPS 140-1 Mode, although Encryption/Decryption key pairs may be generated, the RSA Encrypt and RSA Decrypt services are not available, and therefore, such keys are not usable in this mode. Key-Wrapping-Key Share (KWKShare) = Key share obtained by splitting the KWK into two shares with the Split Key service. Two corresponding shares may be combined with the Combine Key service to enter the KWK into the module.

9.0 Roles and Services

9.1 Roles

The HSM supports two roles. These are the User role and the Security Officer role. Each role has a username and an iKey ID that are selectable by the security officer. The module must be handled in a secure manner prior to initialization because authentication is not required to initialize the module. Cryptographic keys and user-defined data which is created by a specific authenticated user cannot be deleted or modified by another user, regardless of the role. For example, a specific user of the User role may not delete or modify keys or data created by a different user of either the User or SO roles. The SO and User roles cannot operate simultaneously. Only one authenticated user is allowed at a time.

9.1.1 User

The User role can perform cryptographic operations using private keys which are encrypted and stored in flash. The User role cannot create a user.

9.1.2 Security Officer

The Security Officer role can also perform cryptographic operations using private keys which are encrypted and stored in flash. Additionally, the Security Officer may create a user, update the HSM firmware, or command the HSM to "uninitialize."

9.2 Authentication

The HSM uses identity-based authentication to allow subjects to assume one of the two roles. Usernames are transmitted to the HSM over the PCI interface to identify the user. A corresponding personal identification number (SOPIN or UserPIN as described in section 8.0) is input to the HSM from an iKey token over the trusted USB interface. This PIN is hashed and compared with a hash value which is stored in flash and associated with the user's name on the HSM. If the two hash values match, the user is authenticated and assigned a role that is associated with the user's name. To increase security in case the iKey token is compromised, an iKey ID is used to unlock the plaintext PIN that is stored in the iKey. This plaintext iKey ID is input into the module in plaintext as part of the Login service. The module provides a SHA-1 of this iKey ID to the iKey token to unlock the PIN. Because the iKey ID does not authenticate the user to the module, but rather unlocks the plaintext PIN from the iKey, the iKey ID is not an SRDI.

9.3 Initialization

The HSM is shipped in an un-initialized state. At this point, it contains no private or secret keys. The Security Officer initializes the board. Performing this function generates an internally stored master key, and generates a random PIN, which is stored in the Security Officer's iKey token. Initialization also creates the Security Officer account and associates the SHA-1 hash of the random PIN with the Security Officer account.

9.4 User Creation

Once the board has been initialized, the Security Officer can create a User account. Creating the User account generates a random PIN, which is stored in the User's iKey token. The SHA-1 hash of this random PIN is associated with the User account.

9.5 Services

The following table describes which services can be performed by which role, and the SRDI(s) which each service accesses.

Service	FIPS140-1 Level 3 Mode			Non- FIPS140-1 Mode			
	Not authenticated	User Role	SO Role	Not authenticated	User Role	SO Role	SRDIs Accessed
Modular Exponentiation using CRT (note 3)	YES	YES	YES	YES	YES	Yes	None
Modular Exponentiation (note 3)	YES	YES	YES	YES	YES	YES	None
RSA Encrypt (note 8)	NO	NO	NO	NO	YES	YES	EPK (use)
RSA Decrypt (note 8)	NO	NO	NO	NO	YES	YES	DPK (use)
Digital Signature Standard Sign (note 1)	NO	NO	NO	YES	YES	YES	None
Digital Signature Standard Verification (note 1)	NO	NO	NO	YES	YES	YES	None
Self-test	YES	YES	YES	YES	YES	YES	None
Firmware Update	NO	NO	YES	NO	NO	YES	None
Generate Random Number	YES	YES	YES	YES	YES	YES	PRNGKey (create, destroy)
Get Configuration	YES	YES	YES	YES	YES	YES	None
Get Status	YES	YES	YES	YES	YES	YES	None
Verify Firmware	Image	NO	NO	YES	NO	NO	YES
SHA1 Hash	NO	YES	YES	YES	YES	YES	None
SHA1 HMAC (note 1)	NO	NO	NO	YES	YES	YES	None
MD5 Hash	NO	NO	NO	YES	YES	YES	None
MD5 HMAC (note 1)	NO	NO	NO	YES	YES	YES	None
DES Encrypt (note 1)	NO	NO	NO	YES	YES	YES	None
DES Decrypt (note 1)	NO	NO	NO	YES	YES	YES	None

Service	FIPS140-1 Level 3 Mode			Non- FIPS140-1 Mode			
	Not authenticated	User Role	SO Role	Not authenticated	User Role	SO Role	SRDIs Accessed
Triple DES Encrypt (note 1)	NO	NO	NO	YES	YES	YES	None
Triple DES Decrypt (note 1)	NO	NO	NO	YES	YES	YES	None
RC4 Encrypt (note 1)	NO	NO	NO	YES	YES	YES	None
RC4 Decrypt (note 1)	NO	NO	NO	YES	YES	YES	None
Encrypt SHA1 Hash (DES) (note 1)	NO	NO	NO	YES	YES	YES	None
Decrypt SHA1 Hash (DES) (note 1)	NO	NO	NO	YES	YES	YES	None
Encrypt SHA1 Hash (3DES) (note 1)	NO	NO	NO	YES	YES	YES	None
Decrypt SHA1 Hash (3DES) (note 1)	NO	NO	NO	YES	YES	YES	None
Encrypt MD5 Hash (RC4) (note 1)	NO	NO	NO	YES	YES	YES	None
Decrypt MD5 Hash (RC4) (note 1)	NO	NO	NO	YES	YES	YES	None
Generate and Return RSA Key Pair (note 4)	NO	NO	NO	YES	YES	YES	None
Generate and Store RSA Key Pair	NO	YES	YES	NO	YES	YES	PRNGKey (create and destroy), and create either or both of the following pairs: (SPK, VPK) or (EPK, DPK)
Store Public Object (Public RSA Key, user data object)	NO	YES	YES	NO	YES	YES	Enter and store: EPK or VPK
Store Vendor-Defined Data Object	YES	YES	YES	YES	YES	YES	None

Comments? infodev@avaya.com

Service	FIPS140-1 Level 3 Mode			Non- FIPS140-1 Mode			
	Not authenticated	User Role	SO Role	Not authenticated	User Role	SO Role	SRDIs Accessed
Store Private Object (Private RSA Key) (note 4)	NO	NO	NO	NO	YES	YES	Enter and Store: SPK or DPK
Get Public Object (RSA public key, user-defined data object)	NO	YES	YES	NO	YES	YES	Read: SPK or DPK
Get Vendor-Defined Data Object	YES	YES	YES	YES	YES	YES	None
Get Object Information by Object ID	YES	YES	YES	YES	YES	YES	None
Get Object Count	YES	YES	YES	YES	YES	YES	None
Get Object Information by Index	YES	YES	YES	YES	YES	YES	None
Get RSA Key Information by ID (modulus, exponent)	NO	YES	YES	NO	YES	YES	Read: VPK or EPK
Get RSA Key Information by Index (modulus, exponent)	NO	YES	YES	NO	YES	YES	Read: VPK or DPK
Change Object ID	NO	YES	YES	NO	YES	YES	None
Delete Object	NO	YES	YES	NO	YES	YES	Destroy selected key: KWK, SPK, VPK, EPK, DPK.
Delete All Objects	NO	YES	YES	NO	YES	YES	Destroy all keys: KWK, SPK, VPK, EPK, DPK
Initialize Card	YES	NO	NO	YES	NO	NO	MK (create), SOPIN (create and write to trusted path)

Service	FIPS140-1 Level 3 Mode			Non- FIPS140-1 Mode			
	Not authenticated	User Role	SO Role	Not authenticated	User Role	SO Role	SRDIs Accessed
Uninitialize Card (note 7)	NO	NO	YES	NO	NO	YES	Destroy all of the following: MK, SOPIN, UserPIN, KWK, SPK, VPK, EPK, DPK
User Login/Change PIN (note 5)	YES	NO	NO	YES	NO	NO	UserPIN (read from trusted interface)
Create User	NO	NO	YES	NO	NO	YES	UserPIN (create, write to trusted interface) interface)
User Logout	NO	YES	YES	NO	YES	YES	None
Derive Key (note 2)	NO	NO	NO	NO	NO	YES	KWK (create)
Wrap Key (note 4)	NO	YES	YES	NO	YES	YES	KWK (use), Wrap: SPK, DPK
Unwrap Key (note 4)	NO	YES	YES	NO	YES	YES	KWK (use), Unwrap: SPK, DPK
Modify Object	NO	YES	YES	NO	YES	YES	None
RSA Sign (note 4)	NO	YES	YES	NO	YES	YES	SPK (use)
RSA Verify	NO	YES	YES	NO	YES	YES	VPK (use)
Generate Key (note 6)	NO	YES	YES	NO	YES	YES	KWK (create)
Split Key	NO	YES	YES	NO	YES	YES	KWK (split), PRNGKey (create, destroy), Two KWKShares (created

Comments? infodev@avaya.com

Service	FIPS140-1 Level 3 Mode			Non- FIPS140-1 Mode			
	Not authenticated	User Role	SO Role	Not authenticated	User Role	SO Role	SRDIs Accessed
							and written to trusted interface)
Combine Key	NO	YES	YES	NO	YES	YES	KWK (created), two KWKShares (read from trusted interface)
Set LED State	YES	YES	YES	YES	YES	YES	None.

Note 1 =	The key for these commands is input through the PCI bus (data input interface)
Note 2 =	This is a PKCS 12 method for deriving a 3DES key from a password, salt and iteration count.
Note 3 =	The Exponentiation Using CRT and Exponentiation functions are generic math functions; all parameters are input through the PCI interface (data input interface).
Note 4 =	When operating in the FIPS140-1 mode, it is not possible for secret keys, private keys or critical security parameters to cross the PCI bus without being wrapped (encrypted) using the Key-Wrapping Key.
Note 5 =	User Login is the process that takes the board from an unauthenticated state to the authenticated state. Only one user may be authenticated at a particular time. Consequently, the User Login process cannot be started from the authenticated state. Nonetheless, the User Login process cannot be completed successfully without authentication.
Note 6 =	This command is used for generating the key-wrapping-key.
Note 7 =	When the board is in the zeroized state, it is possible to for an unauthenticated user to uninitialize the board.
Note 8 =	These operations must access stored cryptographic keys. The keys may not be input through the PCI interface.

10.0 Key Management

10.1 Key Generation

Random number generation for key generation is accomplished using the algorithm described by appendix C of ANSI standard X9.17. This algorithm will use a seed value V (from appendix C) that is generated by the random number generator in the FastMap chip. Using this algorithm ensures that the keys generated will be consistent with the requirements of FIPS 140-1. Performing the key generation in this manner will ensure that the generated keys will be random and that the process used for their construction will be compatible with FIPS 140-1 requirements. Continuous random number testing is performed on the output of the hardware RNG (in the Fastmap chip) as well as on the output of the FIPS-approved ANSI X9.17 PRNG which is seeded by the RNG. For both continuous tests, the block size of 64 bits.

10.2 Key Storage

Private keys, symmetric keys and other critical security parameters will be stored in plaintext within the security envelope in RAM. Private and symmetric keys may also be stored in Flash, but only when first 3DES3KEY encrypted with the Master Key (MK) of the board. BBRAM is used to store the Master Key.

10.3 Key Entry and Output

When in the FIPS 140-1 mode, private keys and symmetric keys can only cross the cryptographic boundary when 3DES3KEY encrypted with a Key-Wrapping-Key. The Key-Wrapping-Key is generated when the " Generate Key" command is received by the HSM. The command that is used to encrypt and output a private or symmetric key is the "Wrap Key" command. The command that is used to enter and decrypt a private or symmetric key is the "Unwrap Key" command.

10.4 Key Distribution

To distribute a Key-Wrapping-Key between devices, it is split into two parts. The two parts, when exclusively ORed together, generate the Key-Wrapping-Key. The key splitting occurs when the "Write Key Split" command is first issued by the Security Officer. This command will cause one of the key parts to be written to an iKey controlled by the Security Officer. The second key part is written to an iKey controlled by the User. The Security Officer must logout and the

Comments? infodev@avaya.com

User must login before the second "Write Key Split" can be performed. The two iKey tokens used for carrying key parts are labeled with the word "CODE". The two key parts are then physically carried by separate trusted individuals to another device. If this device is also an HSM, the two parts may loaded into it using the "Read Key Split" command. Similarly, this command must be issued twice, once for the Security Officer and once for the User. Separate authentications are required for each "Read Key Split" command. After the second "Read Key Split " command has been successfully completed the destination device will contain the same Key-Wrapping-Key as the originating device. Once two or more devices that contain the same Key-Wrapping-Key, they are said to be in the same family. Devices in the same family may share other secrets. Secrets are moved between devices under the control of a Rainbow Technologies key management utility. The key management utility runs on the host, and uses "Wrap Key" and "Unwrap" commands to move wrapped keys between devices in the same family.

10.5 Key Destruction

Critical security parameters including plaintext private keys, symmetric keys and intermediate values will be zeroized according to various conditions as described in Table 9: Key Destruction on page 231. It is also possible for the security officer to command the board to un-initialize, which causes the data stored in RAM, FLASH and BBRAM to be erased.

Table 9: Key Destruction

Tamper Detected	Voltage Applied		Storage		
	Battery	PCI	BRAM	RAM and Other	Flash
NO	YES	YES	Retained	Retained	Retained
NO	YES	NO	Retained	Erased	Retained
NO	NO	YES	Retained	Retained	Retained
NO	NO	NO	Erased	Erased	Retained
YES	YES	YES	Erased	Erased	Retained
YES	YES	NO	Erased	Erased	Retained
YES	NO	YES	Erased	Erased	Retained
YES	NO	NO	Erased	Erased	Retained

10.6 Key Archiving

Under the control of the Rainbow Technologies key management utility, it is also possible to archive keys. This may be done so that keys may be stored on backup media such as tape or hard drives. The Rainbow Technologies key management utility utilizes the "Wrap Key"

command to perform key archival. All archived keys are 3DES3KEY encrypted. Keys may only be archived and restored between devices in the same family.

11.0 Modes

The HSM has two operating modes. These are the FIPS140-1 mode and the non-FIPS140-1 mode. Before the HSM is initialized with the "Initialize Card" command, it is in the non-FIPS140-1 mode. This command has an input parameter that specifies the mode of the card after initialization. Once initialized, the board remains in one of the two modes. If one wishes to change the operating mode of the card, the card must first be uninitialized using the "Uninitialize Card" command. Then, the card can be initialized with a different operating mode. Uninitializing the card removes all secrets from the card.

11.1 FIPS 140-1 Mode

In the FIPS 140-1 mode, the board may only perform FIPS approved algorithms. These are as follows: DES 3DES ** SHA-1 RSA Sign RSA Verify See the table in services section to identify the conditions necessary for performing various HSM commands in the FIPS140-1 mode. No plaintext private or symmetric keys can cross the cryptographic boundary when the HSM is in the FIPS140-1 mode. **The 3DES algorithm is used to secure private or symmetric keys stored in flash and for the key wrapping and unwrapping functions.

11.2 Non-FIPS 140-1 Mode

In the non-FIPS140-1 mode, the user has greater flexibility in the types of algorithms that can be performed and the manner that keys are handled. For example, in the non-FIPS140-1 mode, the board can perform all the functions of the FIPS140-1 mode plus other functions like MD5 and RC4. In the non-FIPS140-1 mode, keys may cross the cryptographic boundary in plaintext form for certain operations (e.g. DES, RSA CRT exponentiation). It is still possible to store keys on the board so that they cannot be extracted. These non-extractable keys will be erased if a tamper attempt is detected. See the table in services section to identify the conditions necessary for performing various HSM commands in the non-FIPS140-1 mode.

12.0 Self-Tests

The following table describes all of the cryptographic self-tests performed by the HSM module. The following abbrethroughtion is used: KAT = Known Answer Test

Comments? infodev@avaya.com

Self-Test	FIPS 140-1 Mode	Non-FIPS 140-1 Mode	When performed
RSA Encrypt/ Decrypt and Sign/ Verify KATs	Yes	Yes	Power-up, Self-Test Service (ondemand)
DES KAT	Yes	Yes	Power-up, Self-Test Service (ondemand)
3DES KAT	Yes	Yes	Power-up, Self-Test Service (ondemand)
SHA-1 KAT	Yes	Yes	Power-up, Self-Test Service (ondemand)
DSA KAT	No	Yes	Power-up, Self-Test Service (ondemand)
MD5 KAT	No	Yes	Power-up, Self-Test Service (ondemand)
RC4 KAT	No	Yes	Power-up, Self-Test Service (ondemand)
RSA Key Generation Pairwise Consistency Test	Yes	Yes	Generate And Store RSA Key Pair Service, Generate And Return RSA Key Pair Service
Statistical Random Number Generator Tests (Monobit, Poker, Runs, Long Run)	Yes	Yes	Power-up, Self-Test Service (ondemand)
Continuous Random Number Generator Test	Yes	Yes	Whenever a pseudorandom number is generated: key generation, Generate Random Number Service
Firmware RSA Signature Verification Test	Yes	Yes	Power-up, Self-Test Service (ondemand), Firmware Update, Verify Firmware Image Service

13.0 Conclusion

The HSM provides FIPS 140-1 Level 3 cryptographic processing, acceleration and security for RSA signing and verifying functions. In the non-FIPS140-1 mode, it can also bulk data cryptographic algorithms for PKI certificate server, firewall and web server equipment. It is suitable for use in applications requiring up to 200 public key transactions per second where protecting critical security parameters is a high priority. Industries requiring this high level of

performance and security include (but are not limited to) banking, telecommunications, e-commerce, and medical services. In the area of self-test, the HSM provides capabilities consistent with FIPS 140-1 Level 4.

Comments? infodev@avaya.com

Appendix F: Definition of Key Codes

Syntax Description

When using the Telnet applet available under the Portal's Advanced tab, there is an option to specify a keymap URL that points to a key code definition file. If your application uses a different keyboard layout than the standard VT320, a key code definition file can be created and uploaded to the keymap URL. This appendix shows how to create the key code definition file. Almost all special keys can be defined according to the following syntax rule:

[SCA] KEY=STRING

The characters enclosed in [and] are optional. Only one of the characters **'S'** (SHIFT), **'C'** (CTRL) or **'A'** (ALT) may appear before KEY, which is a textual representation of the key you wish to redefine (F1, PGUP and so on.).

The new STRING to be sent when pressing the key should come after the equals character (=). Hash marks (#) in the file declare the line as a comment and will be ignored. The following examples explains the syntax in more detail:

Send the string "test" when pressing the F1 key:

```
F1 = test
```

On pressing Control + PGUP, send the string "pgup pressed":

```
CPGUP = pgup pressed
```

Redefine the key Alt + F12 to send an escape character:

```
AF12 = \\e
```

As can be seen, the string may contain special characters which may be escaped using the backslash (\).

Allowed Special Characters

The following table includes allowed special characters:

Note:

For some of the escape codes you need two backslashes, as these are specific javassh definitions not known by the Java Property mechanism.

Table 10: Allowed Special Characters

Special Character	Explanation
\\b	Backspace. This character is usually sent by the <- key (Backspace key).
\\e	Escape. This character is usually sent by the Esc key.
\n	Newline. This character will move the cursor to a new line. On UNIX systems, it is equivalent to carriage return + newline. Usually the Enter key send this character.
\r	Carriage Return. This key moves the cursor to the beginning of the line. In conjunction with Newline, it moves the cursor to the beginning of a new line.
\t	Tabulator. The tab character is sent by the TAB key and moves the cursor to the next tab stop defined by the terminal.
\\v	Vertical Tabulator. Sends a vertical tabulator character.
\\a	Bell. Sends a terminal bell character which should make the terminal sound its bell.
\\number	Inserts the character that is defined by this number in the ISO Latin1 character set. The number should be a decimal value.

Redefinable Keys

The following table explains which keys may be redefined. As explained earlier, each of the keys may be prefixed by a character defining the redefinition that occurs if it is pressed in conjunction with the SHIFT, CONTROL or ALT keys.

Table 11: Redefinable Keys

Key Representation	Remarks
F1-F20	The Function keys, that is, F1, F2 and so on. up to F20.
PGUP	The Page Up key.
PGDOWN	The Page Down key.
END	The End key.
HOME	The Home (Pos 1) key.

Comments? infodev@avaya.com

Key Representation	Remarks
INSERT	The Insert key.
REMOVE	The Remove key.
UP	The Cursor Up key.
DOWN	The Cursor Down key.
LEFT	The Cursor Left key.
RIGHT	The Cursor Right key.
NUMPAD0-NUMPAD9	The numbered Numeric keypad keys.
ESCAPE	The Escape key.
BACKSPACE	The Backspace key.
TAB	The Tab key.

Example of a Key Code Definition File

Following is an example of the

`keyCodes.at386`

key code definition file, created for an AT-386 Terminal.

```
#
F1=\\eOP
F2=\\eOQ
F3=\\eOR
F4=\\eOS
F5=\\eOT
F6=\\eOU
F7=\\eOV
F8=\\eOW
F9=\\eOX
F10=\\eOY
F11=\\eOZ
F12=\\eOA
#
# Shift F1 thru F10
#
SF1=\\eOp
SF2=\\eOq
SF3=\\eOr
SF4=\\eOs
SF5=\\eOt
SF6=\\eOu
SF7=\\eOv
SF8=\\eOw
SF9=\\eOx
SF10=\\eOy
SF11=\\eOz
SF12=\\eOa
#
# Other cursor movement keys
#
UP=\\e[A
DOWN=\\e[B
RIGHT=\\e[C
LEFT=\\e[D
#
INSERT=\\e[@
# REMOVE=\\177  #( hex 7F  /  Decimal 127  /  Octal  177  /
DEL Key)
#
HOME=\\e[H
PGDOWN=\\e[U
PGUP=\\e[V
END=\\e[Y
#
```


Comments? infodev@avaya.com

Appendix G: SSH host keys

SSH host keys serve much the same purpose as server certificates in SSL/TLS, i.e. they primarily allow clients to authenticate the server, protecting against e.g. "man in the middle" attacks. As with certificates, public/private key pairs are used. Unlike certificates, there is no public key infrastructure and no certificate authorities for the SSH host keys.

Instead, the security of SSH sessions depends on SSH clients keeping track of the public keys that should be used to authenticate different SSH server hosts, not silently accepting new keys from previously unknown server hosts, and refusing or at least strongly warning the user from proceeding with the connection if there is a key mismatch.

Methods for Protection

In many environments, it may be reasonable for a SSH client user to simply accept the key from a previously unknown remote server host when prompted by the client, but to achieve strict protection against a "man in the middle" attack against this very first connection, one of these methods can be used:

- Verifying the "fingerprint" (as displayed by the client) of the new remote host key by some out-of-band means (e.g. verbal communication with the server administrator).

  OR

- Pre-installing the remote host key (previously transferred by some out-of-band means) in the client's key storage, i.e. effectively making the remote host known even before the first connection.

The server administrator also needs to be able to generate new keys (e.g. at initial configuration, or in case the old ones are believed to be compromised), and the client user needs to be able to remove remote host keys that are no longer valid from the client's key storage (e.g. due to the server administrator having generated new keys).

The VPN Gateway

The VPN Gateway can act both as SSH server (when a user connects to the CLI using a SSH client) and as SSH client (when file or data transfers are initiated from the VPN Gateway using the SCP or SFTP protocols). The **`generate`** and **`show`** commands in the **`/cfg/sys/adm/sshkeys`** menu concern the former case, while the

```
knownhosts
```

menu concerns the latter.

The VPN Gateway supports the use of three different SSH host key types: SSH protocol version 1 always uses RSA keys, while for SSH protocol version 2, either RSA or DSA keys can be used. The RSA keys for version 1 differ in form from those for version 2, and are referred to as "RSA1".

Comments? infodev@avaya.com

Appendix H: Adding User Preferences Attribute to Active Directory

For the remote user to be able to store user preferences on the Avaya VPN Gateway (AVG), you need to add the *isdUserPrefs* attribute to Active Directory. This attribute will contain an opaque data structure, containing various information that the user may have saved during a Portal session.

This description is based on Windows 2000 Server and Windows Server 2003. Make sure that your account is a member of the Schema Administrators group.

Install All Administrative Tools (Windows 2000 Server)

1. Open the Control Panel and double-click **Add/Remove Programs**.
2. Select **Windows 2000 Administrative Tools** and click **Change**.
3. Click **Next** and select **Install All Administrative Tools**.
4. Follow the instructions on how to proceed with the installation.

Register the Schema Management dll (Windows Server 2003)

1. Click **Start** and select **Run**.
2. In the **Open** field, enter `regsvr32 schmmgmt.dll.`

   Note that there is a space between regsvr32 and schmmgmt.dll.
3. Click **OK**.

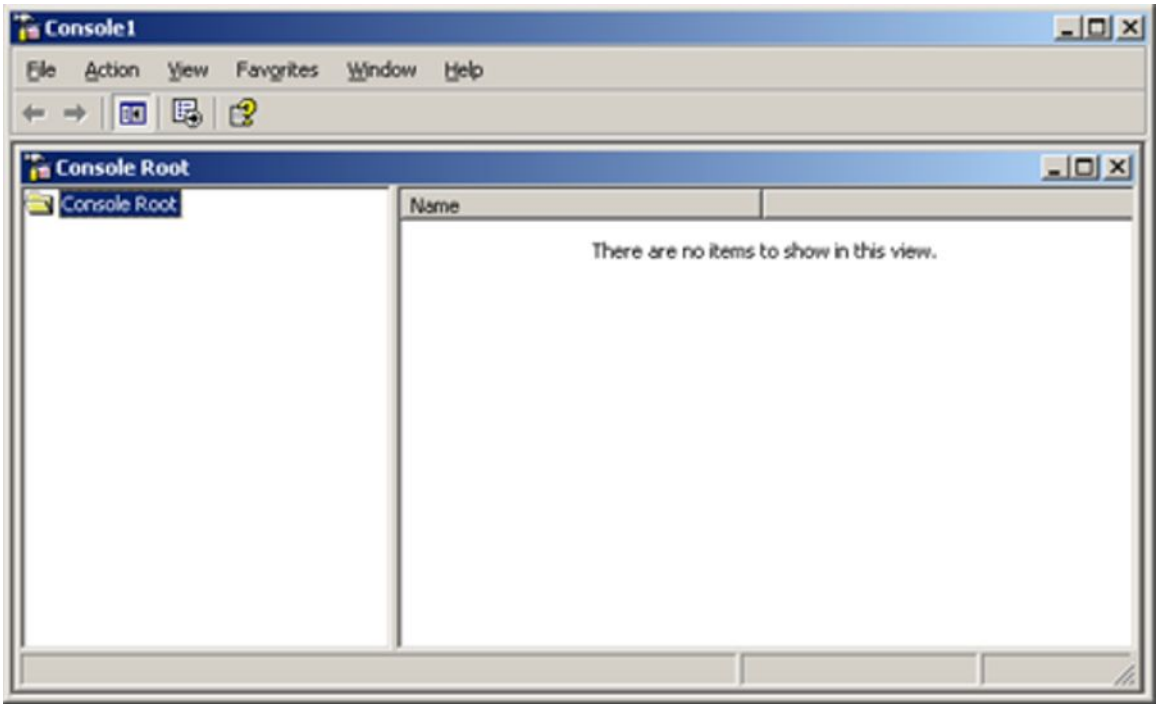
   This command will register schmmgmt.dll on your computer.

Add the Active Directory Schema Snap-in (Windows 2000 Server and Windows Server 2003)

1. Click **Start** and select **Run**.
2. On Windows 2000 Server, enter `mmc` in the **Open** field. On Windows Server 2003, enter `mmc /a` instead.

   Note that there is a space between `mmc` and `/a`.
3. Click **OK**.

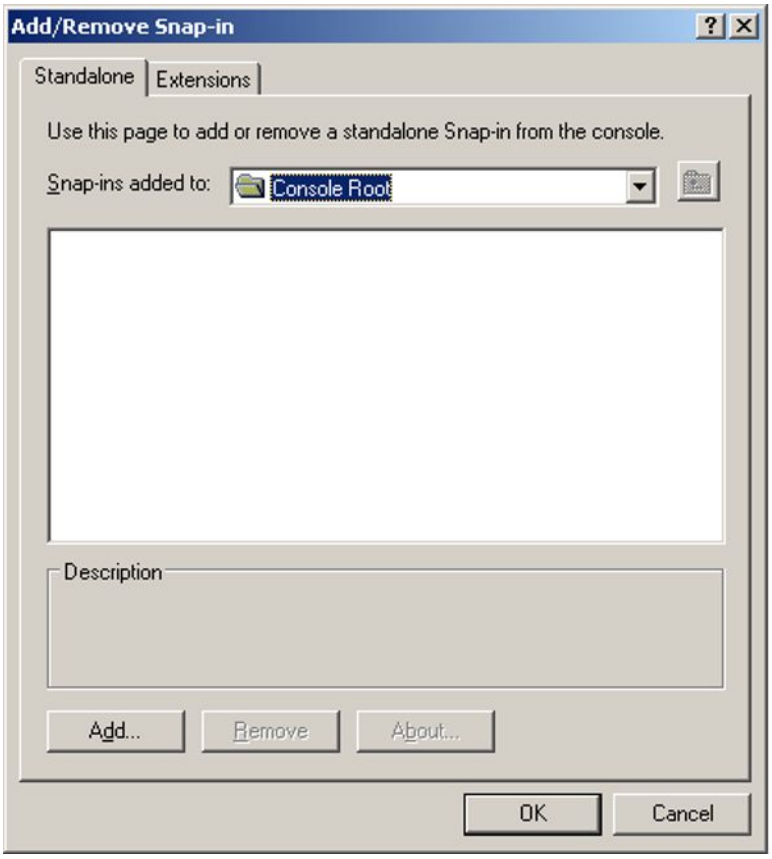
   The Console window is displayed.



4. On the **File** (Console) menu, select **Add/Remove Snap-in**.

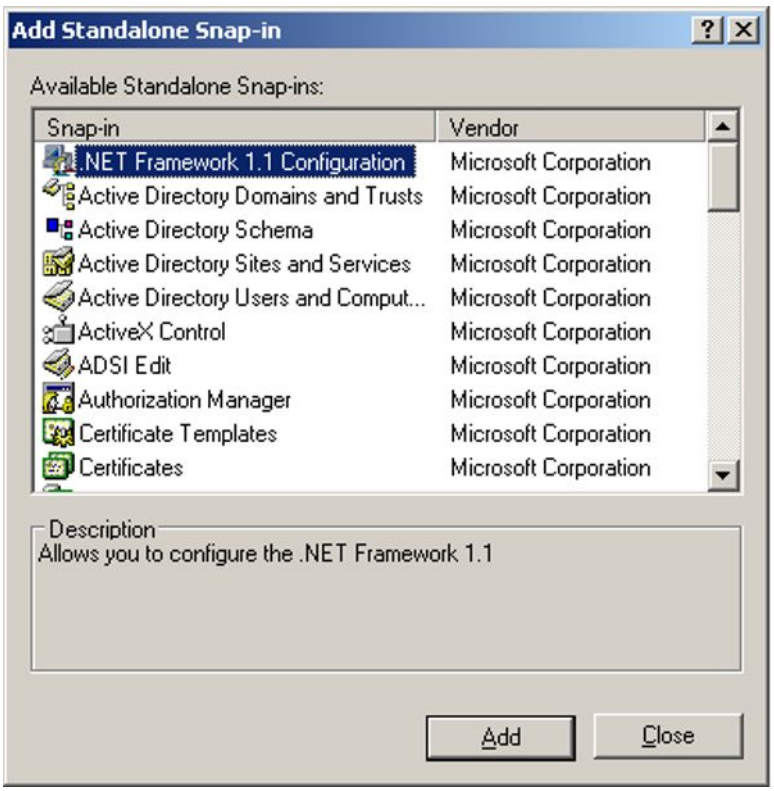
   The Add/Remove Snap-in window is displayed.

Comments? infodev@avaya.com



5. Click **Add**.

   The Add Standalone Snap-in window is displayed.



6. Under Snap-in, select **Active Directory Schema** and click **Add**.

   Active Directory Schema is added to the Add/Remove Snap-in window.
7. Click **Close** to close the Add Standalone Snap-in window.

   The Add/Remove Snap-in window is redisplayed.
8. Click **OK**.

   The Console window is redisplayed.
9. To save the console (including the Schema snap-in), go to the **File** (Console) menu and select **Save**.

   The Save As windows is displayed.
10. Save the console in the `Windows\System 32` root folder.
11. As file name, enter `schmmgmt.msc.`
12. Click **Save**.

Create a Shortcut to the Console Window

1. Right-click **Start**, and select **Open all Users**.
2. Double-click the **Programs and Administrative Tools** folders.

Comments? infodev@avaya.com

3. On the **File** menu, point to **New**, and then select **Shortcut**.

   The Create Shortcut Wizard is displayed.

4. In the Type the location of the item field, type `schmmgmt.msc.`
5. Click **Next**.

   The Select a Title for the Program page is displayed.

6. In the Type a name for this shortcut field, type `Active Directory Schema.`
7. Click **Finish**.

Permit Write Operations to the Schema (Windows 2000 Server)

To allow a domain controller to write to the schema, you must set a registry entry that permits schema updates.

1. In the Console window, on the left pane, right-click **Active Directory Schema**.
2. Select **Operations Master**.
3. Select the check box **The Schema may be modified on this Domain Controller**.
4. Click **OK**.

Create a New Attribute (Windows 2000 Server and Windows Server 2003)

To create the isdUserPrefs attribute, proceed as follows:

1. In the Console window, on the left pane, expand **Active Directory Schema** by clicking the plus (+) sign.

   The Attributes and Classes folders are displayed.

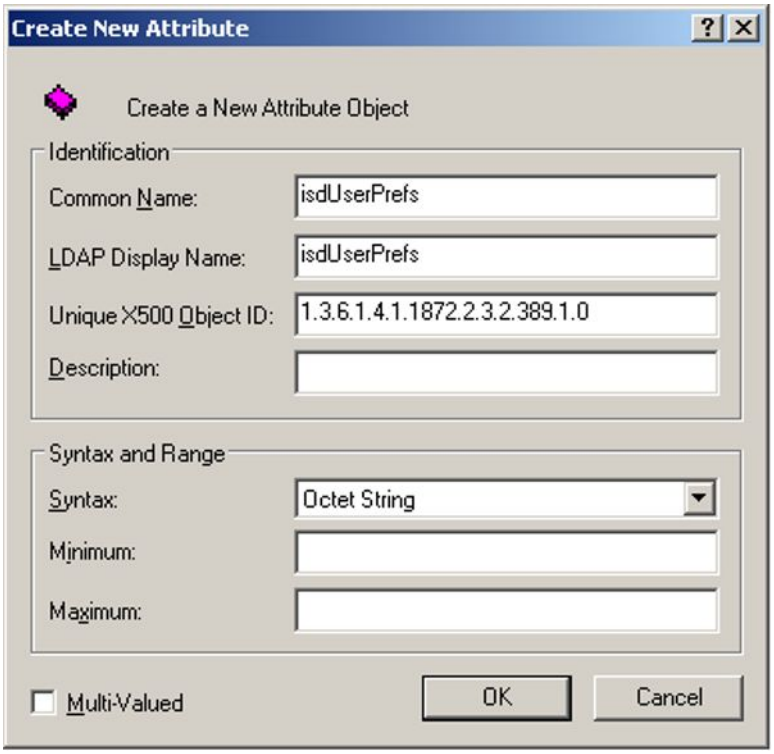
2. Right-click **Attributes**, point to **New** and select **Attribute**.

   You will now receive a warning that creating schema objects is a permanent operation and cannot be undone.

3. Click **Continue**.

   The Create New Attribute window is displayed.

4. Create the isdUserPrefs attribute as shown:



5. Click **OK**.

Create New Class

To create the avayaSSLOffload class, proceed as follows:

1. In the Console window, right-click **Classes**, point to **New** and select **Class**.

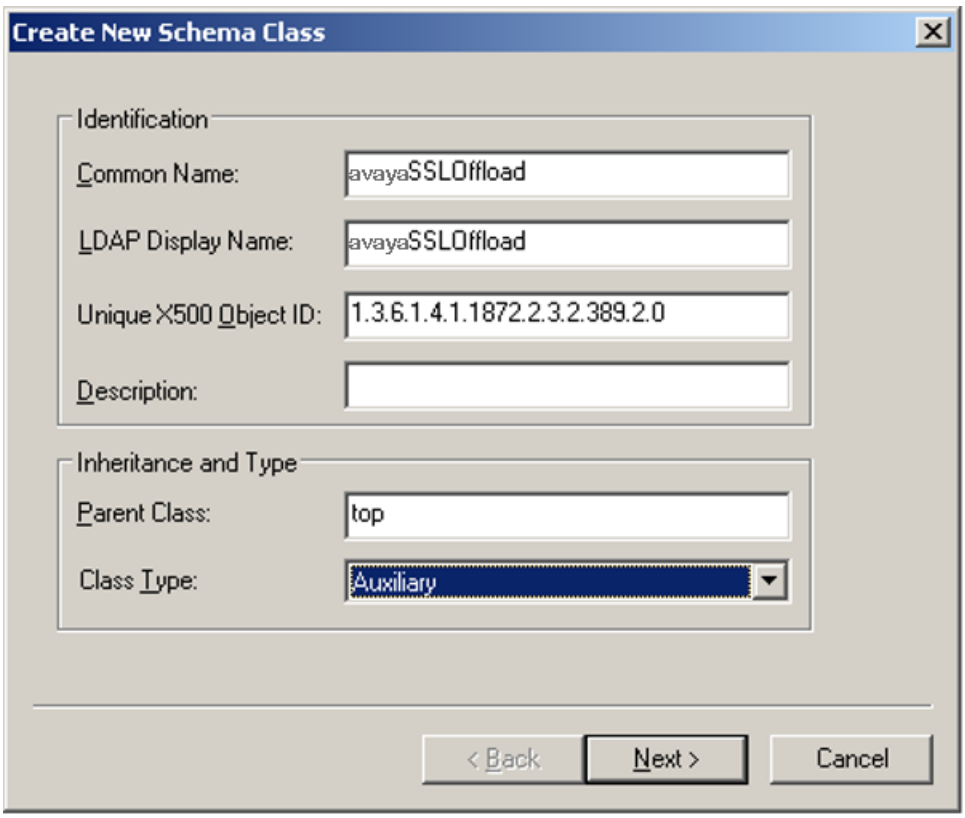
   You will now receive a warning that creating schema classes is a permanent operation and cannot be undone.

2. Click **Continue**.

   The Create New Schema Class window is displayed.

3. Create the avayaSSLOffload class as shown:

Comments? infodev@avaya.com

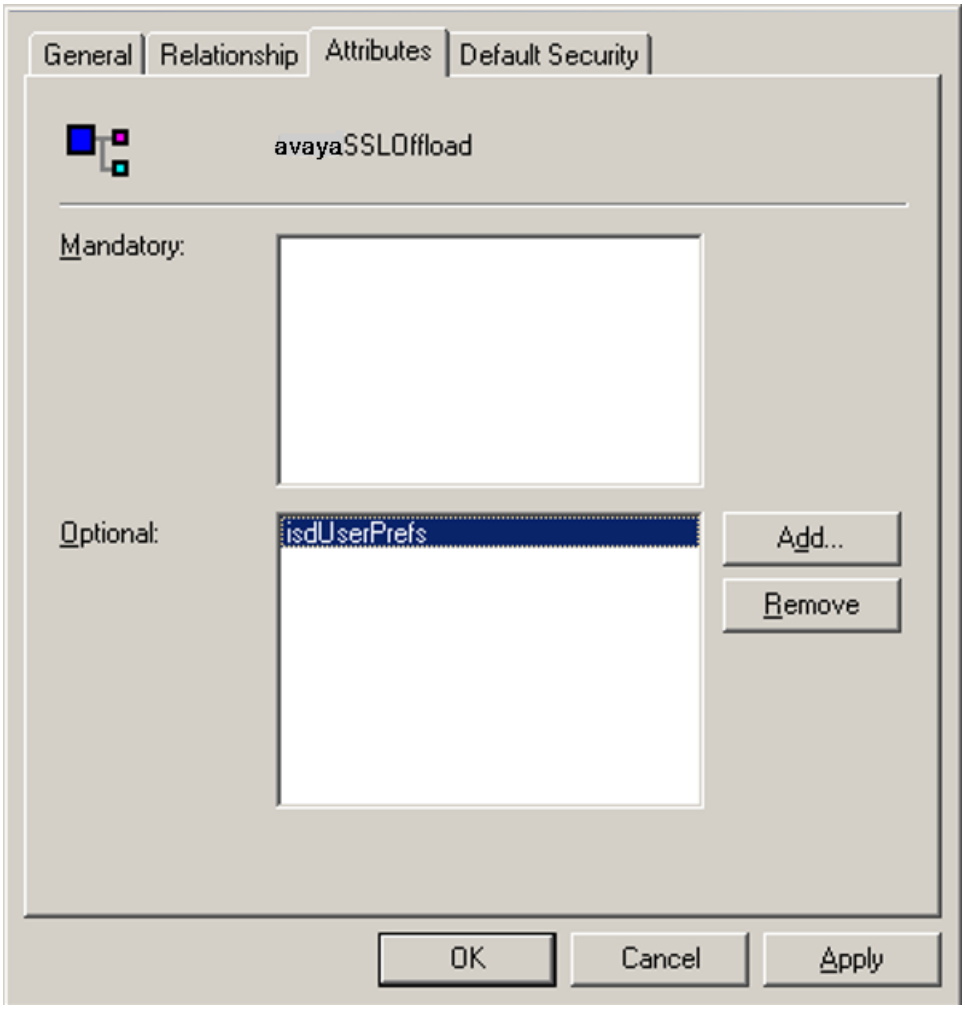


4. Click **Next**.
5. Click **Finish**.

Add isdUserPrefs Attribute to avayaSSLOffload Class

1. In the Console window, on the left pane, expand **Classes**.
2. Select the **avayaSSLOffload** class.
3. Right-click and select **Properties**.

   The Properties window is displayed.
4. Select the Attributes tab and click **Add**.
5. Add the **isdUserPrefs** attribute as optional.



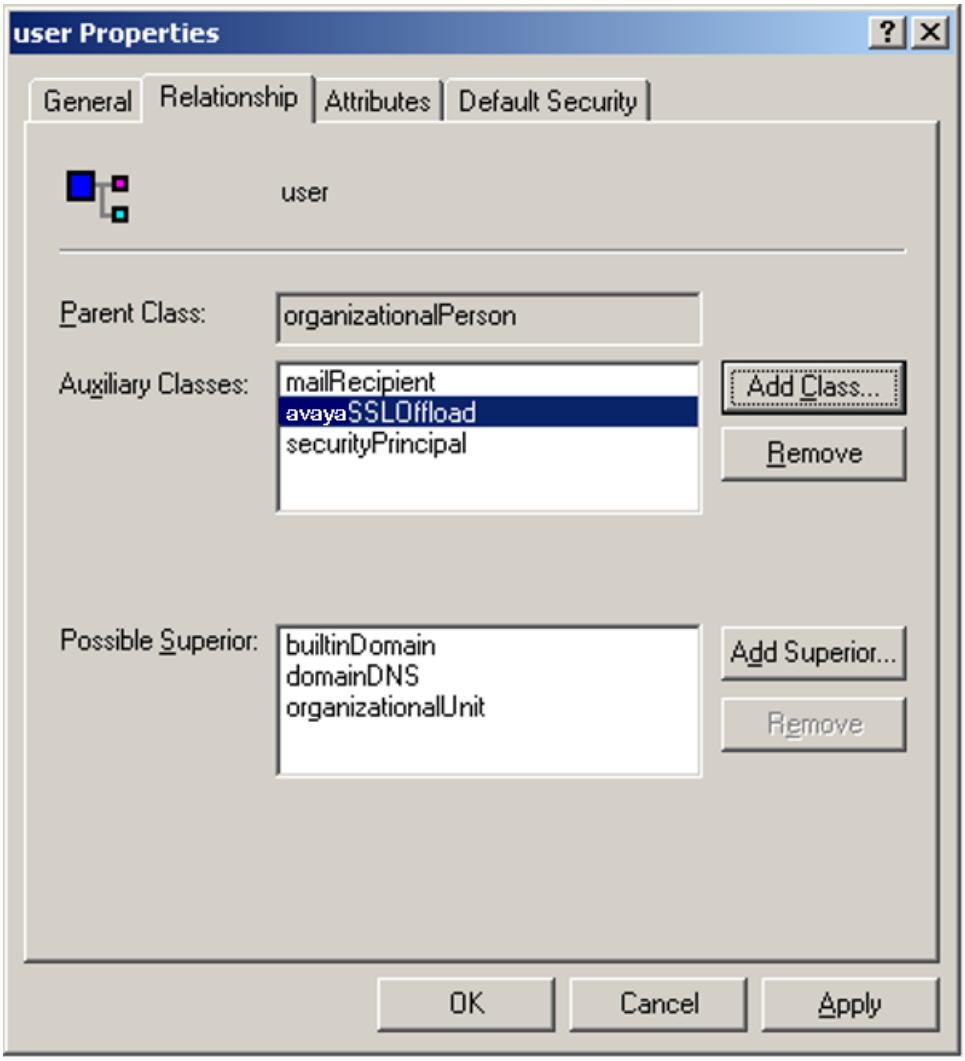
6. On the **Default Security (Security)** tab, set read/write permissions for the group that should have permission to write user preferences to the attribute.
7. Click **OK**.

Add the avayaSSLOffload Class to the User Class

1. In the **Console** window, on the left pane, expand **Classes** and select user.
2. Right-click and select **Properties**.

   The Properties window is displayed.
3. Select the **Relationship** tab.
4. Next to Auxiliary Classes, click **Add Class (Add)**.
5. Add the **avayaSSLOffload** class as an auxiliary class as shown:

Comments? infodev@avaya.com



6. Click **OK**.

   Once you have enabled the User Preferences feature on the VPN Gateway (using the CLI command **`/cfg/vpn #/aaa/auth #/ldap/enauserpre`** or the BBI setting User Preferences under **VPN Gateway>VPN# >Authentication->Auth Servers#(Ldap)** the remote user should now be able to store user preferences in Active Directory.

Comments? infodev@avaya.com

Appendix I: Using the Port Forwarder API

General

This appendix describes some of the tasks needed when using the Port Forwarder API. The JavaDoc will give you a more detailed view of the API.

The Port Forwarder API is used to provide tunnels through the Avaya VPN Gateway (AVG) without having to start any applets from the Portal. It can be used by any type of Java application or applet.

The tunnel specifications are set by defining a port forwarder in the CLI/BBI. It is then referred to when setting up the Port Forwarder API.

Note:

Defined applications are only started automatically if the port forwarder API is used by an applet.

The API and Demo application are available from the Portal. Example: **`https://vpn.example.com/avaya_cacheable/portforwarder.zip`**

The zip file contains both a signed and an unsigned version of the API along with javadoc documentation and a demo application with source code.

Creating a Port Forwarder

The Port Forwarder API is a collection of functions used to provide applications with the ability to send traffic through a previously defined port forwarder link. For instructions on how to configure a port forwarder link on the AVG Portal, see the chapter "Group Links" in the *Avaya Application Guide for VPN*.

To be able to use the Port Forwarder API, two URLs are needed:

- URL for the Portal login (called **`loginUrl`** in the following examples) Example: **`http://vpn.example.com/login_post.yaws?user=test&password=test&authmethod=default&url=`** The parameters are the same as if accessing the Portal through a web browser.
- URL for the actual port forwarder (called **`portForwarderUrl`** in the following examples) Example: **`http://vpn.example.com/link.yaws?t=custom&a=1&b=1&c=1`**

The parameters a, b and c in the second link point out the link according to:

a: VPN number b: Linkset number c: Link number

Demo Application

The Demo application is, in a simple way, showing how the Port Forwarder API is used. It can be run both as a regular application and by using the Java Web Start technology. It takes a couple of parameters needed to point out the Portal and link to use.

-vpnurl	The URL to the portal, e.g. **`https://vpn.example.com`**.
-linktype	The type of the link to use, for example "custom". The link type should be the same as defined in the CLI/BBI.
-vpn	The number of the VPN in the Portal, for example 1.
-linkset	The number of the linkset in the VPN, for example 1.
-link	The number of the link in the linkset, for example 1.

When run as a regular application, the arguments are simply passed on the command line:

```
java com.avaya.avg.demo.PortForwarderDemo -vpnurl https://
vpn.example.com -linktype custom -vpn 1 -linkset 1 -link 1
```

For Java Web Start, parameters are passed through the jnlp file. A template jnlp file is provided along with a corresponding html file. For information about Java Web Start, refer to http://java.sun.com/products/javawebstart.

A correct jnlp file corresponding to the preceding example look like this:

Comments? infodev@avaya.com

```
<?xml version="1.0" encoding="UTF-8"?>
<jnlp spec="1.0+"
    codebase="https://vpn.example.com/"
    href="PortForwarderDemo.jnlp">
  <information>
    <title>PortForwarder Demo</title>
    <vendor>Avaya </vendor>
    <description>Demonstration of PortForwarder API</description>
  </information>
  <offline-allowed/>
  <security>
    <all-permissions/>
  </security>
  <resources>
    <j2se version="1.4+" />
    <jar href="signed_portforwarderdemo.jar"/>
    <jar href="signed_portforwarder.jar"/>
  </resources>
  <application-desc main-class="com.avaya.avg.demo.PortForwarderDemo">
    <argument>-vpnurl</argument>
    <argument>https://vpn.example.com</argument>
    <argument>-linktype</argument>
    <argument>custom</argument>
    <argument>-vpn</argument>
    <argument>1</argument>
    <argument>-linkset</argument>
    <argument>1</argument>
    <argument>-link</argument>
    <argument>1</argument>
  </application-desc>
</jnlp>
```

The Custom Content concept (/cfg/vpn #/portal/content) can be used to host Java Web Start applications on the Portal. Building the demo project results in a content.zip file suitable for content area upload. A precomiled one is also provided. For the material in the content area to be cacheable by the client web browser, it has to be put in a top directory called "/avaya_cacheable".

The demo project zip file has such a directory at it's top level. When uploaded to the content area, the demo is accessible through:

`https://vpn.example.com/avaya_cacheable/PortForwarderDemo.html`

The provided build.xml file contains an example of how to create a content.zip file.

Creating a Port Forwarder Authenticator

A Port Forwarder authenticator must implement the PortForwarderAuthenticator interface:

```
public PortForwarderCredentials getCredentials();
public java.net.PasswordAuthentication getProxyCredentials();
```

Example

Following is an example of the code for creating a Port Forwarder authenticator.

Comments? infodev@avaya.com

```
private String getCookieFromURL(String spec) {
        try {
            URL url = new URL(spec);
            URLConnection connection = null;

            ((HttpURLConnection) connection).setFollowRedirects(false);
            connection = url.openConnection();

            connection.getInputStream();

            /* check if we are authorized */
            if (connection != null) {
                String headerField =
                    getHeaderField(connection, SET_COOKIE_HEADER);

                return headerField.substring(headerField.indexOf('=') + 1,
                                             headerField.indexOf(';'));
            } else {
                return null;
            }
        } catch (MalformedURLException e) {
            e.printStackTrace();
        } catch (IOException e) {
            e.printStackTrace();
        }

        return null;
    }
    PortForwarderAuthenticator pfa =
            new PortForwarderAuthenticator() {
                public PortForwarderCredentials getCredentials() {
                    cookie = getCookieFromURL(loginUrl);
                    if (cookie == null) {
                        return null;
                    }
                    cred.setAvayaToken(cookie);

                    return cred;
                }

                public PasswordAuthentication getProxyCredentials() {
                    LoginDialog loginDialog = new LoginDialog();

                    return new PasswordAuthentication(loginDialog.getUserId(),
                                                      loginDialog.getPassword()
```

```
private String getCookieFromURL(String spec) {
try {
URL url = new URL(spec);
URLConnection connection = null;
((HttpURLConnection) connection).setFollowRedirects(false);
connection = url.openConnection();
connection.getInputStream();
/* check if we are authorized */
if (connection != null) {
String headerField =
getHeaderField(connection, SET_COOKIE_HEADER);
return headerField.substring (headerField.indexOf('=') + 1,
headerField.indexOf(';'));
} else {
return null;
}
} catch (MalformedURLException e) {
e.printStackTrace();
} catch (IOException e) {
e.printStackTrace();
}
return null;
}
PortForwarderAuthenticator pfa =
new PortForwarderAuthenticator() {
public PortForwarderCredentials getCredentials() {
cookie = getCookieFromURL(loginUrl);
if (cookie == null) {
return null;
}
cred.setAvayaToken(cookie);
return cred;
}
public PasswordAuthentication getProxyCredentials() {
LoginDialog loginDialog = new LoginDialog();
return new PasswordAuthentication(loginDialog.getUserId(),
loginDialog.getPassword()
.toCharArray());
}
};
portForwarder.setAuthenticator(pfa);
```

Adding a Port Forwarder Logger

A Port Forwarder logger must implement the PortForwarderLogger interface:

```
public void log(int logLevel, int logCode, Object[] params, Throwable
throwable);
public void log(int logLevel, String msg, Throwable throwable);
```

The first function is used when the Port Forwarder logs a message in the Messages.properties file, i.e. messages of type PortForwarderConstants.LOG_LEVEL_INFO and PortForwarderConstants.LOG_LEVEL_ERROR and the second one is used for messages of

Comments? infodev@avaya.com

type PortForwarderConstants.LOG_LEVEL_DEBUG and PortForwarderConstants.LOG_LEVEL_DEBUG_VERBOSE.

The PortForwarderLogger is added to the Port Forwarder by calling the setLogger function.

Example

Following is an example of the code for adding a Port Forwarder logger.

```
public class PortForwarderLoggerImpl implements PortForwarderLogger {
private final ResourceBundle messages;
private PortForwarderGui portForwarderGui;
/**
* Creates a new instance of PortForwarderLoggerImpl
*/
public PortForwarderLoggerImpl() {
messages = ResourceBundle.getBundle("Messages");
}
/**
* Tells the logger in which gui to log messages.
*
* @param portForwarderGui The gui to use
*/
public void setGui(PortForwarderGui portForwarderGui) {
this.portForwarderGui = portForwarderGui;
}
private String createTimeStamp() {
SimpleDateFormat dateFormat = new SimpleDateFormat("hh:mm:ss.SSS");
String timeStamp = dateFormat.format(new Date());
return timeStamp;
}
private String createMessage(String msg) {
return createTimeStamp() + " : " + msg;
}
public void log(final int logLevel, final int logCode,
final Object[] params, final Throwable throwable) {
if ((logLevel == PortForwarderConstants.LOG_LEVEL_ERROR) ||
(logLevel == PortForwarderConstants.LOG_LEVEL_INFO)) {
String msg =
MessageFormat.format(messages.getString("" + logCode),
params);
String messageString = createMessage(msg);
if (portForwarderGui == null) {
System.err.println("WARNING: Could not write to info area!");
System.err.println(messageString);
if (throwable != null) {
System.out.println(throwable.getMessage());
throwable.printStackTrace();
}
} else {
portForwarderGui.appendInfo(messageString +
System.getProperty("line.separator"));

if (throwable != null) {
portForwarderGui.appendInfo(throwable.getMessage() +
System.getProperty("line.separator"));
throwable.printStackTrace();
}
```

```
}
}
}
public void log(final int logLevel, final String msg,
final Throwable throwable) {
if (logLevel != PortForwarderConstants.LOG_LEVEL_DEBUG_VERBOSE) {
String messageString = createMessage(msg);
if (portForwarderGui == null) {
System.err.println("WARNING: Could not write to info area!");
System.err.println(messageString);
if (throwable != null) {
System.out.println(throwable.getMessage());
throwable.printStackTrace();
}
} else {
portForwarderGui.appendInfo(messageString +
System.getProperty("line.separator"));
if (throwable != null) {
portForwarderGui.appendInfo(throwable.getMessage() +
System.getProperty("line.separator"));
throwable.printStackTrace();
}
}
}
}
}
```

Connecting Through a Proxy

If the port forwarder is connecting through a proxy a number of properties need to be set for the port forwarder to know where and how to connect to the proxy.

The parameters are:

com.avaya.avg.portforwarder.http.proxyHost	The proxy host for HTTP & HTTPS accesses.
com.avaya.avg.portforwarder.http.proxyPort	The proxy port for HTTP & HTTPS accesses.
com.avaya.avg.portforwarder.http.proxyUserName	The proxy username for HTTP & HTTPS accesses.
com.avaya.avg.portforwarder.http.proxyPassword	The proxy password for HTTP & HTTPS accesses.

If the username and/or password is not set, the Port Forwarder API will call the **`PortForwarderAuthenticator.getProxyCredentials()`** function to obtain them.

Comments? infodev@avaya.com

Monitoring the Port Forwarder

The Port Forwarder uses the Observer/Observable framework, meaning that anyone wanting to have information from/about the Port Forwarder can add a Listener to it. Currently, you can monitor Port Forwarder status and statistics.

Note:

When using these features, it is important that the Observer.update() function does not block.

Status

Monitoring the Port Forwarder status gives you the ability to always know the state of the Port Forwarder, for example if it is ready to receive connections. Following is an example of the code for monitoring the status of the Port Forwarder.

```
private static class PortForwarderStatusListenerImpl
        implements PortForwarderStatusListener {
        public void statusChanged(int oldStatusCode, int newStatusCode) {
            statusNotifier.notifyObservers(new Integer(newStatusCode));
        }
    }

    private static class StatusObserver implements Observer {
        public void update(Observable observable, Object value) {
            portForwarderStatus = ((Integer) value).intValue();

            if (portForwarderStatus == PortForwarderConstants.
                                       PF_STATUS_INVALID_CREDENTIALS ||
               portForwarderStatus == PortForwarderConstants.PF_STATUS_STOPPED ||
              portForwarderStatus == PortForwarderConstants.PF_STATUS_GW_ERROR) {
                portForwarderGui.setStatusFailed();
            } else if (portForwarderStatus == PortForwarderConstants.
                                              PF_STATUS_INITIALIZING ||
                       portForwarderStatus == PortForwarderConstants.
                                              PF_STATUS_CONFIGURING) {
                portForwarderGui.setStatusInit();
            } else if (portForwarderStatus == PortForwarderConstants.
                                              PF_STATUS_LISTENERS_UP) {
                portForwarderGui.setStatusOk();
            }
        }
    }

    statusListener = new PortForwarderStatusListenerImpl();
    portForwarder.addStatusListener(statusListener);
```

Statistics

The Port Forwarder keeps track of all bytes passing through, allowing you to display or use the information in any way. An added statistics listener will receive a PortForwarderStatistics object either when a change has occurred or at a defined interval.

Following is an example of the code for monitoring Port Forwarder statistics.

```
    private static class StatisticsObserver implements Observer {
        public void update(Observable ob, Object value) {
            PortForwarderStatistics stats = (PortForwarderStatistics) value;
            System.out.println("Absolute     sent bytes: " +
                               stats.getAbsoluteSentBytes());
            System.out.println("             recv bytes: " +
                               stats.getAbsoluteReceivedBytes());
            System.out.println("             sent rate : " +
                               stats.getAbsoluteSentRate());
            System.out.println("             recv rate : " +
                               stats.getAbsoluteReceivedRate());
            System.out.println("Intermediate sent bytes: " +
                               stats.getIntermediateSentBytes());
            System.out.println("             recv bytes: " +
                               stats.getIntermediateReceivedBytes());
            System.out.println("             sent rate : " +
                               stats.getIntermediateSentRate());
            System.out.println("             recv rate : " +
                               stats.getIntermediateReceivedRate());
            System.out.println("Peak         sent rate : " +
                               stats.getPeakSentRate());
            System.out.println("             recv rate : " +
                               stats.getPeakReceivedRate());
        }
    }

    portForwarder.setStatisticsObserverInterval(3000);
    portForwarder.addStatisticsObserver(new StatisticsObserver());
```

This will print current statistics every 3 seconds.

Comments? infodev@avaya.com

Glossary

Access Rules — Applies to the SSL VPN feature. When a user tries to log in to the VPN server, either through the Portal page or through a VPN client, his or her group membership determines the access rights to different servers and applications on the intranet. This is done by associating one or more access rules (each containing parameters such as allowed network, ports and paths) with a group.

ARP — Address Resolution Protocol. A network layer protocol used to convert an IP address into a physical address, such as an Ethernet address. A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address.

Base Profile — Refers to links and access rules specified for a user group directly under the Group level. If extended profiles are used, the base profile's links and access rules will be appended to the extended profile's links and access rules.

CA (Certificate Authority) — A trusted third-party organization or company that issues digital certificates. The role of the CA in this process is to guarantee that the entity granted the unique certificate is, in fact, who he or she claims to be.

CLI (Command Line Interface) — The text-based interface pertaining to the AVG software, presented to the user after having logged in. The CLI can be accessed through a console connection or remote connection (Telnet or SSH). The CLI is used for collecting information and configuring the AVG.

Cluster (of VPN Gateways) — A cluster is a group of VPN Gateways that share the same configuration parameters. There can be more than one AVG cluster in the network, each with its own set of parameters and services to be used with different real servers. Every cluster has a Management IP address (MIP), which is an IP alias to one of the master VPN Gateways in the cluster.

Console Connection — A connection to the VPN Gateway established through the console port.

CRL (Certificate Revocation List) — A list containing the serial numbers of revoked client certificates. Each CA issues and maintains their own CRLs. If you generate client certificates on the VPN Gateway, you can also create your own CRL.

CSR (Certificate Signing Request) — A request for a digital certificate, sent to a CA. On the VPN Gateway, you can generate a CSR from the command line interface by using the **`request`** command.

DCE (Data Communicatons Equipment)	A device that communicates with a Data Terminal Equipment (DTE) in RS-232C communications.
DER (Distinguished Encoding Rules)	A process for unambiguously converting an object specified in ASN.1 (such as an X.509 certificate, for example) into binary values for storage or transmission on a network.
Digital Certificate	The digital equivalent of an ID card used in conjunction with a public key encryption system. Digital certificates are issued by trusted third parties known as certificate authorities (CAs), after verifying that a public key belongs to a certain owner. The certification process varies depending on the CA and the level of certification.
Digital Signature	A digital guarantee that a document has not been altered, as if it were carried in an electronically-sealed envelope. The "signature" is an encrypted digest of the text that is sent with the text message. The recipient decrypts the signature digest and also recomputes the digest from the received text. If the digests match, the message is proved intact and tamper free from the sender. A digital signature ensures that the document originated with the person signing it and that it was not tampered with after the signature was applied. However, the sender could still be an impersonator and not the person he or she claims to be. To verify that the message was indeed sent by the person claiming to send it requires a digital certificate (digital ID) which is issued by a certification authority.
DIP (Destination IP) Address	The destination IP address of a frame.
DPort (Destination Port)	The destination port number, linking the incoming data to the correct service. For example, port 80 for HTTP, port 443 for HTTPS, port 995 for POP3S.
DTE (Data Terminal Equipment)	A device that controls data flowing to or from a computer. The term is most often used in reference to serial communications defined by the RS-232C standard. This standard defines the two ends of the communication channel as being a DTE and DCE device. However, using a null-modem cable, a DTE to DTE communication channel can also be established between, for example, two computers.
Extended Profile	Extended profiles can be defined for a user group if other links and access rules should apply when the user authenticates by means of a specific authentication method or when connecting from a specific IP address or network.
GSLB (Global Server Load Balancing)	An Application Switch feature that allows you to balance server traffic load across multiple physical sites. The Avaya GSLB implementation takes into account an individual site's health, response time, and geographical location to smoothly integrate the resources of the dispersed server sites for complete global performance.
HTTP Proxy	Applies to the SSL VPN feature. Java applet accessible on the Portal page's Advanced tab, enabling links executed on complex intranet Web pages (containing

Comments? infodev@avaya.com

	plugins like Flash, Shockwave and Java applets) to be sent through a secure connection to the SSL server for redirection.
IP Interface	IP interfaces are defined on the Application Switch and are used for defining the subnets to which the switch belongs. Up to 256 IP interfaces can be configured on an Application Switch. The IP address assigned to each IP interface provides the switch with an IP presence on your network. No two IP interfaces can be on the same IP subnet. The IP interfaces can be used for connecting to the switch for remote configuration, and for routing between subnets and VLANs (if used).
Master	A VPN Gateway in a cluster that is in control of the MIP address, or can take over the control of the MIP address should another master fail. Configuration changes in the cluster are propagated to other members through the master VPN Gateways.
MIB (Management Information Base)	An SNMP structure that describes which groups and objects can be monitored on a particular device.
MIP (Management IP) Address	An IP address that is an IP alias to a master VPN Gateway in a cluster of VPN Gateways. The MIP address identifies the cluster and is used when making configuration changes through a Telnet or SSH connection or through the Browser-Based Management Interface (BBI).
Net Direct Client	The Net Direct client is an SSL VPN client that can be downloaded from the Portal for each user session. As opposed to the LSP and TDI versions of the SSL VPN client, the Net Direct client does not have a user interface. Another difference is that the Net Direct client is packet-based, while the SSL VPN clients uses system calls. The packet-based solution supports more applications (e.g. Microsoft Outlook).
Nslookup	A utility used to find the IP address or host name of a machine on a network. To use the **`nslookup`** command on the VPN Gateway, it must have been configured to use a DNS server.
NTP (Network Time Protocol)	A protocol used to synchronize the real-time clock in a computer. There are numerous primary and secondary servers on the Internet that are synchronized to the Coordinated Universal Time (UTC) through radio, satellite or modem.
AVG	Avaya VPN Gateway.
Passphrase	Passphrases differ from passwords only in length. Passwords are usually short, from six to ten characters. Short passwords may be adequate for logging onto computer systems that are programmed to detect a large number of incorrect guesses, but they are not safe for use with encryption systems. Passphrases are usually much longer—up to 100 characters or more. Their greater length makes passphrases more secure.
PEM (Privacy Enhanced Mail)	A standard for secure e-mail on the Internet. It supports encryption, digital signatures and digital certificates as well as both private and public key methods. Keys and certificates are often stored in the PEM format.

Ping (Packet INternet Groper)	A utility used to determine whether a particular IP address is online.
PKCS12	A standard for storing private keys and certificates.
PKI (public key infrastructure)	Short for public key infrastructure, a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. PKIs are currently evolving and there is no single PKI nor even a single agreed-upon standard for setting up a PKI. However, nearly everyone agrees that reliable PKIs are necessary before electronic commerce can become widespread. A PKI is also called a trust hierarchy.
Portal	Applies to the SSL VPN feature. The Portal page is displayed following a successful login to a virtual SSL VPN server configured as a portal server. The Portal contains five different tabs from where the user can access various intranet resources such as web, mail and file servers.
Portal Guard	The Portal Guard feature is an easy way of "converting" an existing HTTP site to generate HTTPS links, secure cookies etc. The VPN Gateway will not only handle the SSL processing but also see to it that all existing web links are rewritten to HTTPS. This eliminates the need to rewrite each link manually.
Port Forwarder	Applies to the SSL VPN feature. Java applet accessible on the Portal page's Advanced tab, enabling transparent access to applications through a secure connection. By specifying an arbitrary port number on the client along with the desired intranet host and port number, the user can access an intranet application by connecting to localhost on the specified port number.
Real Server Group	A group of real servers that are associated with a virtual server IP address (VIP) or filter on an Application Switch.
RIP (Real Server IP) Address	A real server IP address that the Application Switch load balances to when requests are made to a virtual server IP address (VIP).
RPort (Real Server Port)	The real server port, which a virtual SSL server on the VPN Gateway uses when sending and receiving information to and from the real servers.
Setup Utility	When starting a VPN Gateway the very first time, you enter the Setup utility automatically. The Setup utility is used for performing a basic configuration of the VPN Gateway. The Setup utility first presents you with the choice of setting up the AVG as a single device, or to add the VPN Gateway to an existing cluster. If you perform a reinstallation of the AVG software, you will also enter the Setup Utility after the VPN Gateway has rebooted.
SIP (Source IP) Address	The source IP address of a frame.

Comments? infodev@avaya.com

Slave	A VPN Gateway that depends on a master device in the same cluster for proper configuration.
SNMP (Simple Network Management Protocol)	A network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (a VPN Gateway, for example), to the workstation console (or SNMP manager) used to oversee the network. The SNMP agents return information in a MIB (Management Information Base), which is a data structure that defines what information is obtainable from the device.
SOCKS	A generic, proxy protocol for TCP/IP-based networking applications. The SOCKS protocol provides a flexible framework for developing secure communications by easily integrating other security technologies, e.g. SSL. SOCKS includes two components, the SOCKS server and the SOCKS client. The SOCKS server is implemented at the application layer, while the SOCKS client is implemented between the application and transport layers. The basic purpose of the protocol is to enable hosts on one side of a SOCKS server to gain access to hosts on the other side of a SOCKS server, without requiring direct IP reachability.
SPort (Source Port)	The source destination port, linking the incoming data to the correct service. For example, port 80 for HTTP, port 443 for HTTPS, port 995 for POP3S.
SSH (Secure Shell)	A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels.
SSL (Secure Sockets Layer) Protocol	The SSL protocol is the leading security protocol on the Internet. It runs above the TCP/IP protocol and below higher-level protocols such as HTTP or IMAP. SSL uses TCP/IP on behalf of the higher-level protocols and, in the process, allows an SSL-enabled server to authenticate itself to an SSL-enabled client.
SSL VPN client	Windows application with SOCKS support. When installed on a user's computer, transparent access (not through the Portal page) to intranet applications is enabled.
STP (Spanning Tree Protocol)	An algorithm used in transparent bridges that dynamically determines the best path from source to destination. It avoids bridge loops (two or more paths linking one segment to another), which can cause the bridges to misinterpret results. The algorithm creates a hierarchical "tree" that "spans" the entire network including all switches. It determines all redundant paths and makes only one of them active at any given time.
TLS (Transport Layer Security)	The TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
Traceroute	A utility used to identify the route used for station-to-station connectivity across the network.

Trap	If a trap is defined in the MIB, a trap message is sent from the SNMP agent to the SNMP manager when the trap is triggered. A trap can for example define a hardware failure in a monitored device.
Tunnel Guard	Tunnel Guard is an application that maintains checks that the required components (executables, DLLs, configuration files, etc.) are installed and active on the remote user's machine.
URI (Uniform Resource Identifier)	The addressing technology from which URLs are created. Technically, URLs such as HTTP:// and FTP:// are specific subsets of URIs, although the term URL is mostly heard.
VIP (Virtual Server IP) Address	An IP address that the switch owns and uses to load balance particular service requests (like HTTP) to other servers.
Virtual Router	A shared address between two devices utilizing VRRP, as defined in RFC 2338. One virtual router is associated with an IP interface defined on the Application Switch. All IP interfaces on an Application Switch must be in a VLAN. If there is more than one VLAN defined on the Application Switch, then the VRRP broadcast will only be sent out on the VLAN to which the associated IP interface has been added.
Virtual SSL Server	A virtual SSL server handles a specific service on the VPN Gateway, such as HTTPS, SMTPS, IMAPS, or POP3S. You can create an unlimited number of virtual SSL servers per AVG cluster, and each virtual SSL server is mapped to a virtual server on the Application Switch. To authenticate itself towards clients making requests for the specified service, the virtual SSL server is configured to use a digital certificate.
VLAN (Virtual Local Area Network)	VLANs are commonly used to split up groups of network users into manageable broadcast domains, to create logical segmentation of workgroups, and to enforce security policies among logical segments. Up to 246 VLANs are supported on an Application Switch running Web OS.
VRRP (Virtual Router Redundancy Protocol)	A protocol similar to Cisco's proprietary HSRP address-sharing protocol. The reason for both of these protocols is to ensure devices have a next hop or default gateway that is always available. For example, two or more devices sharing an IP interface are either advertising or listening for advertisements. These advertisements are sent through a broadcast message to address 224.0.0.18. With VRRP, one switch is considered the master and the other is the backup. The master is always advertising through the broadcasts. The backup switch is always listening for the broadcasts. Should the master stop advertising, the backup will take over ownership of the VRRP IP and MAC addresses as defined by the specification. The switch announces this change in ownership to the devices around it by way of a gratuitous ARP and advertisements. If the backup switch didn't do the gratuitous ARP, the Layer 2 device attached to the switch will not know that the MAC address had moved in the network. For a more detailed description, refer to RFC 2338.

Comments? infodev@avaya.com

X.509 A widely-used specification for digital certificates that has been a recommendation of the ITU since 1988.

Comments? infodev@avaya.com

Index

A

activate 65
  software upgrade package 65
  software version 65
Active Directory, add attribute for user preferences . 241
Administrator user, access level 122
Apache software license 209
ASCII terminal 119
attribute for user preferences 241

B

baud rate, console connection 119
bookmarks, add attribute 241
Boot user 60, 122
  access level 122
  software reinstall 60

C

certificate formats 86
certificate signing request (CSR) 81
  generate 81
certificates 81, 92, 102, 149
  add using TFTP 92
  managing 81
  revoke client certificates 102
  view installed certificates 149
ciphers 153–155
  list formats 154
  meaning of string aliases 155
  string aliases 155
  strings 154
  supported 153
  supported strings 155
client authentication 97
  generate client certificates 97
client certificate authentication 95
cluster 31, 34, 130
  general information 31
  interfaces within a cluster 34
  unable to join 130
configuration 31
  parameters 31
connect 120
  through Telnet 120
console port 119
  connecting 119
CRL, see certificate revocation list 102
CSR, see certificate signing request 81

D

database, replicated 31
DisablenewIPSecLogins 13
documentation 9
  other VPN Gateway manuals 9

E

enable 121, 122
  SSH access 122
  Telnet access 121
error log files 151

F

factory default configuration 60, 124
  after reinstalling software 60
  initial setup 124
feature summary 16, 25
  ASA 310-FIPS 25
  software features 16
FIPS security mode 26
  specification 26
first-time configuration 124

G

GNU general public license 209

H

hardware security module 25, 26
  ASA 310-FIPS 25
  iKey authentication 26
host IP 32
host keys (SSH) 239
HSM 27
  wrap key 27

HSM-SO 27
iKey 27
HSM-USER 27

I

idle timeout, command line interface 124
iKey 27, 28
HSM-CODE 27
HSM-SO 27
HSM-USER 27
required iKey for specific operation 28
install options 36, 45, 50, 55
adding ASA 310-FIPS device to existing cluster ..55
adding VPN Gateway to existing cluster 45
first ASA 310-FIPS in new cluster 50
first device in new cluster 36
IP address types 32

K

key code definition file 235
key formats 86
known hosts 239
known hosts (SSH) 239

L

license information 209
Apache software license 209
GNU general public license 209
OpenSSL 209
SSLeay license 209

M

major release upgrade 63
management IP 32
Management IP 32, 130
cannot contact 130
master 31, 49
configuration 31, 49
minor release upgrade 63
MIP, see Management IP 32

N

network 149
diagnostics 149
Note passwords 122

O

OpenSSL license issues 209
Operator user, access level 122

P

passwords 132
regain access after losing 132
portal bookmarks, add attribute 241
portal IP 32
ports 33

R

real server IP 32
reboot 132
ASA indicated as down 132
reinstalling software 60
revoke 102, 103
certificates issued by external CA 102
certificates issued by own organization 103
Root user, access level 122

S

Secure Shell (SSH) 121, 127
connect using 121
unable to connect using 127
security modes on the ASA 310-FIPS 25
slave 31, 49
configuration 31, 49
SNMP 159, 165
agent 159
supported MIBs 159
supported traps 165
software 16, 63, 65
activate downloaded upgrade package 65
features in this version 16
minor or major release upgrade 63
version handling when upgrading 65
SSH host keys 239
ssh known hosts 239
SSH, see Secure Shell 121, 127
SSL 149
view configured servers 149
SSLeay license 209
starting device, first time 35
supported 153

ciphers 153
syslog messages, list of 167
syslog servers 151
error log files 151
system diagnostics 149, 151
active alarms 151
error log files on Syslog server 151
events log file 151
network diagnostics 149

T

Telnet 127
unable to connect using 127
terminal emulation 119
timeout value, command line interface 124
troubleshooting 127, 130–132, 137, 141, 149
a user fails to authenticate to the Portal 141
ASA 310-FIPS cluster needs to be reconstructed 137
ASA stops responding 131
Cannot contact MIP 130
lost passwords 132
network diagnostics 149
unable to add to cluster 130
unable to connect through SSH 127
unable to connect through Telnet 127
view certificates and SSL servers 149

U

upgrade 63, 65
activate software package 65
handling software versions 65
minor or major release upgrade 63
user 122
access levels 122
categories 122
passwords 122
user preferences 241

V

virtual IP 32

W

wrap key 27
generation of 27