

Part No. 217315-A Rev 00
March 2005

4655 Great America Parkway
Santa Clara, CA 95054

Firewall User's Guide and Command Reference

Service Delivery Module 8660 Release 2.2.7 for the
Passport 8600 Series Switch



>THIS IS **THE WAY**

>THIS IS **NORTEL™**

Copyright © Nortel Networks Limited 2005. All rights reserved.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this document may be reproduced in any form by any means without prior written authorization of Nortel Networks, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

U.S. Government End Users: This document is provided with a “commercial item” as defined by FAR 2.101 (Oct 1995) and contains “commercial technical data” and “commercial software documentation” as those terms are used in FAR 12.211-12.212 (Oct 1995). Government End Users are authorized to use this documentation only in accordance with those rights and restrictions set forth herein, consistent with FAR 12.211- 12.212 (Oct 1995), DFARS 227.7202 (JUN 1995) and DFARS 252.227-7015 (Nov 1995).

Nortel Networks, Inc. reserves the right to change any products described herein at any time, and without notice. Nortel Networks, Inc. assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Nortel Networks, Inc. The use and purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of Nortel Networks, Inc.

Service Delivery Module 8660 Release 2.2.7 for the Passport 8600 Series Switch, Alteon 5008, 5010, 5012, 5100, 5300, 5400, 5500, 5600, 5700, 5105, 5106, 5109, 5114, 5308, 5408, 5610, 5710, Alteon iSD-SFD, Alteon Firewall, Firewall OS, Alteon SFA, Alteon Firewall Accelerator, and Alteon Accelerator OS are trademarks of Nortel Networks, Inc. in the United States and certain other countries.

Check Point, OPSEC, and SmartUpdate are trademarks of Check Point Software Technologies Ltd. FireWall-1 and VPN-1 are registered trademarks of Check Point Software Technologies Ltd.

Portions of this manual are Copyright © 2001 Check Point Software Technologies Ltd. All Rights Reserved.

Portions of this manual are Copyright © 2001 Dell Computer Corporation. All Rights Reserved.

Any other trademarks appearing in this manual are owned by their respective companies.

Export

This product, software and related technology is subject to U.S. export control and may be subject to export or import regulations in other countries. Purchaser must strictly comply with all such laws and regulations. A license to export or reexport may be required by the U.S. Department of Commerce.

Licensing

This product includes software developed by Check Point Software Technologies (<http://www.checkpoint.com>). This product also contains software developed by other parties.

See [Appendix C](#), “Software licenses,” for more information.

Regulatory Compliance

FCC Class A Notice. The equipment complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: 1) The device may not cause harmful interference, and 2) This equipment must accept any interference received, including interference that may cause undesired operation.

The equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. The equipment generates, uses and can radiate radio-frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. Operation of this equipment in a residential area is likely to cause harmful interference. In such a case, the user will be required to correct the interference at his own experience.

Do not make mechanical or electrical modifications to the equipment.

Industry Canada: This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil Numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

VCCI Class A Notice: This is a Class A product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur. In such a case, the user may be required to take corrective actions.

Japanese VCCI Class A Notice

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Taiwan EMC Notice

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

CE Notice: The CE mark on this equipment indicates that this equipment meets or exceeds the following technical standards: EN55022, EN55024, EN60950, and all supporting document requirements.

Safety Information

Caution—Nortel Networks products are designed to work with single-phase power systems having a grounded neutral conductor. To reduce the risk of electric shock, do not plug Nortel Networks products into any other type of power system. Contact your facilities manager or a qualified electrician if you are not sure what type of power is supplied to your building.

Caution—Not all power cords have the same ratings. Household extension cords do not have overload protection and are not meant for use with computer systems. Do not use household extension cords with your Nortel Networks product.

Caution—Your Nortel Networks product is shipped with a grounding type (three-wire) power cord. To reduce the risk of electric shock, always plug the cord into a grounded power outlet.

Nordic Lithium Battery Cautions

(Norvege) ADVARSEL—Litiumbatteri - Eksplosjonsfare. Ved utskifting benyttes kun batteri som anbefalt av apparatfabrikanten. Brukt batteri returneres apparatleverandøren.

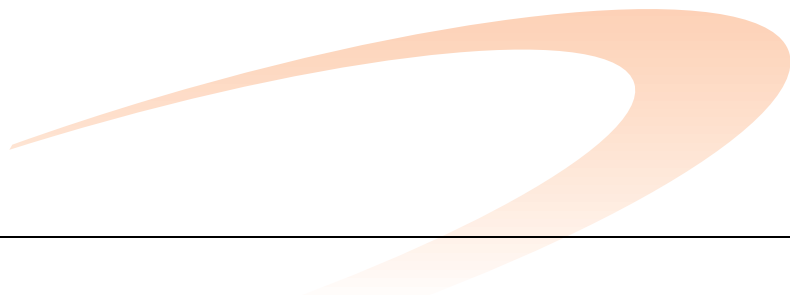
(Sverige) VARNING—Explosionsfara vid felaktigt batteribyte. Använd samma batterityp eller en ekvivalent typ som rekommenderas av apparattillverkaren. Kassera använt batteri enligt fabrikantens instruktion.

(Danmark) ADVARSEL! Litiumbatteri - Eksplosionsfare ved fejlagtig håndtering. Udskiftning må kun ske med batteri af samme fabrikat og type. Levér det brugte batteri tilbage til leverandøren.

(Suomi) VAROITUS—Paristo voi räjähtää, jos se on virheellisesti asennettu. Vaihda paristo ainoastaan laitevalmistajan suosittelemaan tyyppiin. Hävitä käytetty paristo valmistajan ohjeiden mukaisesti.

Warranty

Nortel Networks provides a limited warranty on all its products for a period of one year from the date of shipment. Free technical support and free replacement of hardware is provided for the first 90 days after shipment. You may choose to purchase additional service and support from Nortel Networks. Please contact your local sales representative for more information.



Contents

Preface	15
Who Should Use This Book	15
How This Book Is Organized	15
Typographic Conventions	17
Locating your software	18
Reading path	19
How to Get Help	20
Chapter 1	
Introduction	21
Feature summary	21
Software	21
Hardware	22
Firewall iSD ports	23
Performance	25
Certification	25
System management	25
Logging and monitoring	25
8660 SDM basics	26
Network elements	26
Networks	26
Firewalls	27
Management interfaces	27
Passport 8600 and firewall iSD VLANs	28
Chapter 2	
Initial setup	31
Overview of initial setup tasks	31

Basic requirements	32
Example networks	33
Network elements	35
Firewall iSD management network	35
SmartCenter Server	35
Trusted network	36
Untrusted network (Internet)	36
Using the CLI for basic configuration	36
New Passport 8600 CLI commands for the 8660 SDM	36
config naap	37
show naap	37
config cluster	38
show cluster	38
Modified Passport 8600 CLI commands for the 8660 SDM	39
config vlan <vid> create	39
show config module <value>	40
Configuring the 8660 SDM	41
Initializing the firewall iSD	44
Using the join command	50
Creating the firewall interface	52
Configuring VRRP	53
Configuring the firewall iSD and Check Point SmartCenter Server static routes ..	54
Setting the license key	54
Example:	54
Switching management and console ports among iSDs	56
Switching iSDs	56
Halting disk drives on the 8660 SDM	57
Halting configured firewall iSDs	57
Halting non-configured firewall iSDs	59
Reinitializing halted firewall iSDs	61
Allowing SMART Client access to the iSDs	62
Installing Check Point management tools	62
Editing the Windows NT hosts file	63
Installing Check Point SmartServer and SmartConsole	64
Defining a firewall object in the SmartDashboard	76
Establishing Secure Internal Communication	79

Managing all clusters from one Check Point management station82
 Creating a firewall policy test rule86
 Creating and installing firewall iSD security rules89
 Managing Check Point licenses90
 Installing central licenses with SmartUpdate90
 Re-installing an existing license91
 Installing a license on an NT Workstation92

Chapter 3

Using JDM to configure firewall iSDs 93

Overview of JDM tasks93
 Configuring firewall iSD clusters93
 Creating firewall VLANs97
 Configuring VLAN IP addresses102
 Enabling and disabling NAAP104
 Enabling and disabling a firewall iSD105
 Viewing firewall iSD states107
 Accessing the Browser-Based Interface109
 Viewing SDM Management Port properties110
 Example network configuration111

Chapter 4

System management basics 119

Management tools119
 Users and passwords120

Chapter 5

The Command Line Interface 123

Accessing the CLI123
 Using the local serial port123
 Defining the remote access list124
 Displaying the access list124
 Adding items to the access list124
 Using Telnet125
 Enabling Telnet access126
 Starting the Telnet session127

Using Secure Shell	127
Enabling SSH access on the firewall iSD	127
Starting the SSH session	129
Using the CLI	129
Basic operation	129
The Main Menu	130
Idle time-out	131
Multiple administration sessions	131
Global commands	131
Command line history and editing	133
Command line shortcuts	134
Command stacking	134
Command abbreviation	134
Tab completion	134
Chapter 6	
Command reference	135

Main Menu	135
Information Menu	138
Info_host Menu	140
Information Menu	141
Route Information Menu	141
VRRP Information Menu	143
Configuration Menu	144
System Menu	146
Backup Menu	148
Date and Time Menu	149
DNS Servers Menu	151
Cluster Menu	152
Access List Menu	154
Administrative Applications Menu	155
Platform Logging Menu	173
User Menu	178
Network Configuration Menu	183
Port Menu	184
Interface Menu	185
VRRP Interface Menu	187

- VRRP Settings Menu 188
- Advanced Settings Menu 191
- Firewall License Menu 204
- Firewall Configuration Menu 205
 - Sync Configuration Menu 207
- SMART Clients Menu 208
- SmartUpdate Configuration Menu 208
- Miscellaneous Settings Menu 209
- Boot Menu 210
 - Software Management Menu 211
- The Maintenance Menu 212
 - Diagnostic Tools Menu 213
 - Firewall Maintenance Menu 213
 - Tech Support Dump Menu 214
 - OSPF Debug Menu 215

Chapter 7
Browser-Based Interface 217

- Features217
- Getting started218
 - Requirements218
 - Enabling the Browser-Based Interface218
 - Setting up the web browser220
 - Starting the Browser-Based Interface220
- Browser-Based Interface basics222
 - Interface components222
 - Basic operation223
 - Global command forms224
 - Apply225
 - Diff227
 - Revert228
 - Logout229
 - Help230

Chapter 8
BBI forms reference. 233

- Overview233

Monitor forms	234
Monitor > System	234
Monitor > Hosts	235
Monitor > Syslog	236
Monitor > About	237
Cluster forms	238
Cluster > Time	238
Cluster > iSDs	239
Cluster > Logs > Syslog	240
Cluster > Logs > ELA	241
Cluster > Logs > Archive	243
Cluster > Miscellaneous	244
Network forms	245
Network > DNS	246
Network > NTP	247
Network > Ports	248
Network > Ports > Update (Add or Modify)	249
Network > Interfaces	250
Network > Interfaces > Update (Add or Modify)	251
Network > VRRP	252
Network > Gateway	254
Network > Routes > Static	254
Network > Routes > Static > Update (Add, Delete, or Modify)	255
Network > Routes > Proxy ARP	256
Network > Routes > OSPF > General	257
Network > Routes > OSPF > Area Index	258
Network > Routes > OSPF > Area Index > Update (Add or Modify)	259
Network > Routes > OSPF > Interface	260
Network > Routes > OSPF > Interface > Update (Modify)	261
Firewall forms	263
Firewall > Settings	263
Firewall > License Management	264
Firewall > License Management > Update (Delete or Modify)	265
Firewall > Synchronization	267
Operations forms	268
Operation > Configuration	268

Operation > Update269

Administration forms271

Administration > Users272

Administration > Users > Add New User273

Administration > Access List274

Administration > Access List > Update (Add or Modify)275

Administration > Telnet-SSH276

Administration > Web > General277

Administration > Web > Create Cert278

Administration > Web > Server Certs279

Administration > Web > Server Certs > Update (Add or Modify)280

Administration > Web > CA Certs281

Administration > Web > CA Certs > Update (Add or Modify)282

Administration > SNMP > General283

Administration > SNMP > System284

Administration > SNMP > Trap Hosts285

Administration > SNMP > Trap Hosts > Update (Add or Modify)286

Administration > SNMP > USM Users287

Administration > SNMP > USM Users > Update (Add or Modify)288

Administration > SNMP > Advanced289

Diagnostics forms290

Diagnostics > System Commands290

Chapter 9

Applications 293

Virtual Router Redundancy Protocol294

VRRP on the firewall iSDs294

 Firewall iSD cluster and VRRP294

 VRRP router parameters295

 Active master determination296

High Availability firewall configuration299

 Requirements300

 Installing the redundant firewall iSD301

 Configuring the redundant firewall iSD301

 Configuring VRRP on both firewall iSDs302

 Establishing trust on redundant iSDs308

Synchronizing firewall iSDs	309
Configuring synchronization using the CLI	309
Configure HA at the Check Point SmartDashboard	310
Example SmartDashboard configuration for HA	312
Chapter 10	
Open Shortest Path First	317
OSPF overview	317
Types of OSPF areas	318
Types of OSPF routing devices	319
Neighbors and adjacencies	319
Link-State Database	320
Shortest Path First tree	320
Authentication	321
Internal and external routing	321
Firewall OSPF implementation	322
Configurable parameters	322
Defining areas	323
Assigning the area index	323
Using the area ID to assign the OSPF area number	324
Attaching an area to a network	324
Interface cost	325
Electing the DR and BDR	325
Router ID	326
Authentication	326
Simple authentication	326
MD5 authentication	326
OSPF features not supported in this release	327
OSPF configuration examples	327
Example 1: simple OSPF domain	328
Configuring a single firewall iSD with OSPF	328
Configuring OSPF support	330
Verifying OSPF support	331

Chapter 11
Upgrading the software. 333

Compatibility 334

Types of upgrade 335

 Firewall iSD upgrades 335

 Built-in firewall software upgrades 336

 Check Point management station upgrades 336

Overview of upgrade tasks 336

Installing a minor/major release upgrade 337

Activating the software upgrade package 339

 Single member (iSD) cluster upgrade 339

 Two member (iSD) cluster upgrade 340

Reinstalling Software 345

 Reinstalling software using FTP 345

Chapter 12
Event Logging API. 349

Configure the Check Point SmartCenter Server 350

Configuring ELA on the firewall iSD 355

The Check Point SmartView Tracker 357

Appendix A
Common tasks. 359

Tuning Check Point NG performance 360

 Connection parameters 360

 NAT parameters 361

Reading system memory information 362

Cluster backup and clone procedures 363

 Backing up 363

 Cloning 364

Generating a public or private DSA key pair 366

Appendix B
Troubleshooting. 369

Failed to establish trust between SmartCenter Server and firewall iSD 369

Actions	369
Cannot download policy on firewall iSD	371
Action	371
Poor performance with other devices	371
Action	371
Cannot log into the management station from the SMART Client	372
Actions	372
Check Point sends connection failed messages to the firewall iSD	372
Action	372
VRRP configuration tips	372
VRRP: active master backup fails	374
Actions	374
VRRP: Both masters are active	375
Actions	375
Poor performance under heavy traffic	376
Action	376
Appendix C	
Software licenses.....	377
Apache Software Licence	377
mod_ssl License	378
OpenSSL and SSLeay Licenses	379
OpenSSL License	379
Original SSLeay License	380
PHP License	381
SMTPclient License	382
GNU General Public License	383
Index	389



Preface

This *User's Guide* describes the components and features of the 8660 Service Delivery Module Firewall 1 (SDM FW1), FW2, and FW4 system and explains how to perform initial setup, configuration, and maintenance.

The term “8660 SDM” is used in this document when descriptions or procedures apply to any of the 8660 SDM models (SDM FW1, FW2, and FW4). When references are to specific 8660 SDM boards, the model is referenced.

The firewall modules consist of a processor PCI Mezzanine Card (PrPMC) and a disk drive. The PrPMC and disk drive are referred to collectively as a firewall integrated Service Director (iSD). Therefore, the term “firewall iSD” is used to refer to the firewall modules themselves. See *Installing the 8660 Service Delivery Module (SDM) for the Passport 8600 Series Switch* (part number 217314-A) for more information.

Once you have completed network configuration using this guide, you must rely on the documentation from Check Point to develop and administer security policies.

Who Should Use This Book

This *User's 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.

How This Book Is Organized

The chapters in this book are organized as follows:

Chapter 1, “Introduction”, provides an overview of the major features of the 8660 SDM, including the physical layout of its components and the basic concepts behind their operation.

Chapter 2, “Initial setup”, describes how to perform start-up configuration on a firewall iSD. An example network is shown, along with instructions on how to configure the 8660 SDM CLI and Check Point™ SmartCenter Server.

Chapter 3, “Using JDM to configure firewall iSDs”, shows procedures for configuring firewall iSDs using the JDM.

Chapter 4, “System management basics”, describes the various tools used for managing the system, and explains basic management concepts.

Chapter 5, “The Command Line Interface”, describes how to access and use the text-based management interface for collecting system information and performing configuration.

Chapter 6, “Command reference”, explains the menus, commands, and parameters of the text-based management interface.

Chapter 7, “Browser-Based Interface”, provides an introduction to the Browser-Based Interface (BBI), and includes instructions for accessing the firewall iSD system management features from a web browser.

Chapter 8, “BBI forms reference”, identifies and explains each form available through the BBI.

Chapter 9, “Applications”, provides configuration examples for clustering firewall iSDs in a redundant configuration for High Availability (HA) using VRRP, synchronization for stateful failover, and VLAN tagging. There is also an overview of the VRRP implementation.

Chapter 10, “Open Shortest Path First”, provides an overview of the Open Shortest Path First (OSPF) protocol, describes the implementation of OSPF on the firewall iSD, and includes OSPF configuration examples.

Chapter 11, “Upgrading the software”, describes how to upgrade or reinstall the firewall iSD system component software.

Chapter 12, “Event Logging API”, describes how to view firewall iSD log messages with your Check Point SmartView Tracker.

Appendix A, “Common tasks”, describes routine management functions.

Appendix B, “Troubleshooting”, provides suggestions for troubleshooting basic problems.

Appendix C, “Software licenses”, provides licensing information for the software used in this product.

Typographic Conventions

The following table describes the typographic styles used in this book.

Table 1 Typographic conventions

Typeface or Symbol	Meaning	Example
AaBbCc123	This fixed-width type is used for names of commands, files, and directories used within the text. It also depicts on-screen computer output and prompts.	View the <code>readme.txt</code> file. Main#
<i>AaBbCc123</i>	This italicized type shows book titles, special terms, or words to be emphasized.	Read your <i>User's Guide</i> thoroughly.
AaBbCc123	This fixed-width, bold type appears in command examples. It shows text that must be typed in exactly as shown.	Main# sys
< <i>AaBbCc123</i> >	Italicized type within angle-brackets appears in command examples as a parameter placeholder. Replace the indicated text with the appropriate real name or value when using the command. Do not type the brackets.	To establish a Telnet session, enter: host# telnet <IP address>
[]	Command items shown inside square brackets are optional and can be used or excluded as the situation demands. Do not type the brackets.	host# ls [-a]
	Command items separated by the vertical bar depict a list of possible values, only one of which should be entered. The vertical bar can be literally considered to mean "or." This can also be used to separate different selections within a window-based menu bar.	System# autoneg on off Select Edit Copy from the window's menu bar.
<Key>	Non-alphanumeric keyboard items are shown in regular type inside brackets. When directed, press the appropriate key. Do not type the brackets.	Press the <Enter> key.

Locating your software

You can download the most current software image from the Nortel Networks™ Customer Support web site at www.nortel.com/support.

For additional information, refer to *Release Notes for the Passport 8600 Series Switch Software Release 3.7.6* (part number 217316-A).

You can also find a comprehensive list of the required filenames and how to upgrade your Passport software in the *Upgrading to Passport 8000 Series Switch Software Release 3.7.6* (part number 318843-A). For instructions on how to access this and other technical documentation for the 8660 SDM, see “[Reading path](#)” on page 19.

Reading path

You can download the most current technical documentation for your Passport 8000 Series Switch from the Nortel Networks™ Customer Support web site at www.nortel.com/support in your browser.

If, for any reason, you cannot find a document, use the **Search** function in the top right-hand side of the web site:

- 1 Click **Search**.
The **Search** page opens.
- 2 Ensure the **Support** tab is selected on the **Search** page.
- 3 Enter the title or part number of the document in the **Search** field.
- 4 Click **Search**.

You can print the listed technical manuals and release notes free, directly from the Internet. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

How to Get Help

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

If you purchased a Nortel Networks service program, contact Nortel Networks Technical Support. To obtain contact information online, go to the www.nortel.com/contactus URL, then click Technical Support.

Additional information about the Nortel Networks Technical Solutions Centers is available from the www.nortel.com/callus URL.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to www.nortel.com/erc.



CHAPTER 1

Introduction

The Service Delivery Module Firewall 1 (SDM FW1), SDM FW2, and SDM FW4 are each a combination of dedicated hardware and software (hardened OS, security applications, and networking technology). Each addresses the need for security, performance, and ease of use.

The software is a combination of Alteon Single System Image (SSI) software and the FireWall-1[®] NG software from Check Point[™].

Feature summary

The 8660 SDM is an Intelligent input/output (I/O) module that runs its own software independently of the Passport 8600 software. Passport 8600 Series Switch Software Release 3.7.6 is enhanced to include the 8660 SDM in the family of I/O modules supported.

Software

The SDM FW1, FW2, and FW4 ship with the following software installed:

- Check Point FireWall-1 NG with Application Intelligence
- Firewall OS consisting of the Alteon SSI software

The following are features of the software:

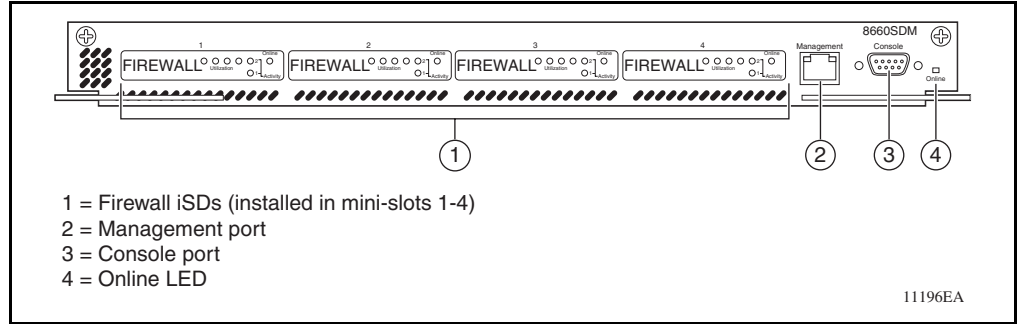
- Command Line Interface (CLI)
- Browser-Based Interface (BBI)
- Network Address Translation (NAT)
- Utility to back up and restore configuration and images
- Anti-spoofing support
- Advanced user filtering using an Access Control list

Hardware

The 8660 SDM has four unique application module slots instead of external I/O ports.

Figure 1-1 shows the faceplate of an SDM FW4.

Figure 1-1 SDM FW4 faceplate



Each 8660 SDM application module is available in three different models using a custom-designed general and security processor (Processor PCI Mezzanine Card [PrPMC]) running the Check Point Firewall-1 NG software. The 8660 SDM solution requires that you have at least one Passport 8600 L2-7 Intelligent Routing Switch.

The three 8660 SDM models are:

- 8660 SDM card with one application mini-slot (mini-slot 4) populated with a firewall iSD (SDM FW1)
- 8660 SDM card with two application mini-slots (mini-slots 3 and 4) populated with firewall iSDs (SDM FW2)
- 8660 SDM card with four application mini-slots (mini-slots 1–4) populated with firewall iSDs (SDM FW4)

Table 1-1 lists the 8660 SDM hardware features.

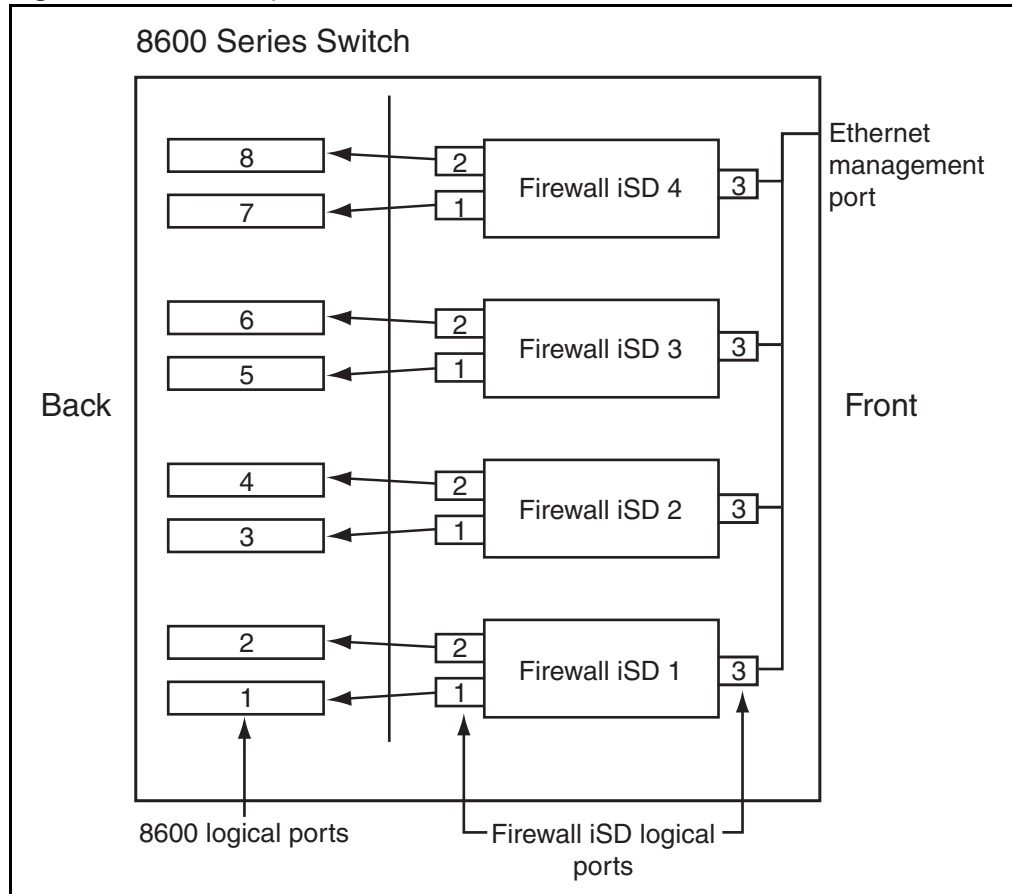
Table 1-1 8660 SDM hardware features

Footprint	One slot in a Passport 8600 chassis
CPU	Intel
RAM	512 Mbytes
Number of iSD slots	Four

Firewall iSD ports

Each firewall iSD has three Ethernet ports defined. Ports 1 and 2 face the backplane of the 8660 SDM board. Port 3 connects to the management port on the front faceplate of the 8660 SDM. See [Figure 1-2](#).

Figure 1-2 Ports setup



NOTE – The mini-slots on the 8660 SDM are numbered from left to right (1-4). However, the firewall iSDs are installed from right to left (that is, for an SDM FW1, the firewall iSD is in mini-slot 4; for an SDM FW2, the firewall iSDs are installed in mini-slots 3 and 4, and so on).

Table 1-2 describes the firewall iSD logical ports.

Table 1-2 Firewall iSD logical ports

Port	Description
1 (Control plane)	<ul style="list-style-type: none"> ■ Used strictly for cluster and Check Point management ■ NAAP VLAN (VLAN ID 4094) ■ Management VLAN
2 (Data plane)	<ul style="list-style-type: none"> ■ Used for data ■ Used for Check Point sync when High Availability (HA) is enabled ■ Firewall and Firewall Peering VLAN — up to 256 VLANs ■ Sync VLAN
3 (Maintenance)	<ul style="list-style-type: none"> ■ Isolated to the Ethernet management port on the front of the 8660 SDM and the logical Port 3 of the other firewall iSDs. ■ Used for maintenance ■ Connects to the management port on the front faceplate of the 8660 SDM

For further information on VLANs, refer to [“Passport 8600 and firewall iSD VLANs”](#) on page 28.

NOTE – There are two methods for upgrading software on the firewall iSD. The first method uses the ASF5100_2.2.7.0_SDM_R55.img file. The second method uses the ASF5100_2.2.7.0_SDM_R55.pkg file. The .pkg file is currently unavailable. In future up-issues of software, the .pkg file will be available. Additional configuration can be necessary when upgrading using the .pkg method.

Management and serial ports

The Ethernet management port on the 8660 SDM is an MDI 10/100/1000Base-T port.

The 8660 SDM has one serial port for attaching console devices. The console port provides terminal access to the 8660 SDM for the CLI. The console cable is straight-through, as opposed to null modem.

Both the Ethernet management port and the console port are shared among the iSDs. To access each firewall iSD individually, you must select the active firewall iSD using the Passport 8600 Series Switch CLI. This switches the front-facing console port to manage the firewall iSD of your choice. For information on using the Passport 8600 Series Switch CLI to switch among firewall iSDs on the 8660 SDM, see [“Switching management and console ports among iSDs”](#) on page 56.

Performance

Table 1-3 shows the hardware performance numbers for the firewall iSD.

Table 1-3 8660 SDM hardware performance

8660 SDM model	Throughput (Mbps)	Concurrent sessions	New connections per second
SDM FW1	300	250 000	2500
SDM FW2	600	500 000	5000
SDM FW4	1200	1 000 000	10 000

Certification

- Secured by Open Platform for Security (OPSEC)

System management

- Browser-Based Interface (HTTP and HTTPS), as well as CLI (serial, Telnet and Secure Shell [SSH]), offers easy configuration of network settings
- Extensive diagnostics

Logging and monitoring

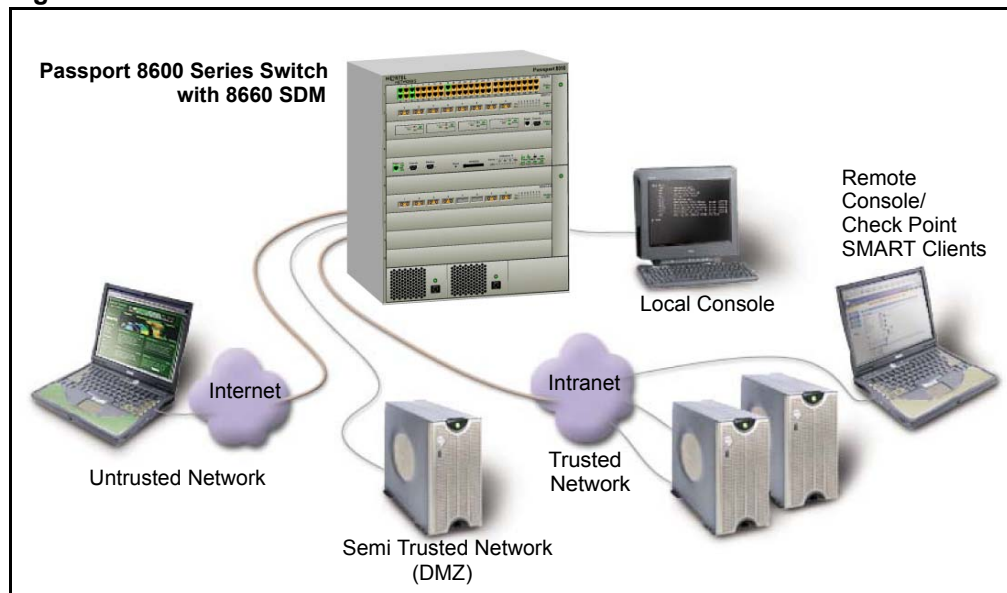
- SNMP V2c and V3 event and alarm traps
- Large RAM for local logging with periodic transfer to management server
- Hard drive for storing log messages

8660 SDM basics

Network elements

Figure 1-3 shows a basic network using the Passport 8600 Series Switch with the 8660 SDM installed in slot 3.

Figure 1-3 Network elements



Networks

■ Trusted networks

These represent internal network resources that must be protected from unauthorized access. Trusted networks usually provide internal services such as a company's intranet, as well as valued applications made available to external clients, such as public e-commerce web sites.

■ Semi-trusted networks

To increase security, services intended primarily for external clients are often placed on a separate network so that a hostile intrusion would not affect the company's internal networks. A network isolated in this way is also known as a De-Militarized Zone (DMZ). For more information, see your Check Point documentation.

■ Untrusted networks

These are the external networks that are presumed to be potentially hostile, such as the Internet.

Firewalls

■ 8660 SDM

The 8660 SDM with firewall iSDs is placed in the path between your various trusted, semi-trusted, and untrusted networks. It examines all traffic moving between the connected networks and either allows or blocks that traffic, depending on the security policies defined by the administrator.

Management interfaces

■ Local console

A local console is used for entering basic network information during initial configuration. Once the system is configured, the local console can be used to access the text-based Command Line Interface (CLI) for collecting system information and performing additional configuration. The firewall iSD console is not used to manage or install firewall policies.

■ Remote console/Check Point SMART clients

- For a list of trusted users, the administrator can separately allow or deny Telnet or Secure Shell (SSH) access to the firewall iSD CLI, and HTML or SSL access to the Browser-Based Interface. Remote access features can be used for collecting system information and performing additional configuration, but not to manage or install firewall policies.
- Check Point SMART Client software, such as the SmartDashboard, can be installed on one or more administrator workstations on your network. This software usually provides a graphical user interface (GUI) for creating, modifying, and monitoring firewall policies. For security, SMART Clients do not interact directly with the firewalls. Instead, any policy changes made in a SMART Client are forwarded to the SmartCenter Server, which then loads them onto the firewalls. For convenience, a SMART Client can be installed on the management station running the SmartCenter Server (see following Note on [page 28](#)).

■ Check Point SmartCenter Server management station

The management station running the SmartCenter Server holds the master policy database for all the firewalls in your network. Its job is to establish Secure Internal Communications (SIC) with each valid iSD and load the iSD with the appropriate security policies. The SmartCenter Server may be enabled on the iSD in the CLI setup utility.

NOTE – If you have a second firewall iSD in the cluster to implement an active-standby (High Availability [HA]) firewall configuration, you must install the SmartCenter Server on a management station. In this case, do not enable the SmartCenter Server on the firewall iSD when prompted in [Step 11](#) of the initial setup routine, which starts on [page 48](#).

Passport 8600 and firewall iSD VLANs

[Figure 1-4](#) shows the Management, Sync, and Check Point VLAN configurations.

Figure 1-4 Management, Sync, and Check Point VLANs

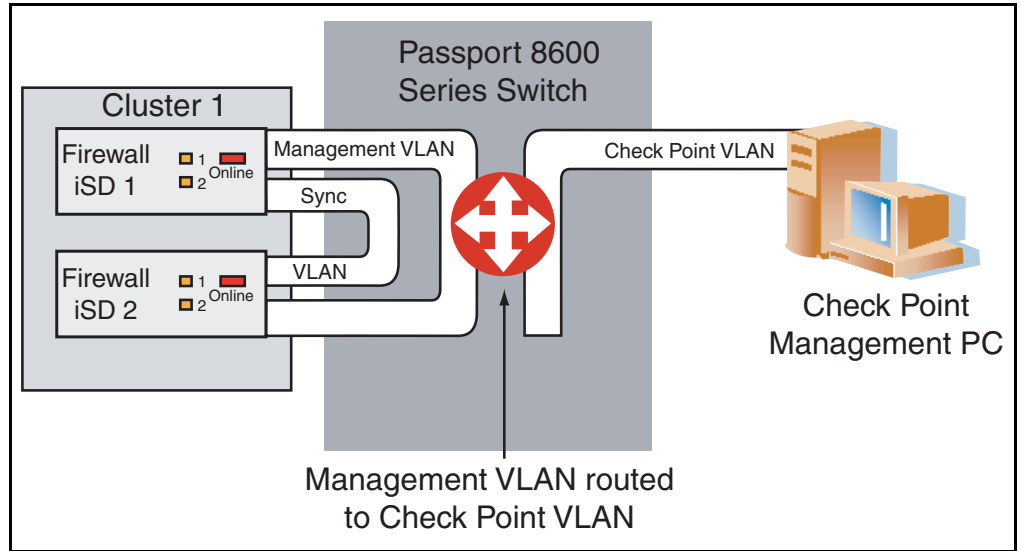


Table 1-4 describes the Passport 8600 and firewall iSD VLANs. The VLANs can be created using either CLI commands or the Java Device Manager (JDM).

Table 1-4 Passport 8600 and firewall iSD VLANs

VLAN	Description
*Management VLAN	<ul style="list-style-type: none"> ■ ID 1 - 4092 ■ Used for management of the iSDs. ■ Configured on the Passport 8600 Series Switch and on each firewall iSD. ■ Configured on logical Port 1 of each firewall iSD during device (iSD) initialization.
*Sync VLAN	<ul style="list-style-type: none"> ■ ID 1 - 4092 ■ Used when multiple devices exist in a cluster for synchronization of configurations, software, and session records. ■ Configured on the iSDs and the Passport 8600 Series Switch. ■ Configured on logical Port 2 of the firewall iSD. ■ Must have the lowest VLAN ID number configured in the cluster.
**NAAP VLAN (ID 4094)	<ul style="list-style-type: none"> ■ ID 4094 ■ Used by the Passport 8600 Series Switch for system level management of the firewall iSD. ■ Configured on the Passport 8600 Series Switch only.
**Firewall VLAN	<ul style="list-style-type: none"> ■ ID 1 - 4092 ■ L2 bridged VLAN into the firewall iSD (directs traffic in and out of the firewall iSD) ■ Results in traffic being bridged into the firewall iSD (where routing occurs), and bridged out. ■ Configured on either the trusted or the untrusted side of the firewall. ■ Maximum of 256 Firewall VLANs on the firewall iSD.
**Firewall Peering VLAN	<ul style="list-style-type: none"> ■ ID 1 - 4092 ■ Directs traffic in and out of the firewall iSD. ■ L3 routed VLAN (used to route between the firewall iSD and the Passport 8600 Series Switch (that is, they exchange routing information)). ■ Configured on either the trusted or the untrusted side of the firewall. ■ Can be more than one Firewall Peering VLAN per Passport 8600 chassis. ■ Contains only ports on the 8660 SDM slot.
**Check Point VLAN	<ul style="list-style-type: none"> ■ Used for the Check Point server connection. ■ Recommended that it be in a VLAN by itself. ■ Routed into the Management VLAN.
* Created using the “config cluster” command on the Passport 8600 Series Switch.	
** Created using the “create VLAN” command on the Passport 8600 Series Switch.	

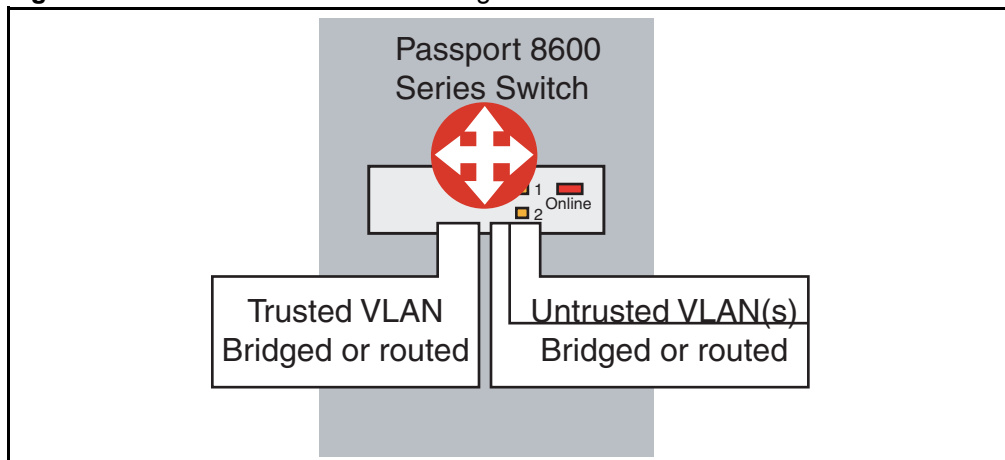
The Check Point VLAN is the normal Passport 8600 VLAN used for the Check Point management station. It is not a specific firewall VLAN. In this document, Check Point VLAN is used as a naming convention to easily identify it.

NOTE – Nortel Networks recommends that you avoid using the same VLAN ID for the Sync VLAN and the Management VLAN.

NOTE – The Sync VLAN must have the lowest VLAN ID of any configured on the firewall iSD.

Figure 1-5 shows the Firewall VLAN and Firewall Peering VLAN.

Figure 1-5 Firewall and Firewall Peering VLANs





CHAPTER 2

Initial setup

This chapter describes how to perform initial setup for configuration of an 8660 SDM. Basic configuration is performed on the firewall iSD to allow remote access using Telnet or SMART Client. The Check Point management tools are then installed on a workstation.

NOTE – For basic information on preparing the Passport 8600 Series Switch and firewall modules for initial configuration, see *Getting Started* (part number 320095-A) and *Installing the 8660 Service Delivery Module (SDM) for the Passport 8600 Series Switch* (part number 217314-A).

Overview of initial setup tasks

Initial setup involves the following tasks:

- Ensuring your network has the basic requirements ([page 32](#))
- Using the CLI for basic configuration ([page 36](#))
- Installing Check Point management tools ([page 62](#))

Basic requirements

The following requirements are needed prior to configuring the firewall iSD:

- 8660 SDM installed according to directions in *Installing the 8660 Service Delivery Module (SDM) for the Passport 8600 Series Switch* (part number 217314-A).
- Network cables attached, and module powered on and connected to a console terminal.
- 8660 SDM firewall iSDs running firewall OS version 2.2.7.0 or higher (factory-installed on new units).
- A Check Point license for each firewall iSD.
- A Check Point license for the Check Point management station, if implemented.
- *One subnet assigned for internal firewall iSD use. This subnet must consist of the following IP addresses:
 - One Management IP (MIP) address.
 - An IP address for the firewall iSD.
- A list of subnets that will be statically configured on the iSD for internal networks, plus the IP address of the internal router that handles routes for these networks.
- The IP address of the default gateway for data moving through the iSD to the Internet.
- An IP address reserved for the iSD on each trusted, untrusted, and semi-trusted subnet that will connect directly to the iSD. (You can create multiple interfaces on a single port. Each interface will have a unique IP address, subnet, vlan association.)

NOTE – *The highest IP address and lowest IP address in the subnet range are reserved for broadcasts and should not be assigned to specific devices.

Example networks

Figure 2-1 shows the example network that is the basis for the procedures that are described in this chapter. Once the network information is collected, you can use the Setup utility to initialize the firewall iSD as described in “[Initializing the firewall iSD](#)” on page 44.

In this example, the network spans 192.168.1.0/24. This is an SDM FW1 configuration — the 8660 SDM is in Slot 3 of the Passport 8600 Series Switch. Firewall iSD 4 (in mini-slot 4) is configured in this example. Ensure you have connected the console cable between the serial port on the 8660 SDM and the serial port of a computer with terminal emulation software.

Figure 2-1 Example network with the 8660 SDM FW1

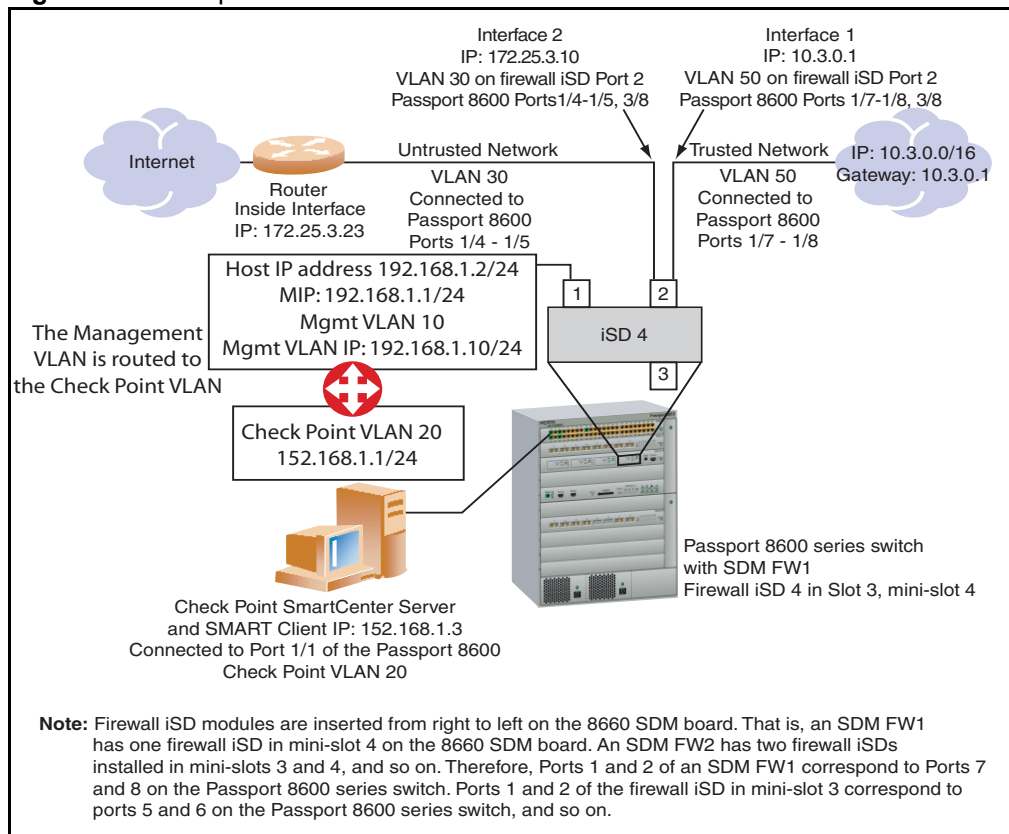
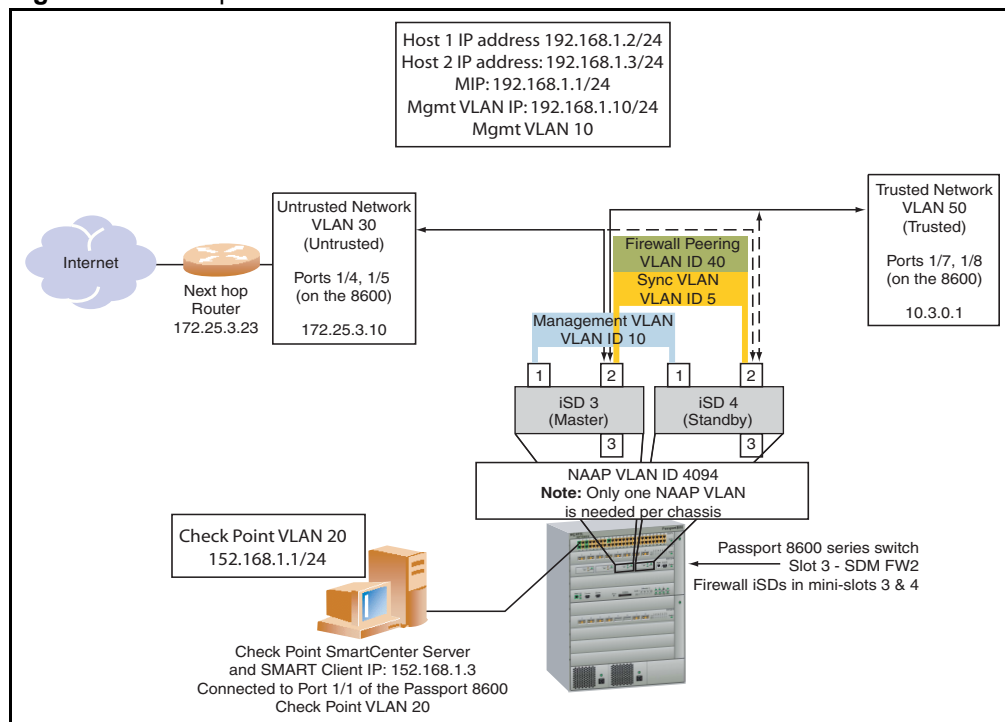


Figure 2-2 shows the example network with an 8660 SDM FW2 installed in slot 3 of the Passport 8600.

Figure 2-2 Example network with an 8660 SDM FW2



The rules for configuring networks and ports are as follows:

- You can configure one address per interface, with one network address range.
- You can assign multiple interfaces to a port (up to 255).
- Each IP interface is configured to represent a network attached to a firewall iSD.
- Interfaces on the same port cannot share the same network.
- A network device that is connected to an interface must be configured to use the interface IP address as the default gateway. This directs traffic through the iSDs.

Network elements

The network elements are the following:

- “Firewall iSD management network” on page 35
- “SmartCenter Server” on page 35
- “Trusted network” on page 36
- “Untrusted network (Internet)” on page 36

Firewall iSD management network

- The firewall iSD IP address in the example network is 192.168.1.2 and the Management IP (MIP) address is 192.168.1.1/24.
- The MIP must be configured on Port 1 of the firewall iSD. Once configured, that port cannot be assigned to an interface. Use Port 2 (of the firewall iSD) for firewall traffic.
- The MIP address supports iSD clustering with a redundant iSD in a high-availability (HA) failover configuration. That is, the Management VLAN can be used to provide sync.
- If you have only one iSD in your system, you must still configure the MIP address.

NOTE – The management network port is for administrative purposes such as the BBI, Telnet, SSH, and the Check Point management tools such as the SmartCenter Server and the SMART Client (see “[Installing Check Point management tools](#)” on page 62).

NOTE – To provide a secure remote access path for a secondary SmartCenter Server or SMART Client, you can configure it on the Trusted Network.

SmartCenter Server

You can install the SmartCenter Server on the firewall iSD host (if HA is not enabled) or on a Check Point management station. In the example network, it is implemented on a Check Point management station. The Check Point management station IP address is 152.168.1.3.

NOTE – If you have a second iSD in the cluster to implement an HA firewall configuration, you must install the SmartCenter Server on a management station. If this is your situation, do not enable the SmartCenter Server on the firewall iSD when prompted in Step 11 of “[Initializing the firewall iSD](#)” on page 44.

NOTE – If you previously installed the SmartCenter Server on the firewall iSD, you must first re-image the firewall iSD if you want to install SmartCenter Server on a Checkpoint management station.

Trusted network

- The Trusted Network IP address range is 10.3.0.0/16.
- The Trusted Network connects to logical port 2 of firewall iSD 4, which corresponds to logical port 8 on the Passport 8600 Series Switch. This is IP Interface 1. The Interface address is 10.3.0.1.

Untrusted network (Internet)

- The default gateway IP address of the firewall iSD is 172.25.3.23. This is the internal interface of the upstream router.
- The Untrusted Network connects to logical port 2 of firewall iSD 4, which corresponds to logical port 8 on the Passport 8600 Series Switch. This is IP Interface 2. The Interface address is 172.25.3.10.

Using the CLI for basic configuration

This section describes initial configuration procedures using CLI commands from both the Passport 8600 Series Switch console and the firewall iSD console. For procedures to configure the firewall iSDs using the JDM, see [“Using JDM to configure firewall iSDs” on page 93](#). If you have an SDM FW2 or FW4, you must identify the firewall iSD to be configured. For commands to switch among the firewall iSDs, see [“Switching management and console ports among iSDs” on page 56](#).

New Passport 8600 CLI commands for the 8660 SDM

The following are new commands added to the Passport 8600 CLI to manage the firewall iSD:

- [“config naap” on page 37](#)
- [“show naap” on page 37](#)
- [“config cluster” on page 38](#)
- [“show cluster” on page 38](#)

config naap

Table 2-1 shows the available commands and syntax for **config naap**.

Table 2-1 Config naap

Command Syntax and Usage

```
connect <dev#> [<NAAP port#>]
disable
enable
info
minislot-state <enable|disable> <Slot#> [<Mini-Slot#>]
set-console <Slot#> <Mini-Slot#>
```

show naap

Figure 2-3 shows an example of the **show naap** command string.

Figure 2-3 Show naap

```
>Passport-8610 : 5# show cluster
Naap Information:-----
                Naap State : Enabled
                Naap Vlan : 4094
                Naap Mac : 00:05:ad:45:66:a6
Naap Inter-Chassis-Link :
    Console on Slot 2 : MiniSlot 4
    Console on Slot 8 : MiniSlot 4

Naap Peer Devices:-----
  1:      HW_ISD:SW_ASF5100      UP/UP      Local      IP192.168.1.3
        SW_IMAGE_VERSION : 2.2.7.0_sdm
        Naap Mac: 00:00:50:11:d6:46 - 2/7

  2:      HW_ISD:SW_ASF5100      UP/UP      Local      IP192.168.1.2
        SW_IMAGE_VERSION : 2.2.7.0_sdm
        Naap Mac: 00:00:50:11:56:a6 - 8/7
```

config cluster

Table 2-2 shows the available commands and syntax for **config cluster**.

Table 2-2 Config cluster

Command Syntax and Usage

```
add <Slot#> <Mini-Slot#>
create <firewall|ssl|ids|vpn>
sync vlan <value>
delete
info
mgmt vlan <value>
remove <Slot#> <Mini-Slot#>
```

show cluster

Figure 2-4 shows an example of the **show cluster** command string.

Figure 2-4 Show cluster

```
NEW 8600 CLI COMMANDS
>Passport-8610:5/config/cluster/1# show cluster
=====
                        SDM Cluster Information
=====
ID   TYPE   SIZE  MGMTVLAN  SYNCVLAN  MEMBERS
-----
1   firewall  2     10         5          (3,1) (3,2)
2   firewall  2     20         5          (3,3) (3,4)

>Passport-8610:5/config/vlan/100# create byport 1 firewall-vlan cluster 1
```

Modified Passport 8600 CLI commands for the 8660 SDM

The following commands have been modified for the Passport 8600 CLI to manage the firewall iSD:

- “`config vlan <vid> create`” on page 39
- “`show config module <value>`” on page 40

`config vlan <vid> create`

Table 2-3 shows the available commands and syntax for `config vlan <vid> create`.

Table 2-3 Config vlan <vid> create

Command Syntax and Usage

`byport <sid> [name <value>] [color <value>] [naap-vlan] [firewall-vlan] [firewall-peering-vlan] [cluster <value>]`

show config module <value>

Figure 2-5 shows an example of the **show config module <value>** command string.

Figure 2-5 Show config module <value>

```
>Passport-8010CO : 6# show config module naap
Preparing to Display Configuration...
#
# THU FEB 17 10:48:28 2005 UTC
# box type           : Passport-8010co
# software version   : REL3.7.6.0
# monitor version    : 3.7.6.0/001
#
#
# Asic info :
# SlotNum  Name      CardType  MdaType  Parts  Description
#
# Slot 1   --       0x00000001 0x00000000
# Slot 2   Alteon  SDM 0x70e20108 0x00000000      BFM: OP=3 TMUX=2 RARU=4 CPLD=9
# Slot 3   --       0x00000001 0x00000000
# Slot 4   8608GT  0x20220108 0x00000000      IOM: GMAC=4 BFM: OP=2 TMUX=2 RARU=2
CPLD=8
# Slot 5   --       0x00000001 0x00000000
# Slot 6   8690SF  0x200e0100 0x00000000      CPU: CPLD=15 SFM: OP=2 TMUX=2 SWIP=2 F
AD=1 CF=11
# Slot 7   --       0x00000001 0x00000000
# Slot 8   Alteon  SDM 0x70e20108 0x00000000      BFM: OP=3 TMUX=2 RARU=4 CPLD=9
# Slot 9   8608GT  0x20220108 0x00000000      IOM: GMAC=4 BFM: OP=2 TMUX=2 RARU=2
CPLD=4
# Slot 10  --       0x00000001 0x00000000
config

# LICENSE CONFIGURATION

mac-flap-time-limit 500

#
# NAAP CONFIGURATION
#

naap enable
naap set-console 2 4
naap set-console 8 4

back
```


Configuring the 8660 SDM

Configuring the 8660 SDM requires that you perform configurations at both the Passport 8600 Series Switch console, and at the firewall iSD console. In this example, the configurations are done first from the Passport 8600 Series Switch console. The configuration procedures include all steps to complete initial configuration on an SDM FW1, FW2, or FW4. Optional steps (based on the 8660 model) are identified where applicable.

Using the Passport 8600 Series Switch console, enter the following commands:

1. Create the firewall cluster.

```
config cluster <cluster-id> create firewall
```

Example:

```
Passport-8610:5# conf cluster 1 create firewall
```

2. Add the firewall iSD to a cluster.

```
config cluster <cluster-id> add <slot> <mini-slot>
```

Example:

```
Passport-8610:5# conf cluster 1 add 3 4
```

NOTE – Add a second firewall iSD for a two-member cluster. You must always create a cluster during initial configuration of the firewall iSD. A cluster contains either one firewall iSD, or two firewall iSDs.

3. Create the Management VLAN.

```
conf cluster <cluster-id> mgmt vlan <vid>
```

Example:

```
Passport-8610:5# conf cluster 1 mgmt vlan 10
```

4. Create the Sync VLAN (required only if the cluster will contain two firewall iSDs).

NOTE – This step is optional. If you plan to cluster firewall iSDs in HA mode, Nortel Networks recommends that you create the Sync VLAN. However, in the single firewall iSD cluster configuration (for example, [Figure 2-1 on page 33](#)), it is not necessary to configure the Sync VLAN.

```
config cluster <cluster-id> sync vlan <vid>
```

Example:

```
Passport-8610:5# conf cluster 1 sync vlan 5
```

5. Create Firewall VLANs for each firewall interface, and add them to the appropriate clusters.

```
config vlan <vid> create byport <stg-id> firewall-vlan cluster <cluster-id>
```

Example:

```
Passport-8610:5# config vlan 30 create byport 1 firewall-vlan
cluster 1
```

```
Passport-8610:5# conf vlan 30 ports add 1/4-1/5
```

```
Passport-8610:5# config vlan 50 create byport 1 firewall-vlan
cluster 1
```

```
Passport-8610:5# conf vlan 50 ports add 1/7-1/8
```

6. Create Firewall Peering VLANs and add them to the appropriate clusters.

```
config vlan <vid> create byport <stg-id> firewall-peering-vlan cluster <cluster-id>
```

```
config vlan <vid>
```

```
config vlan <vid> ip create <ip>
```

```
config ip ospf enable
```

Example:

```
Passport-8610:5# config vlan 40 create byport 1 firewall-
peering-vlan cluster 1
```

```
Passport-8610:5# conf vlan 40
```

```
Passport-8610:5# config vlan 40 ip create 192.170.1.10/24
```

```
Passport-8610:5# config ip ospf enable
```

NOTE – Open Shortest Path First (OSPF) is supported only in configurations where there is one firewall iSD in a cluster. If you plan to have two firewall iSDs in a cluster, omit the OSPF configuration commands.

7. Add the IP address for the Management VLAN on the Passport 8600 Series Switch (192.168.1.10/24).

```
config vlan <vid> ip create <ip>
```

```
config vlan <vid> ip ospf enable
```

```
config ip ospf enable
```

Example:

```

Passport-8610:5# config vlan 10 ip create 192.168.1.10/24
Passport-8610:5# config vlan 10 ip ospf enable
Passport-8610:5# config ip ospf enable

```

8. Create the VLAN for the Check Point management server.

```

config vlan <vid> create byport <stg-id>
config vlan <vid> ports add <slot> <port>
config vlan <vid> ip create <ip>
config vlan <vid> ip ospf enable
config ip ospf enable

```

Example:

```

Passport-8610:5# config vlan 20 create byport 1
Passport-8610:5# config vlan 20 ports add 1/1
Passport-8610:5# config vlan 20 ip create 152.168.1.1/24
Passport-8610:5# config vlan 20 ip ospf enable
Passport-8610:5# config ip ospf enable

```

9. Create the NAAP VLAN for communication between the Passport 8600 and the firewall iSD.

```

config vlan <vid> create byport <stg-id> naap-vlan

```

Example:

```

Passport-8610:5# conf vlan 4094 create byport 1 naap-vlan

```

10. Enable NAAP.

```

config naap enable

```

Example:

```

Passport-8610:5/config/naap# enable

```

11. Identify the firewall iSD.

```

config naap set-console <slot> <mini-port>

```

Example:

```

Passport-8610:5# config naap set-console 3 4

```

After you complete these steps, and if you have a new installation of the firewall iSD software image, connect to the firewall iSD console now to initialize the unit. See [“Initializing the firewall iSD” on page 44](#).

If you must upgrade the firewall iSD software, refer to [Chapter 11, “Upgrading the software,” on page 333](#).

If you must remove the 8660 SDM from the Passport 8600 Series Switch, refer to [“Halting disk drives on the 8660 SDM” on page 57](#).

Initializing the firewall iSD

Press **Enter** on the SDM console terminal to establish the connection. The iSD login prompt appears. Enter the default login name (`admin`) and the default password (`admin`). This connects you to the firewall iSD console. If the firewall iSD is set to factory defaults, a special Setup utility menu appears. See [Figure 2-6 on page 44](#).

NOTE – Initialization is only required on the first firewall iSD of a cluster. If you are adding a second firewall iSD to a cluster, enter the **join** command rather than **new**. For instructions to add a second firewall iSD to a cluster using the Setup utility, see [“Using the join command” on page 50](#).

NOTE – Before upgrading the software on the iSD, you must perform the initial setup procedures as explained in this chapter. Once initial setup is complete, see [Chapter 11, “Upgrading the software,” on page 333](#) for more information.

Figure 2-6 Firewall iSD Setup utility menu

```
login: admin
Password: admin (not displayed)
Alteon Firewall
HW platform: ASF
Software version 1.0.0.1

-----
[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.
```

Using the Setup utility

The following procedure is an example of the Setup utility prompts and user input for configuration. Follow the example to initialize a new installation. After answering the various Setup questions, the Check Point software is initialized.

NOTE – The IP addresses used in the following steps are taken from the example network on [page 33](#). Enter information for your specific network configuration.

1. Select a “new” installation.

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

2. Enter the port number to be used for the management network.

Port 1 must be used for management with this release.

```
Enter port number for the management network [1-3]: 1
```

3. Enter the host IP address for this firewall iSD:

There is one host IP address for each firewall iSD. This is the IP address you want to assign to the firewall iSD.

```
Enter IP address for this machine: 192.168.1.2
```

4. Enter the network mask for the entire subnet:

```
Enter network mask [255.255.255.0]: 255.255.255.0
```

5. Enter the Management VLAN ID.

This Management VLAN must have the same VLAN ID as the Management VLAN created on the Passport 8600 Series Switch. See [“Create the Management VLAN.” on page 41](#).

```
Enter VLAN tag id (or zero for no VLAN) [0]: 10
```

6. Enter the Management IP (MIP) address information.

These addresses must be in the subnet.

```
Enter the Management IP (MIP) address: 192.168.1.1
Making sure the MIP does not exist...ok
```

7. Set your time zone by selecting continent or ocean, then country, then region.

For example:

```
Timezone setting
1 - Africa
2 - Americas
3 - Antarctica
4 - Arctic Ocean
5 - Asia
6 - Atlantic Ocean
7 - Australia
8 - Europe
9 - Indian Ocean
10 - Pacific Ocean
Select a continent or an ocean: 2
```

```
Countries:
1 - Anguilla
2 - Antigua & Barbuda
3 - Argentina
4 - Aruba
5 - Bahamas
6 - Barbados
7 - Belize
8 - Bolivia
9 - Brazil
10 - Canada
11 - Cayman Islands
12 - Chile
13 - Colombia
14 - Costa Rica
15 - Cuba
16 - Dominica
17 - Dominican Republic
18 - Ecuador
19 - El Salvador
20 - French Guiana
21 - Greenland
22 - Grenada
23 - Guadeloupe
24 - Guatemala
25 - Guyana
26 - Haiti
27 - Honduras
28 - Jamaica
29 - Martinique
30 - Mexico
31 - Montserrat
32 - Netherlands Antil
33 - Nicaragua
34 - Panama
35 - Paraguay
36 - Peru
37 - Puerto Rico
38 - St Kitts & Nevis
39 - St Lucia
40 - St Pierre & Mique
41 - St Vincent
42 - Suriname
43 - Trinidad & Tobago
44 - Turks & Caicos Is
45 - United States
46 - Uruguay
47 - Venezuela
48 - Virgin Islands (U
49 - Virgin Islands (U
Select a country: 45
```

Regions:

```

1 - Adak Aleutian Islands
2 - Anchorage Alaska Time
3 - Boise Mountain Time - south Idaho & east Oregon
4 - Chicago Central Time
5 - Denver Mountain Time
6 - Detroit Eastern Time - Michigan - most locations
7 - Honolulu Hawaii
8 - Indiana/Knox Eastern Standard Time - Indiana - Starke County
9 - Indiana/Marengo Eastern Standard Time - Indiana - Crawford County
10 - Indiana/Vevay Eastern Standard Time - Indiana - Switzerland Cnty
11 - Indianapolis Eastern Standard Time - Indiana - most locations
12 - Juneau Alaska Time - Alaska panhandle
13 - Kentucky/Monticello Eastern Time - Kentucky - Wayne County
14 - Los_Angeles Pacific Time
15 - Louisville Eastern Time - Kentucky - Louisville area
16 - Menominee Central Time - Michigan - Wisconsin border
17 - New_York Eastern Time
18 - Nome Alaska Time - west Alaska
19 - North_Dakota/Center Central Time - North Dakota - Oliver County
20 - Phoenix Mountain Standard Time - Arizona
21 - Shiprock Mountain Time - Navajo
22 - Yakutat Alaska Time - Alaska panhandle neck
Select a region: 17

```

8. Set the current date and time:

```

Enter the current date (YYYY-MM-DD) [2004-01-05]:<Enter to accept default>
Enter the current time (HH:MM:SS) [13:14:09]:<Enter>

```

9. Generate a new Secure Shell (SSH) host key for use with secure remote administration sessions:

```

Generate new SSH host keys (yes/no) [yes]: y
This may take a few seconds...ok

```

Nortel Networks recommends that you generate a new SSH key to maintain a high level of security when connecting to an iSD using an SSH client.

10. Set the new administrator password.

The current default administrator password is admin. Nortel Networks recommends that you change the password.

```
Enter a password for the "admin" user: <password>
Re-enter to confirm: <password>
```

11. Choose whether to enable the Check Point SmartCenter Server on the firewall iSD.

NOTE – The first time you initialize a firewall iSD, you are presented with the Check Point SmartCenter Server options as described in this Step. If you have previously initialized the firewall iSD, these options will not appear. If you wish to repeat the initialization process, including enabling the Check Point SmartCenter Server, you must first re-install the firewall iSD software.

Setup gives you the option of configuring your firewall iSD with or without a co-located SmartCenter Server. Enabling the SmartCenter Server on the management interface lets you use the interface without requiring Secure Internal Communications (SIC) and without a second license required for hosting the SmartCenter Server on the management station. However, you cannot take advantage of this feature if you intend to install a second firewall iSD in a cluster with this one. In that case, you must enter 1 at the prompt and install the SmartCenter Server on the management station.

For Check Point NG with Application Intelligence software, Setup provides two options (selections 3 and 4) that support Check Point Express licensing. See Check Point documentation for more information on Check Point Express.

NOTE – If you install the SmartCenter Server on the firewall iSD now, but decide later to add a second firewall iSD to the cluster (to implement an HA firewall iSD configuration), you must re-image your system and repeat Setup to uninstall the SmartCenter Server.

```
Select installation type:
1. Check Point Gateway
2. Check Point Gateway and SmartCenter Server
3. Check Point Gateway Express
4. Check Point Gateway Express and SmartCenter Server
Enter your selection: (1/2/3/4) [1]:
```


12. If you chose 2 or 4 in [Step 11 on page 48](#), enter the management server administrative password.

```
Enter Check Point Primary SmartCenter Server admin password:
<password>
Re-enter to confirm: <password>
```

13. If you chose 1 or 3 in [Step 11 on page 48](#), you will be prompted to set the Check Point SIC one-time password.

The SIC password is required later when you establish SIC between an external Check Point management station and a firewall iSD. Check Point documentation refers to this password as the “Authentication Key” (see [page 79](#)).

```
Enter onetime SIC password: <SIC password>
Re-enter to confirm: <SIC password>
```

14. Allow self-configuration to complete.

Once the basic configuration information has been entered, the system begins a phase of self-configuration and initialization. During this phase, a series of messages are displayed. **The self-configuration phase is complete when the following message is displayed:**

```
Applying Check Point firewall and SmartCenter Server settings...
Initializing system.....ok
Configuring firewall...Done
Setup successful. Relogin to configure.

login:
```

The firewall iSD you have initialized reboots at the end of the self-configuration phase.

To install the Check Point license, see “[Setting the license key](#)” on [page 54](#).

Using the join command

If you have initialized a firewall iSD, use the **join** command to add a second iSD to form a cluster.

NOTE – You must add the second firewall iSD to the cluster before proceeding. Use either the 8600 CLI (see [Step 2 on page 41](#)) or the JDM (see [Chapter 3, “Using JDM to configure firewall iSDs,” on page 93](#)) to add the second firewall iSD to the cluster.

1. At the Setup# prompt, enter join.

```
>> Setup# join
```

2. Enter the port number to be used for the management network.

Port 1 must be used for management with this release.

```
Enter port number for the management network [1-3]: 1
```

3. Enter the host IP address for this firewall iSD:

There is one host IP address for each firewall iSD. This is the IP address you want to assign to the firewall iSD.

```
Enter IP address for this machine: 192.168.1.3
```

4. Enter the management VLAN ID.

This management VLAN must have the same VLAN ID as the management VLAN created on the Passport 8600 Series Switch. See [“Create the Management VLAN.” on page 41](#).

```
Enter VLAN tag id (or zero for no VLAN) [0]: 10
```

5. Enter the Management IP (MIP) address information.

The host IP and MIP addresses must be in the subnet. The MIP entered here must be the same as that specified on the first firewall iSD.

```
Enter the Management IP (MIP) address: 192.168.1.1
Making sure the MIP does not exist...ok
```

Once the Setup utility has been used for basic system configuration, the Setup menu is no longer displayed upon subsequent logins. Instead, the CLI Main Menu is displayed:

```
[Main Menu]
  info      - Information Menu
  cfg       - Configuration Menu
  boot      - Boot Menu
  maint     - Maintenance Menu
  diff      - Show pending config changes [global command]
  apply     - Apply pending config change [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]

>> Main#
```

Creating the firewall interface

Once you have initialized the firewall iSD, create the firewall interfaces.

Configure VLAN 5 (sync VLAN), VLAN 30 (untrusted side of the network) and VLAN 50 (trusted side of the network) on the firewall iSD.

From the firewall iSD console, enter the following:

```
/cfg/net/if 5
mask 255.255.255.0
vlan 5
port 2
en
apply
```

```
/cfg/net/if 30
addr1 172.25.3.10
mask 255.255.255.0
vlan 30
port 2
en
apply
```

```
/cfg/net/if 40
addr1 192.170.1.10
mask 255.255.255.0
vlan 40
port 2
en
apply
```

```
/cfg/net/if 50
addr1 10.3.0.1
mask 255.255.255.0
vlan 50
port 2
en
apply
```

NOTE – Port 2 of the firewall iSD is the default port for firewall interfaces — you do not need to enter this information. Port 1 of the firewall iSD is only for management. Do not create a firewall interface on this port.

NOTE – VLAN tags configured on a firewall iSD interface allow the VLAN-configured hosts on that interface to participate as VLAN members. By default, you must specify a VLAN ID for every interface created on an individual iSD. The VLAN IDs should match corresponding 8600 VLAN IDs.

Configuring VRRP

Virtual Router Redundancy Protocol (VRRP) allows devices to have a next hop or default gateway that is always available. Virtual Router Identifier (VRID) is used to distinguish between VRRP messages. Configure VRRP and VRID for clusters containing two firewall iSDs in HA mode.

In this example, firewall iSDs being clustered are in mini-slots 3 and 4 of the 8660 SDM.

Configure the sync VLAN:

```
/cfg/net/if 5/vrrp
ip1 5.5.5.2
ip2 5.5.5.3
vrid 5
```

Configure VRRP sub-address and VRID:

```
/cfg/net/if 30/vrrp
ip1 172.25.3.1
ip2 172.25.3.2
vrid 30
```

```
/cfg/net/if 50/vrrp
ip1 10.3.0.2
ip2 10.3.0.3
vrid 50
```

On each firewall iSD, you must enable HA:

```
/cfg/net/vrrp/ha y
apply
```

Synchronize the firewall iSDs:

```
/cfg/fw/sync
en
apply
```

Configuring the firewall iSD and Check Point SmartCenter Server static routes

From the firewall iSD console, do the following:

1. **Create a static route on the firewall iSD to 152.168.1.3 subnet.**

Example:

```
>>Main# /cfg/net/adv/route/routes/add 152.168.1.3
255.255.255.255 192.168.1.10
>>Main# apply
```

2. **Repeat step 1 for other clusters.**

Repeat the above steps for other clusters if they share the same policies, and if one Check Point management station is to control all clusters.

3. **Create a static route on the Checkpoint SmartCenter Server to 152.168.1.3 subnet.**

Example:

```
c: route add -p 192.168.1.0 255.255.255.0 152.168.1.1
```

Setting the license key

During this portion of the initialization process, you must install additional networks and a Check Point license. Each firewall iSD is required to have its own Check Point license.

NOTE – The 8660 SDM ships with a 15-day trial license that auto-installs for new or join installations. After the trial period ends, a license error appears when you try to push policies to the iSDs.

If local licensing is used, enter Check Point licensing information for the firewall iSDs.

NOTE – If central licensing is used, skip this step. With central licensing, the license is pushed from the Check Point SmartCenter Server in a later step.

The license information will be part of your Check Point package. The license(s) you received from Check Point should be specifically configured for your iSD Host IP addresses.

Example:

- Expiry date: 01jun2005

- Feature string: CPSUITE-EVAL-3DES-NG CK-CHECK-POINT
- License string: dSYUjTPHO-RytGHckej-MiiS47a8N-isML6Vfnn

NOTE – Be sure to enter the information exactly as shown on your specific Check Point license.

Use the following CLI commands to install your Check Point licenses on each firewall iSD, and configure information about the network.

```

>> # /cfg/pnp/add
Enter the IP Address :
Enter the Expiry date for the License :<Expiration date>
Enter the Feature string :<Feature string>
Enter the License string :<License string>
Changes applied successfully.
```

You can also use the following command by logging in to the shell:

```

*****
cplic put 10.10.1.1 10Mar2005 aUGiiv4th-CwFtsefjy-aZJpfDeTl-q4D7MxJij
cpmp-eval-1-3des-ng CK-E28A2HK753CE
*****
```

Switching management and console ports among iSDs

For an SDM FW2 or SDM FW4, you must switch management and console ports among the firewall iSDs to have configuration access to each. This section describes those commands.

Switching iSDs

1. Determine which firewall iSD is connected to the 8660 SDM console port.

Use the `config naap info` command:

```
Passport-8610:5# conf naap info
```

```
Naap Information:
```

```
=====
```

```
Naap State: Enabled
```

```
Naap Vlan: 4094
```

```
Naap Stg: 1
```

```
Naap Mac: 00:80:2d:ba:d4:00
```

```
Naap Inter-Chassis-Link:
```

```
Console on Slot 3: MiniSlot 4
```

```
Naap Peer Devices:
```

```
=====
```

```
1: HW_ISD:SW_ASF5100 UP/UP Local IP192.168.1.2
   SW_IMAGE_VERSION: 2.2.7.0_sdm
```

```
Naap Mac: 00:00:50:11:56:a6 - 3/7
```

```
2: HW_ISD:SW_ASF5100 UP/UP Local IP192.168.1.3
   SW_IMAGE_VERSION: 2.2.7.0_sdm
```

```
Naap Mac: 00:00:50:11:5a:32 - 3/5
```

NOTE – The naap peer device numbering (indexing) is created in the order that firewall iSDs are configured.

2. Select the firewall iSD to which you want to connect.

Use the `config naap set-console <slot#> <minislot#>` command:

```
config naap set-console 3 3
```



```
Passport-8610:5/config/naap# CPU5 [03/04/05 11:29:13] CPU
INFO Console on SDM Blade: 3 set to MiniSlot: 3
```

NOTE – The confirmation message shown in Step 2 does not appear in a Telnet session. If you are not using a Telnet session, see Step 3 to confirm the correct firewall iSD is selected.

3. Confirm the `set-console` change.

Re-issue the `config naap info` command to confirm that the console port has switched to the correct firewall iSD (in this example, the firewall iSD in slot 3, mini-slot 3).

Halting disk drives on the 8660 SDM



CAUTION—Every firewall iSD — including non-configured iSDs — must be halted prior to removing an 8660 SDM from the chassis, or for power cycling the 8660 SDM. Failure to do so can seriously damage the disk drives, and cause loss of data. Disk drives will become operational automatically when the 8660 SDM is re-inserted in the chassis slot.

You can access the 8660 SDM CLI using one of two methods:

- through the 8600 CPU serial port/Telnet
- through the 8660 SDM serial port

You must use the 8660 SDM console port to halt firewall iSDs that are not configured or registered with the 8600. When connecting directly to the 8660 SDM serial port, you must use the 8600 CLI `config naap set-console` command to specify the firewall iSD. The `config naap connect` command is used to connect to a firewall iSD from the 8600 CPU serial port/Telnet.

To select a firewall iSD to halt, see [“Switching management and console ports among iSDs” on page 56](#).

Halting configured firewall iSDs

Log in from the Passport 8600 console to connect to the firewall iSD and proceed as follows for a configured firewall iSD:

1. Identify the `naap peer devices`.

Use the `config naap info` command:

```
Passport-8610:5# conf naap info
```

See “Switching iSDs” on page 56 for an example of the `conf naap info` command output.

2. Connect to the first naap peer device (firewall iSD).

Use the `connect <dev#> [<NAAP port#>]` command:

NOTE – When you enter the `conf naap info` command, the output includes naap peer devices. These are listed in numerical order. Refer to this numbering scheme when entering the `<dev#>` variable. See “Switching iSDs” on page 56 for an example of the `conf naap info` command output. In this example, you are connecting to naap peer device 1, which is the 8660 SDM in slot 3, minislots 4 (that is, the firewall iSD connected to logical port 7).

```
Passport-8610:5/config/naap# connect 1
```

```
Trying to connect to Naap Peer 00:00:50:11:56:a6...
```

```
Connection established:
```

```
login: admin
```

```
Password:
```

```
Alteon Firewall
```

```
Hardware platform: ASF Launch Pad
```

```
Software version: 2.2.7.0_sdm
```

```
-----
```

```
[Main Menu]
```

```
info - Information 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]
```

```
>> Main# boot
```

```
-----
```

```
[Boot Menu]
software - Software Management Menu
halt - Halt the iSD
reboot - Reboot the iSD
delete - Delete the iSD

>> Boot# halt

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

Power down
```

NOTE – Ensure all firewall iSDs associated with an 8660 SDM are halted before powering down or removing the 8660 SDM from the switch. The `Power down` message is displayed when the firewall iSD is successfully halted.

```
>> Main# exit

Session terminated.

Naap Peer connection closed
```

NOTE – You can also enter `quit` or `q` to exit.

Repeat Step 2 for each naap peer device (that is, firewall iSD) in the SDM FW2 or SDM FW4 that you will power down or remove.

Halting non-configured firewall iSDs

For non-configured firewall iSDs, use the following steps to halt a firewall iSD:

1. **Log in from the Passport 8600 series switch console.**
2. **Determine which firewall iSD is connected to the 8660 SDM console port.**

Use the `config naap info` command:

```
Passport-8610:5# conf naap info
```

See “Switching iSDs” on page 56 for an example of the `config naap info` command output.

3. Select a firewall iSD.

Use the `config naap set-console` command to select a different iSD than the one connected to the console port.

```
config naap set-console 3 4
```

4. Log in from the 8660 SDM console serial port.

```
login: admin
```

```
Password:
```

```
Alteon Firewall
```

```
Hardware platform: ASF Launch Pad
```

```
Software version: 2.2.7.0_sdm
```

```
-----  
[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# boot
```

```
-----  
[Boot Menu]
```

```
software - Software Management Menu
```

```
halt - Halt the iSD
```

```
reboot - Reboot the iSD
```

```
>> Boot# halt
```

```
Confirm action 'halt'? [y/n]: y
```

```
Power down
```

NOTE – Ensure all firewall iSDs associated with an 8660 SDM are halted before powering down or removing the 8660 SDM from the switch. The `Power down` message is displayed when the firewall iSD is successfully halted.

```
>> Main# exit
```

```
Session terminated.
```

```
Naap Peer connection closed
```

NOTE – You can also enter **quit** or **q** to exit.

Repeat Steps 2 and 3 for each naap peer device (that is, firewall iSD) in the SDM FW2 or SDM FW4 that you will power down or remove.

Reinitializing halted firewall iSDs

If you halt the disk drives, but do not remove the 8660 SDM from the chassis slot (or otherwise do not remove power), you must disable and then enable the iSD to bring it back up.

Halt and reinitialize (power cycle) the disk drives as follows:

```
Passport-8610:5# config naap minislot-state disable 3 3
Halt ISDS before disabling minislot-state. Do you want to
continue? (y/n)? y
```

Power down

```
Passport-8610:5# config naap minislot-state enable 3 3
```

NOTE – Enabling the firewall iSD reboots iSD. The reboot takes about 3 minutes.

Allowing SMART Client access to the iSDs

The following procedure gives firewall iSD access to a Check Point SMART Client when the SmartCenter Server is enabled on a firewall iSD. If the SmartCenter Server was not installed on the firewall iSD during the initial setup, this procedure is not required.

1. At the firewall iSD console, login as admin and enter the following commands:

```
>> /cfg/fw/client/add 152.168.1.3          <Network Example SMART Client IP
address>
>> apply
```

The command `/cfg/fw/client/add` adds a new member to the list of SMART Clients that can manage the SmartCenter Server on the firewall iSD. SMART Clients interface directly with the Check Point SmartCenter Server, which interfaces with the iSD. For other commands that allow you to delete members or reorder the list, see [“/cfg/fw/client” on page 208](#).

2. Enter the following command to allow traffic between the SmartCenter Server on the firewall iSD and recently added SMART Clients.

```
>> Main# apply
>> Main# /cfg/fw/dis
>> Firewall Configuration# apply
>> Firewall Configuration# /cfg/fw/ena
>> Firewall Configuration# apply
```

Allow several minutes for the FireWall-1 services to stop before entering the `/cfg/fw/ena`.

NOTE – Traffic is interrupted by the `/cfg/fw/dis` command until the FireWall-1 services are re-enabled by the `/cfg/fw/ena` command.

3. Launch the Check Point SmartDashboard to connect to the SmartCenter Server.

Installing Check Point management tools

The 8660 SDM uses standard Check Point software tools to install, maintain, and monitor firewall policies. You can install the SmartCenter Server on a firewall iSD or on a remote management station. You can install the SMART Client on the same machine as the

SmartCenter Server, or on a separate machine that can be reached from the SmartCenter Server. If you have two iSDs in the cluster, you must implement the SmartCenter Server on the management station.

The following Check Point tools must be installed on appropriate administrator workstations in your network:

- Check Point SmartCenter Server—The SmartCenter Server is the central database for your 8660 SDM board. The SmartCenter Server establishes secure communications with your firewall iSDs, stores firewall policies, and uploads the policies to the iSDs as necessary. The SmartCenter Server can be enabled on the firewall iSD during initial setup (see “[Initializing the firewall iSD](#)” on page 44).
- Check Point SMART Clients—SMART Clients interface with the SmartCenter Server to provide a GUI for creating, editing, updating, and monitoring firewall security policies. The SMART Client software can be installed on administrative workstations in your network or on the same workstation as the SmartCenter Server.

NOTE – If you have already enabled the SmartCenter Server in the initial setup ([Step 11 on page 48](#)), or if you have installed an appropriate SmartCenter Server and SmartDashboard on workstations in your network, proceed to “[Defining a firewall object in the SmartDashboard](#)” on page 76.”

Editing the Windows NT hosts file

For Windows NT-based installations, edit the Windows NT hosts file to include the firewall iSD information. This step allows the Check Point management station to recognize an iSD's IP address and name. It is recommended that you edit the hosts file before you install the Check Point management station software.

1. Edit the `c:\winnt\system32\drivers\etc\hosts` file on the Check Point SmartCenter Server and add one line with the firewall iSD IP address and name. For example, to associate the firewall iSD “isd1” with its host IP address, enter the following:

```
192.168.1.2 isd1
```

You are now ready to proceed with the Check Point management station as described in “[Installing Check Point SmartServer and SmartConsole](#)” on page 64.

Installing Check Point SmartServer and SmartConsole

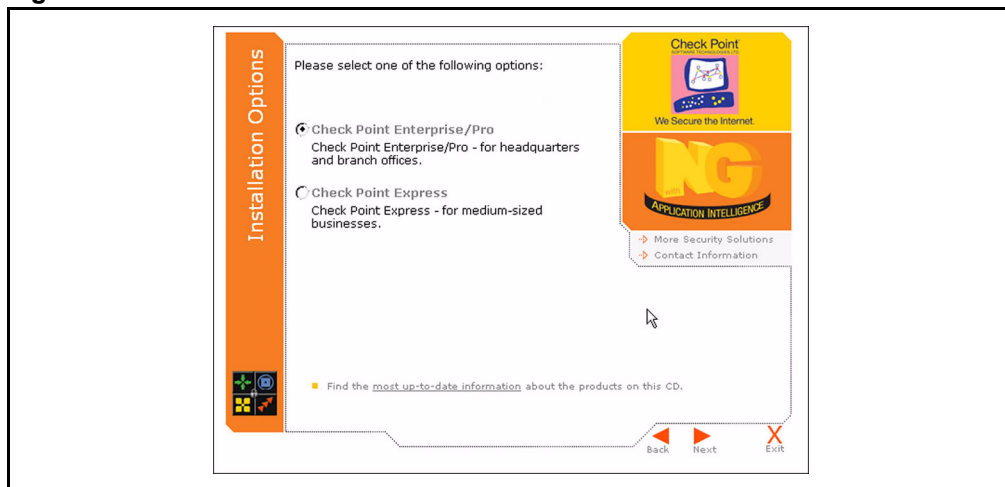
This procedure describes how to install the Check Point management tools (SmartServer and SmartConsole) for VPN-1 Pro NG with Application Intelligence (R55).

Before you begin installation, make sure your management station meets or exceeds the following minimum requirements:

- Operating System: Windows NT 4.0 SP6a or Windows 2000 Server and Advanced Server (SP2)
- Processor: Intel Pentium II 300 MHz or better
- Disk space: 40 MB
- Memory: 256 MB
- Check Point Management Suite software (R55)
- Access to the management network on the firewall iSD

1. Launch the Check Point Management Suite setup program on the management station. The installation program begins with the screen prompt shown in Figure 2-7.

Figure 2-7



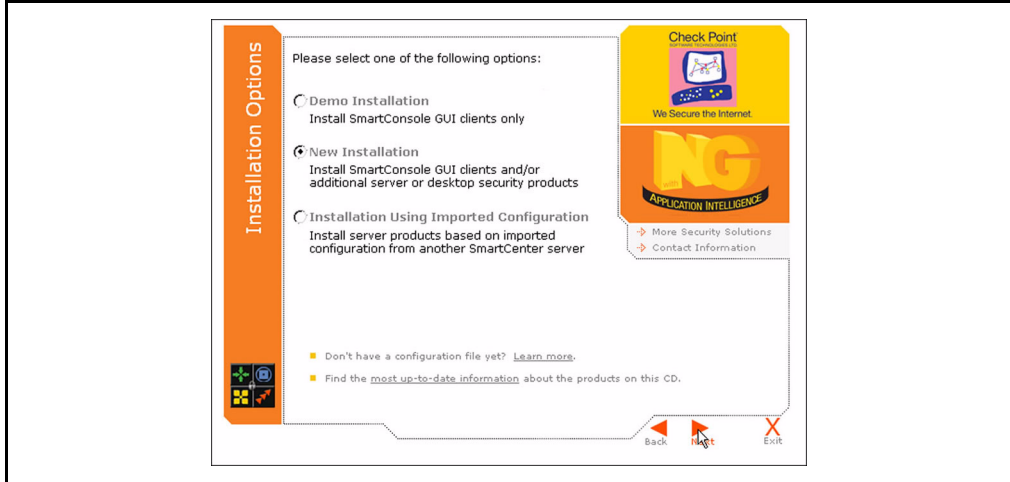
You can choose either Check Point Enterprise/Pro or Check Point Express, but be sure you match the selection you made in [Step 11 on page 48](#) during the initial setup procedure for the firewall iSD host. For a description of the Check Point Enterprise/Pro and Express features, refer to the Check Point web site:

<http://www.checkpoint.com/products/enterprise/smartcenter.html>

2. After choosing the installation option, click Next.

3. When prompted, check **New Installation**, then click **Next**. See **Figure 2-8**.

Figure 2-8

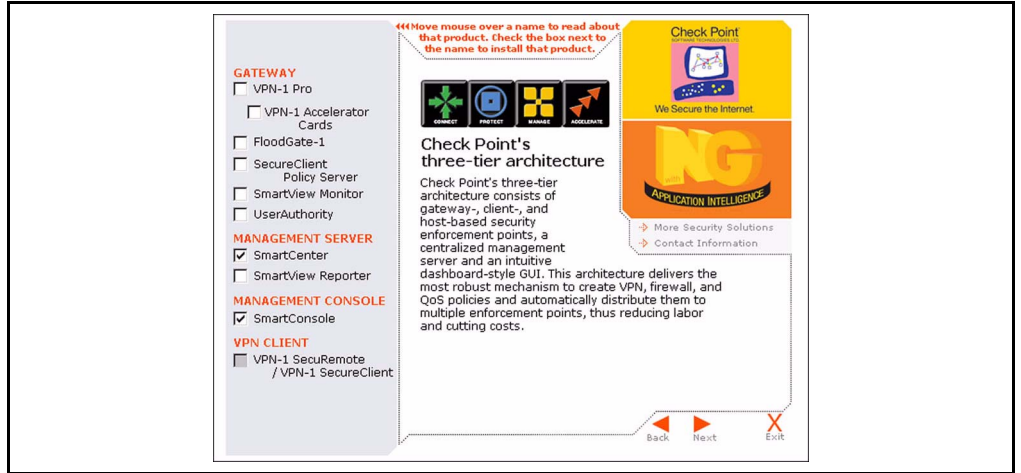


4. When prompted, check **SmartCenter (optional)** and **SmartConsole**, then click **Next**. See **Figure 2-9 on page 66**.

Check SmartCenter if you selected 1 or 3 in **Step 11 on page 48**; do not check SmartCenter if you selected 2 or 4. The SmartConsole selection includes all of the GUI Client tools you need for the SMART Client that administers the Check Point features on the firewall iSD.

NOTE – You can have multiple SMART Clients by installing the SmartConsole components on additional workstations separate from the primary management workstation. For these instances, do not select SmartCenter.

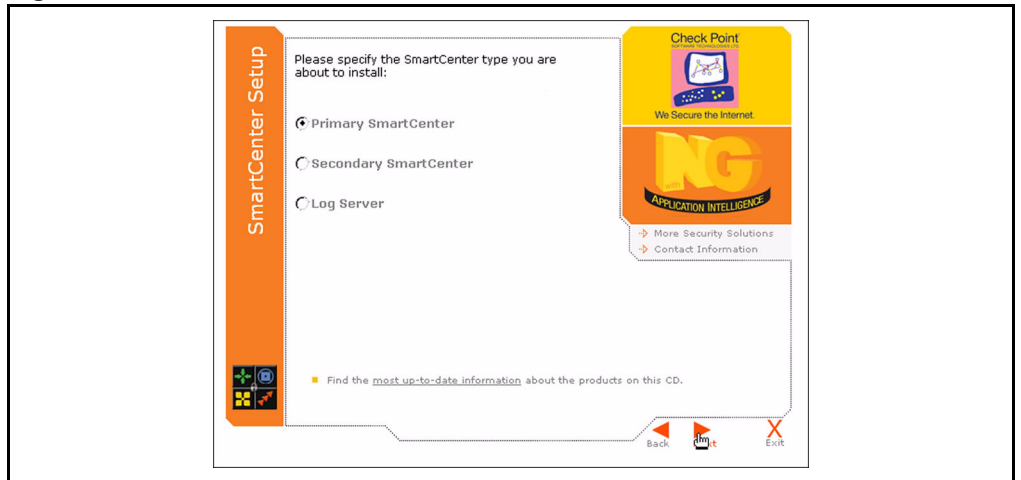
Figure 2-9



5. When prompted, check Primary SmartCenter, then click Next. See Figure 2-10.

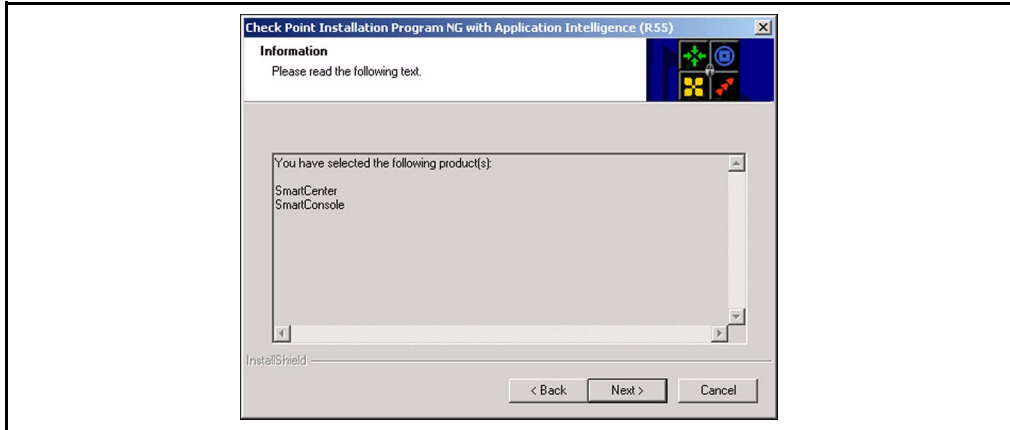
NOTE – This screen appears only if you checked the SmartCenter box in Step 4 on page 65.

Figure 2-10



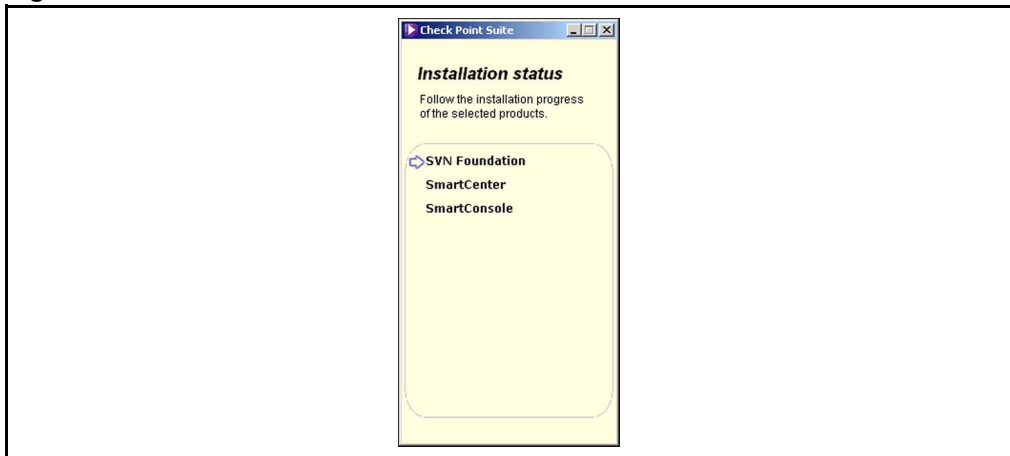
6. The Information screen confirms the product choices you have made. If these are correct, click Next. See [Figure 2-11](#).

Figure 2-11



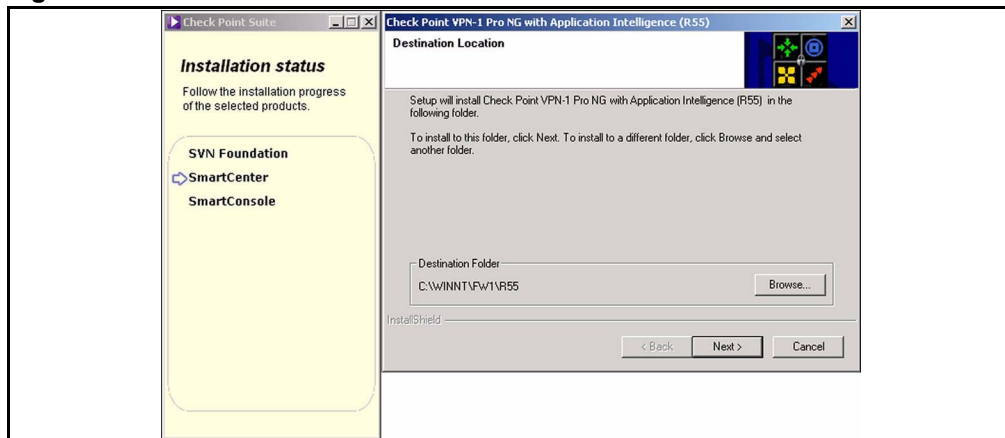
At this point, the program installs the SVN Foundation software (standard), SmartCenter (if selected), and SmartConsole components. The Installation Status window displays the information status. See [Figure 2-12](#).

Figure 2-12



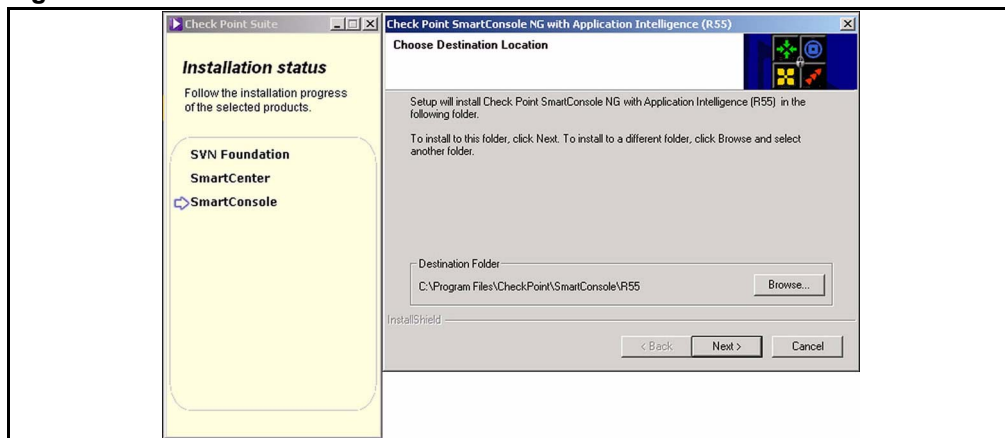
7. When prompted, click Next to continue. See [Figure 2-13](#).

Figure 2-13



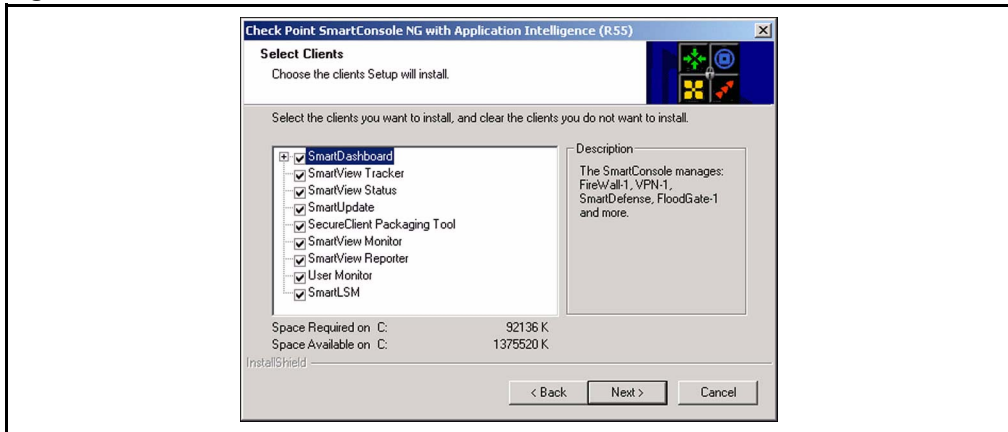
8. When prompted, click Next to continue. See [Figure 2-14](#).

Figure 2-14



9. When prompted, specify the SmartConsole components to be installed. See [Figure 2-15](#).

Figure 2-15

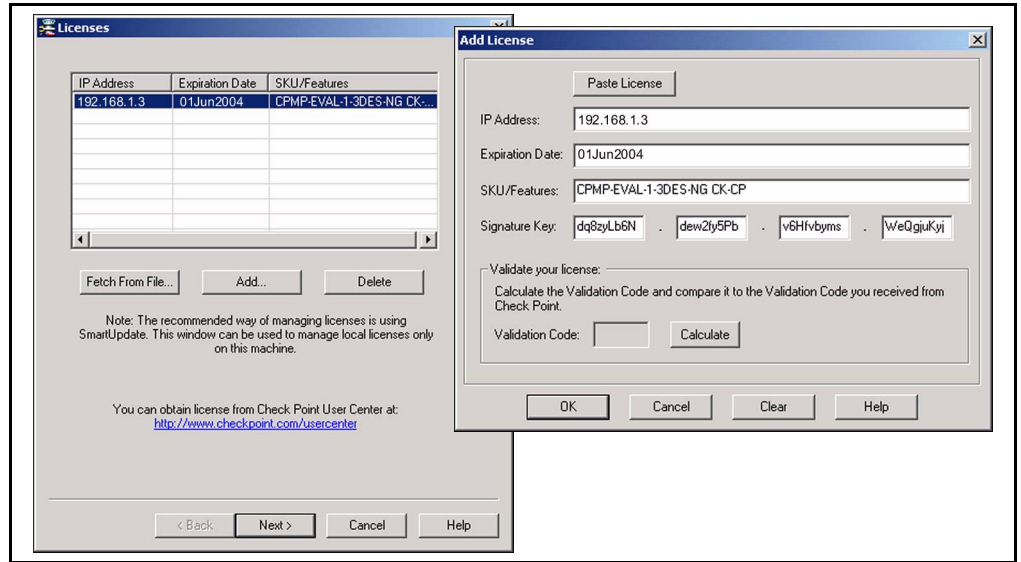


Check Point Enterprise/Pro preselects all the SmartConsole components. Check Point Express preselects the top four components. Refer to the Check Point web site for a description of the selection rationales (see [Step 1](#) on [page 64](#)).

NOTE – In previous versions of the Check Point management tool software, backward compatibility was an option. With R55, backward compatibility is a standard feature that is installed in the background.

10. When prompted, specify a valid Check Point license for the SmartCenter Server. Click the Fetch From File... or Add... button (see [Figure 2-16](#), left) and specify the appropriate license data (see [Figure 2-16](#), right).

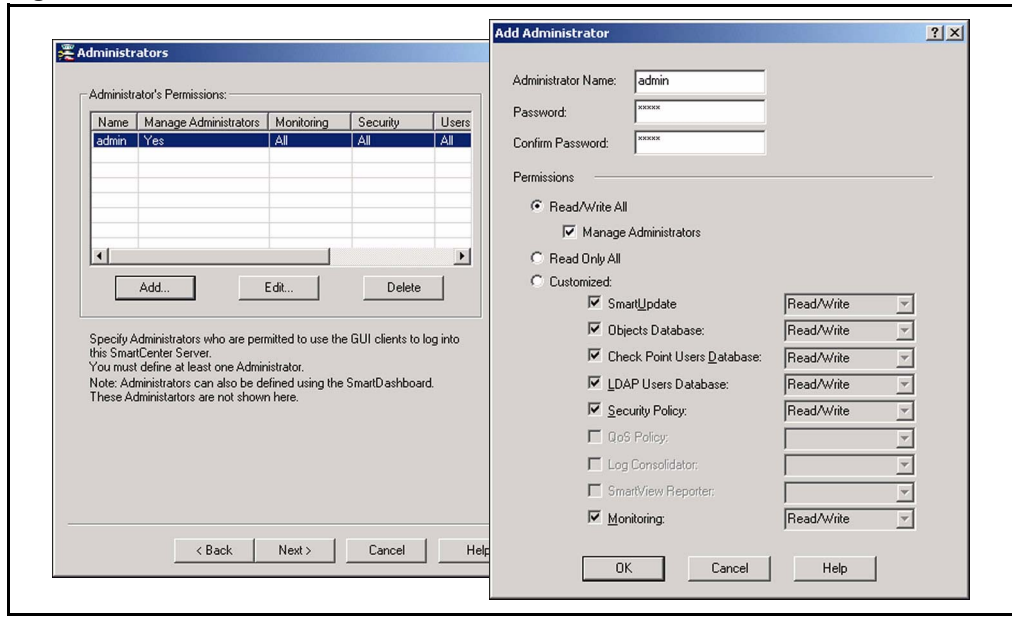
Figure 2-16



When you have entered the license data, click OK, and Next.

11. When prompted, click the Add... button (see [Figure 2-17](#), left) and enter login information for SmartCenter administrators (see [Figure 2-17](#), right).

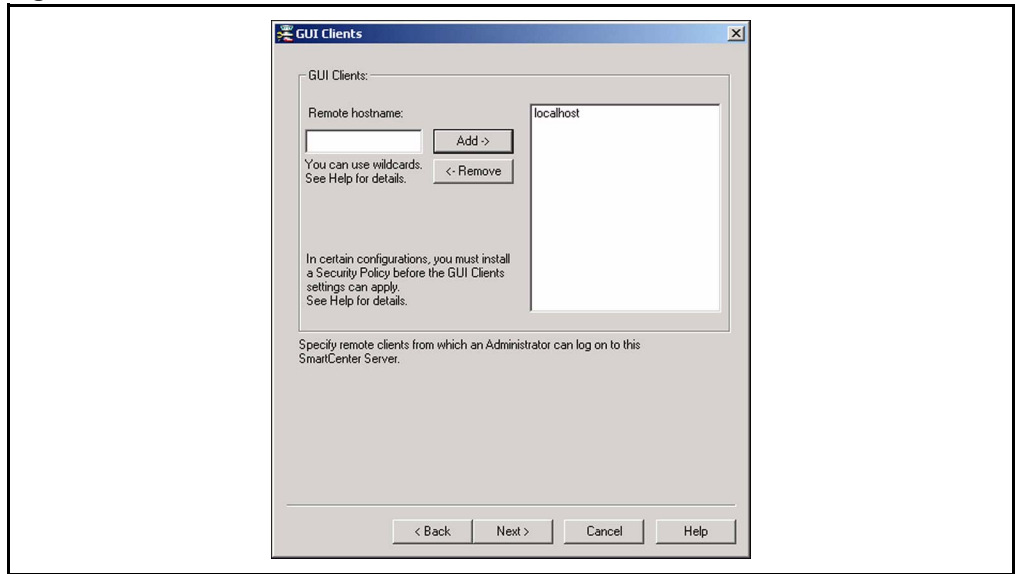
Figure 2-17



When you have entered the administrator information, click OK and Next.

12. When prompted, add any remote GUI Clients (also known as SMART Clients). See [Figure 2-18](#).

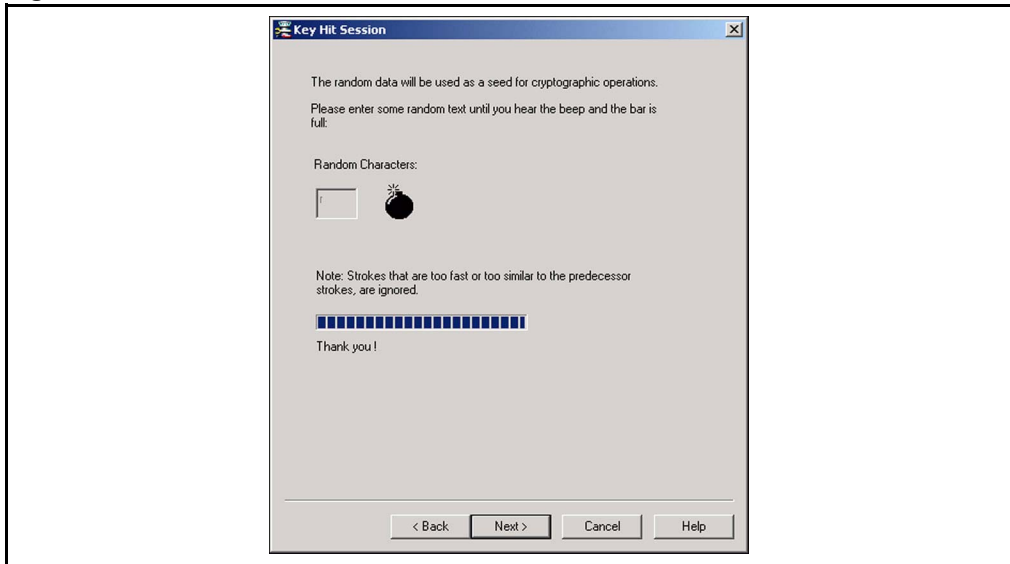
Figure 2-18



Enter *localhost* or the host's IP address if the GUI client is on the same host as the SmartCenter Server. Also specify the DNS hostname or IP address of other management clients that will be permitted to interface with this management station. Click Next to continue.

13. When prompted, type random characters for the cryptographic seed. See [Figure 2-19](#).

Figure 2-19

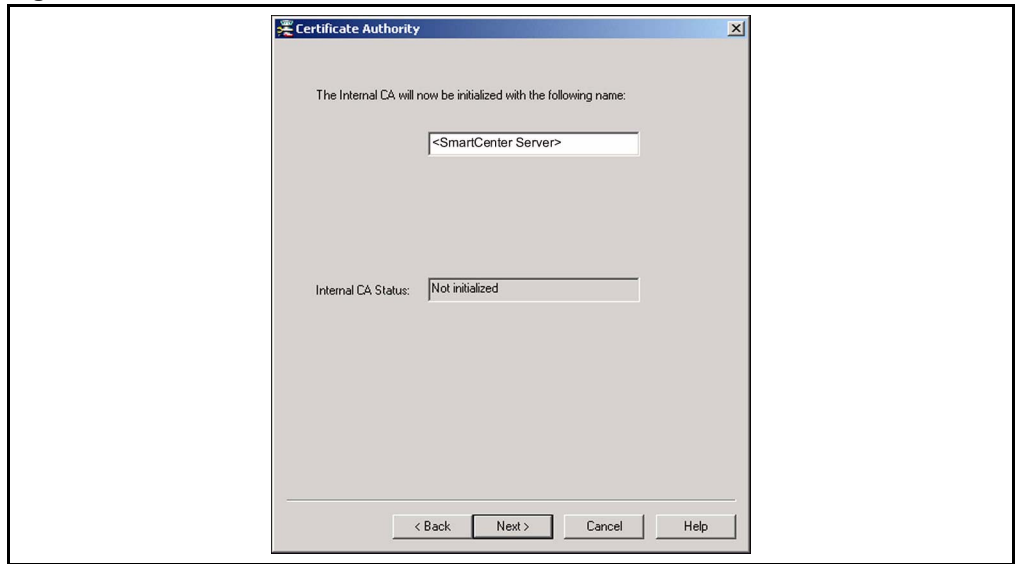


NOTE – Do not type the characters quickly. When overfilled, the input buffer may take a few moments to process.

When the cryptographic seed is generated, click Next to continue.

14. Initialize the Certificate Authority. If the FQDN is correct, click the Send to CA button. See Figure 2-20.

Figure 2-20



15. Record the SmartCenter Server fingerprint by clicking Export to file.... See Figure 2-21.

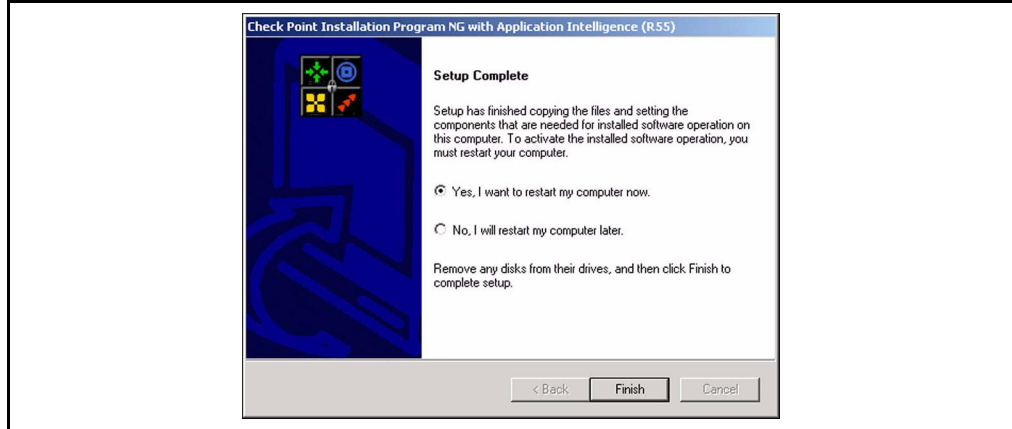
Figure 2-21



As a security measure, this fingerprint is required in a later step to ensure that no one has impersonated the administrator. Press Finish to continue.

16. When prompted, reboot the management station. See [Figure 2-22](#).

Figure 2-22



Once the station is rebooted, installation of the SmartCenter Server and SmartConsole are complete. The next task is [“Defining a firewall object in the SmartDashboard”](#) on page 76.

Defining a firewall object in the SmartDashboard

1. Launch the SmartDashboard software by clicking Start ▶ Programs ▶ Check Point SmartConsole R55 ▶ SmartDashboard.
2. Log in using an administrator account. See [Figure 2-23](#).

Figure 2-23



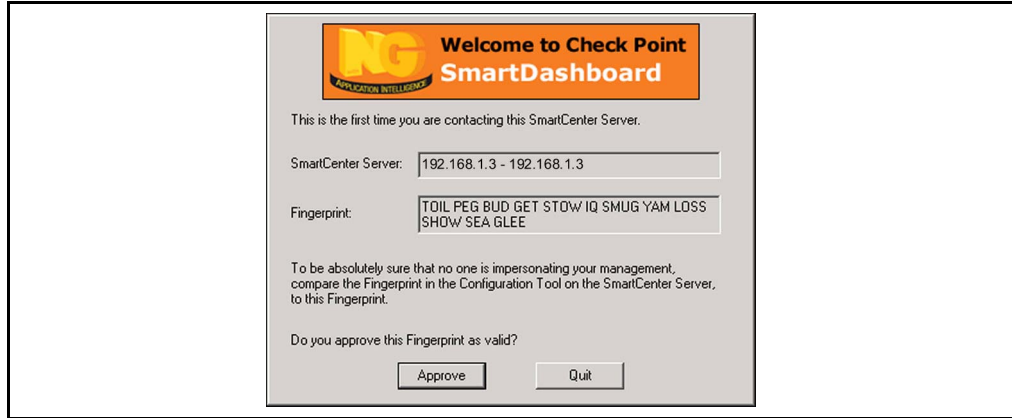
Enter one of the user name/password combinations configured during the installation of the Management Server tools in [Step 11](#) on [page 71](#). Also specify the IP address of the SmartCenter Server and click OK.

NOTE – Be sure you have added this IP address in the client access list to allow SMART Client access to the firewall iSD (see [Step 1](#) on [page 62](#)).

3. **Verify the Check Point fingerprint.**

At this point, the SmartDashboard contacts the Management Server. Since this is the first contact, you are prompted to verify the current fingerprint. See [Figure 2-24](#) on [page 77](#).

Figure 2-24

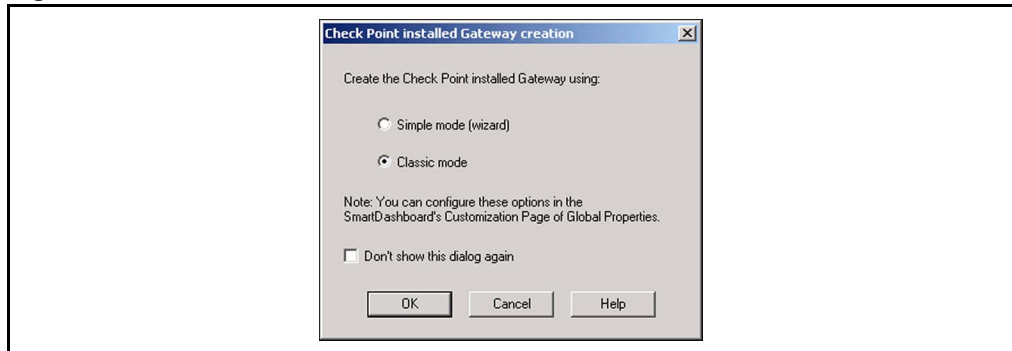


Click **Approve** to verify that the fingerprint is the same as the one obtained during installation of the Management Server tools during [Step 15](#) on [page 74](#).

4. Create a new Gateway object to represent the newly installed firewall iSD.

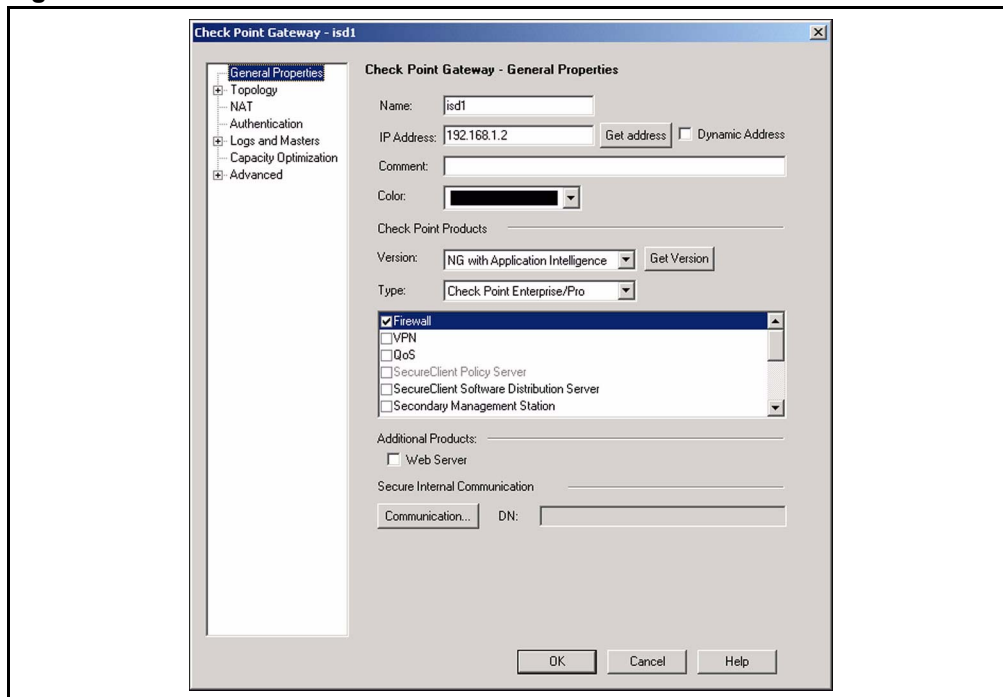
From the SmartDashboard Network Objects pane, right-click on the Check Point object, then click **New Check Point > Gateway...** When the **Check Point installed Gateway creation** window appears, select **Classic mode**. See [Figure 2-25](#).

Figure 2-25



5. Define the firewall iSD object parameters. See [Figure 2-26](#).

Figure 2-26



Enter the following information:

- Name: If this is a Windows NT machine, use the name you specified in [“Editing the Windows NT hosts file”](#) on page 63. Otherwise just type in a name (isd1 in the example).
- IP Address: The address of the newly installed firewall iSD. In our example, the address is 192.168.1.2.
- Check Point products:
 - Version: Select NG with Application Intelligence.
 - List Window: Select **Firewall**

Leave the General Properties window open for use in [Step 2](#) in [“Establishing Secure Internal Communication”](#) on page 79.

Establishing Secure Internal Communication

Check Point FireWall-1 NG with Application Intelligence uses a one-time password to initiate Secure Internal Communications (SIC) between configured objects and the management station.

NOTE – This procedure assumes your SmartCenter Server is installed on a separate workstation. If you enabled SmartCenter Server on the firewall iSD in [Step 11](#) on [page 48](#), you do not need to establish SIC.

1. Reset SIC at the firewall iSD by entering these commands:

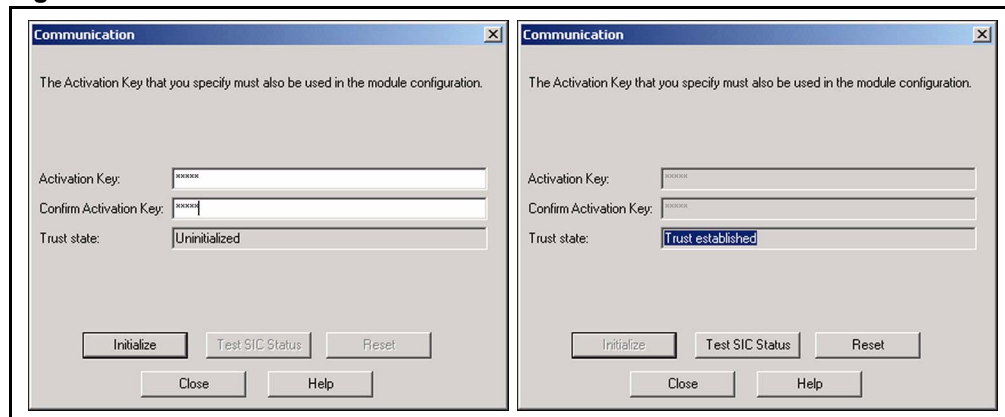
```
>> Main # /cfg/fw/sic
Enter the Host IP Address :192.168.1.2           Example host IP
Enter new Check Point SIC Password :
Confirm password:
This operation may take a while to complete
and traffic can be interrupted for 5 minutes. Do you want to continue
(y/[n])? y
SIC Reset Succeeded...
```

NOTE – If SIC is already established, you need to reset SIC to establish SIC again. If policies are already installed, issue the shell command, “fw unloadlocal”.

NOTE – What is referred to as *password* on the firewall iSD is referred to as *Activation Key* at the SmartDashboard.

- At the SmartDashboard, click on the **Communication** button in the **General Properties** window (see [Step 5](#) on [page 76](#)). The **Communications** window appears (see [Figure 2-27](#), left).

Figure 2-27

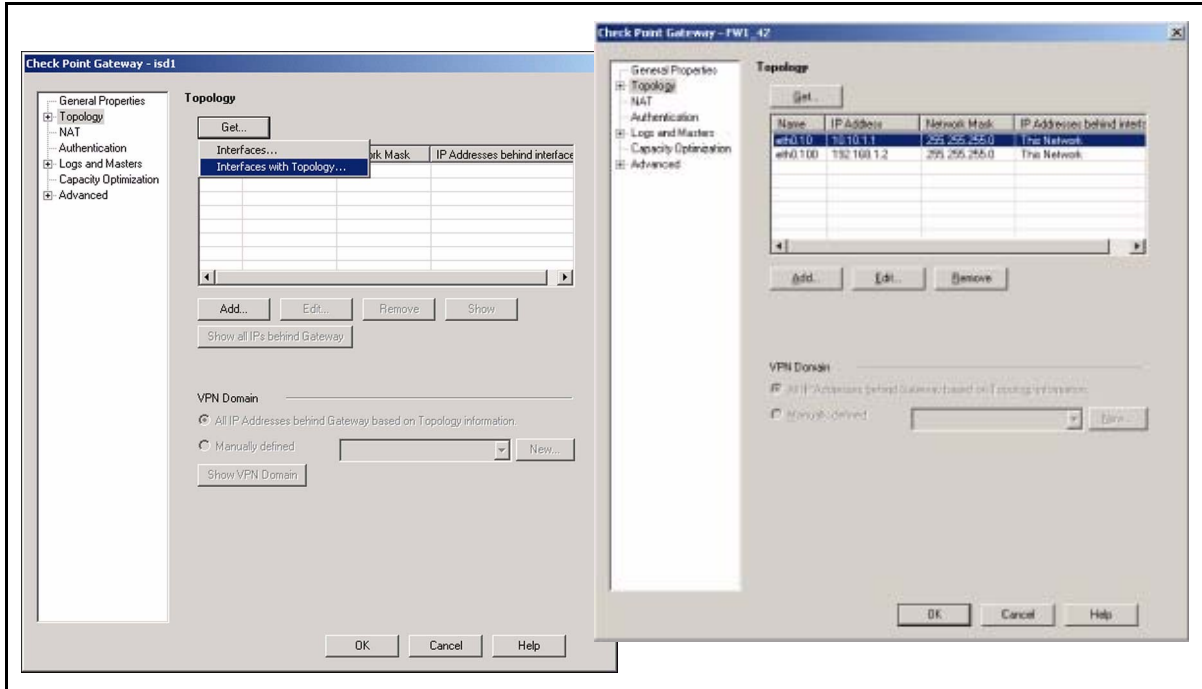


Enter the Activation Key (the SIC password) and click **Initialize**. The SmartCenter Server contacts the firewall iSD and exchanges security information. When successful, the window indicates “Trust established” ([Figure 2-27](#), right). Click **Close**.

- Get the interfaces for the firewall iSD object.

NOTE – Select the Topology section of the Check Point Gateway window and click Get..., then select Interfaces with Topology... This retrieves the interfaces you configured on the firewall iSD and topology information (under the *IP Addresses behind interfaces* header). The topology information is needed to implement anti-spoofing. See [Figure 2-28](#) on [page 81](#).

Figure 2-28



The interface `eth0_10` refers to the VLAN for cluster management, and `eth1_100` refers to the VLAN for Check Point management.

NOTE – The cited interfaces are examples only. Your configuration information and VLAN IDs will display in the **Topology** window.

4. Click **OK** to close the Check Point Gateway window.
5. From the SmartDashboard menu bar, select **File > Save**.

Managing all clusters from one Check Point management station

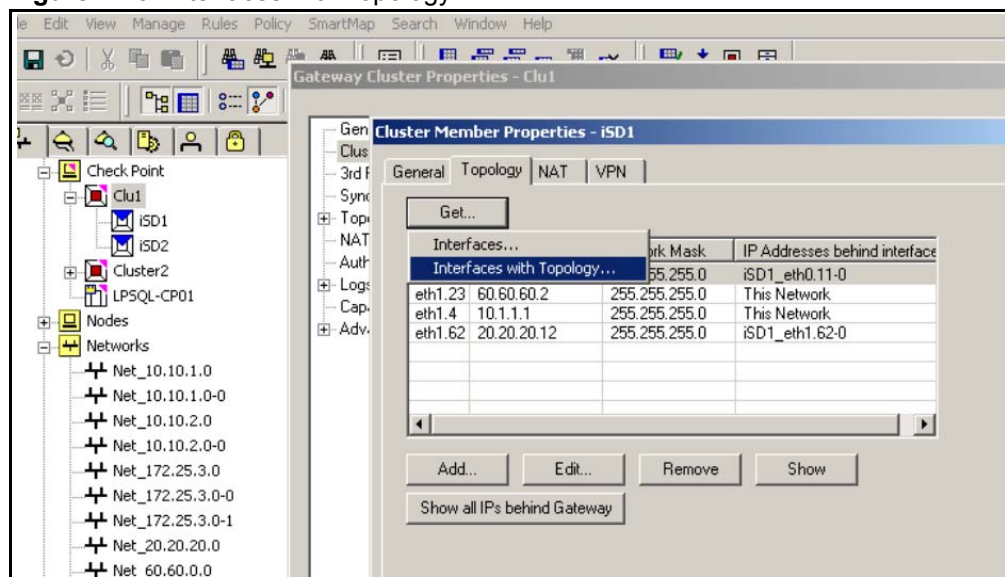
In this example, assume the following:

- IP address is 172.25.3.38/24
- Default gateway IP is 172.25.3.100

From the Check Point management station:

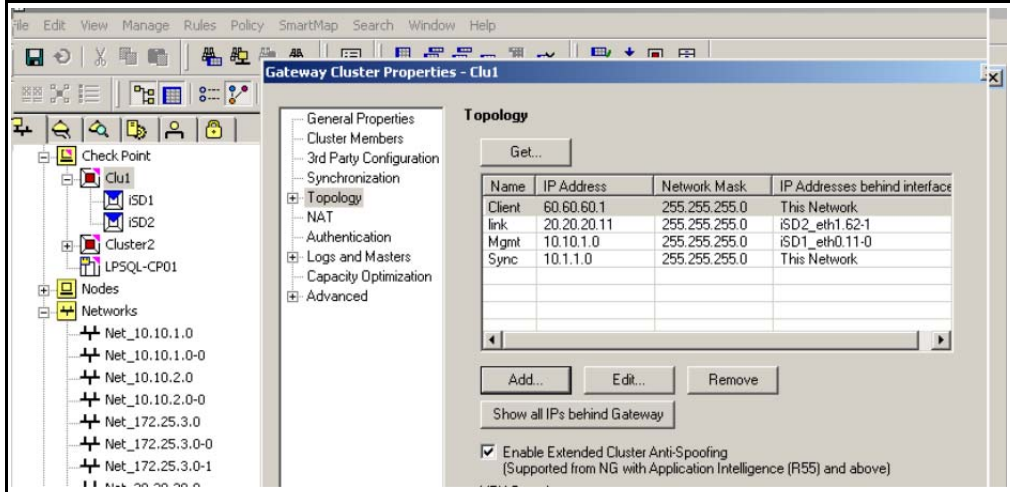
1. Go to each firewall iSD and get “Interfaces with Topology” (cluster member topology). See [Figure 2-29](#).

Figure 2-29 Interfaces with Topology



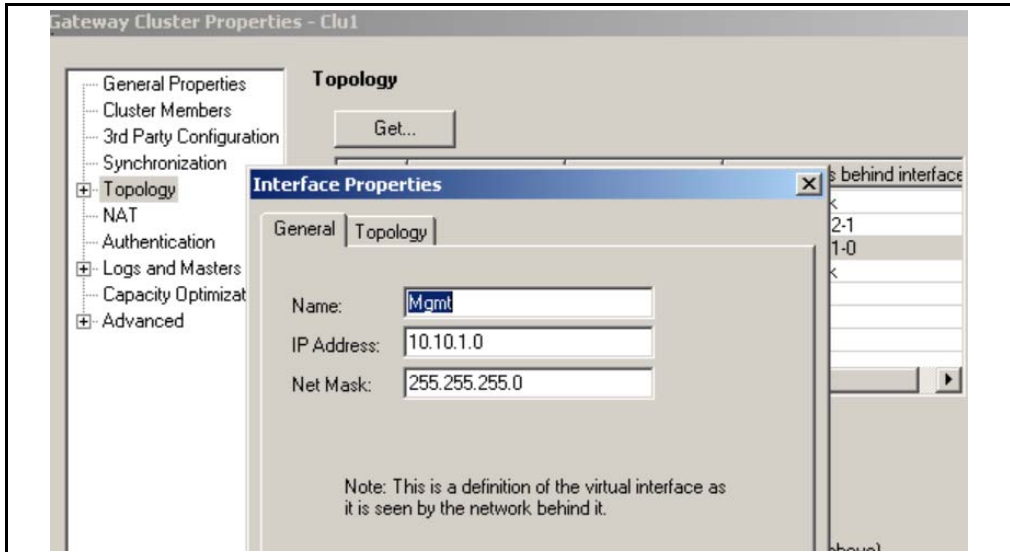
2. Go to cluster topology. See [Figure 2-30](#).

Figure 2-30 Gateway Cluster Properties window



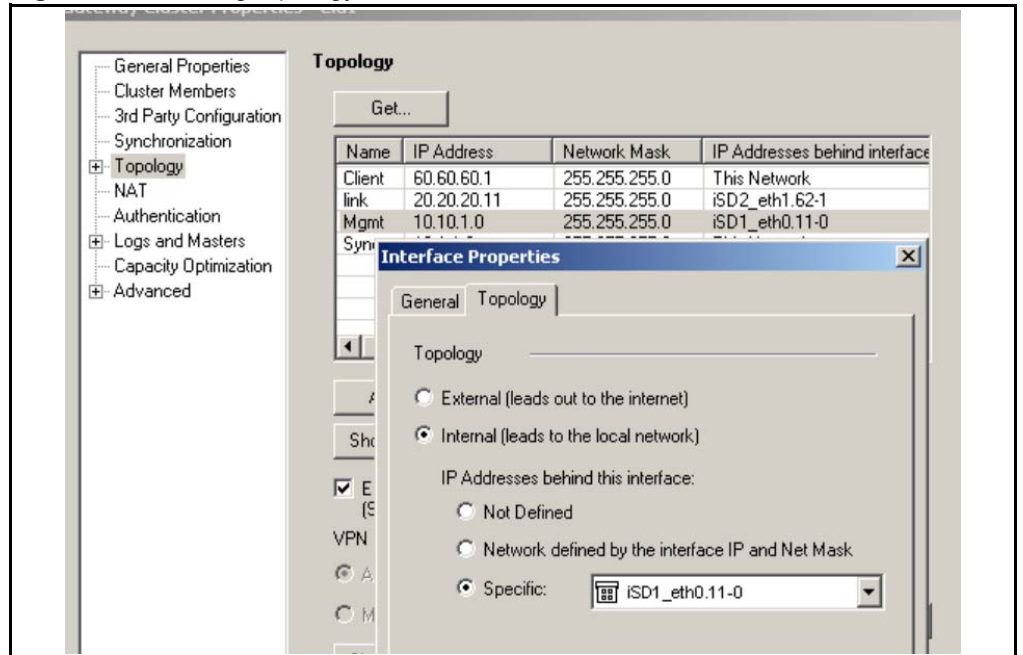
3. Add the interface or interfaces manually. See [Figure 2-31](#).

Figure 2-31 Adding interfaces



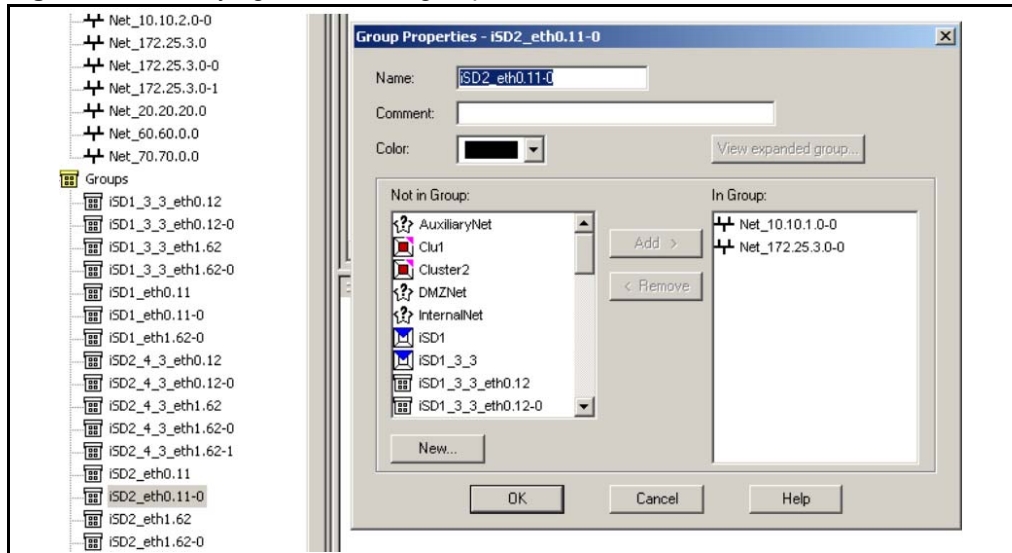
4. Set the interface cluster topology to the appropriate group (select Specific and choose the appropriate network group). See [Figure 2-32](#).

Figure 2-32 Setting topology



5. Double-click the network group in the Groups drop-down list to verify it. See [Figure 2-33](#).

Figure 2-33 Verifying the network group



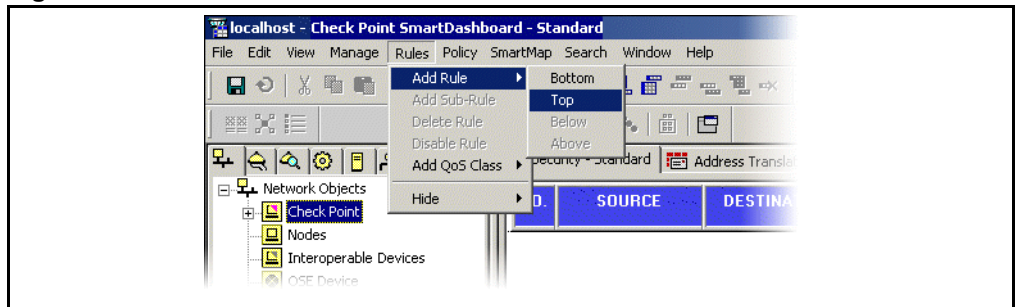
6. Repeat Steps 1–5 for each cluster.

Creating a firewall policy test rule

At this point in the initial setup, Nortel Networks recommends a test to ensure that the system components are properly configured. For this test, create a policy rule that allows any and all traffic to pass through the firewall iSD. Later, once the firewall operation is confirmed, you can remove this test policy and create firewall security rules that restrict undesirable traffic.

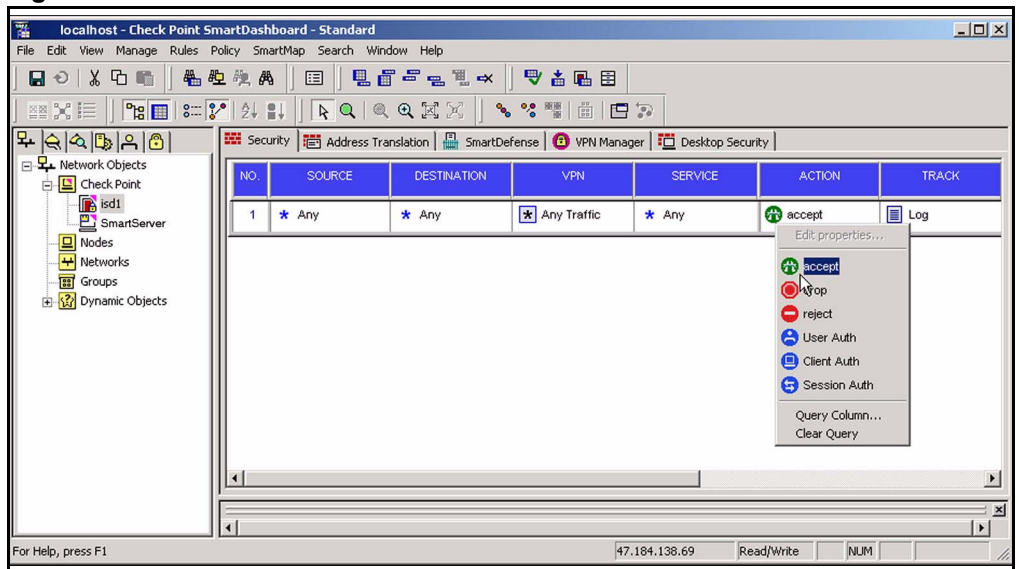
From the SmartDashboard menu bar, select **Rules > Add Rule > Top**. A new rule is added to the rulebase. The default action of the new rule is “drop,” indicating that all traffic from any source to any destination does not pass through the firewall iSD. See [Figure 2-34](#).

Figure 2-34



Change the action of the new rule to **accept** by right-clicking on the “drop” action icon and selecting “accept” as the new action from the pop-up list. See [Figure 2-35](#).

Figure 2-35

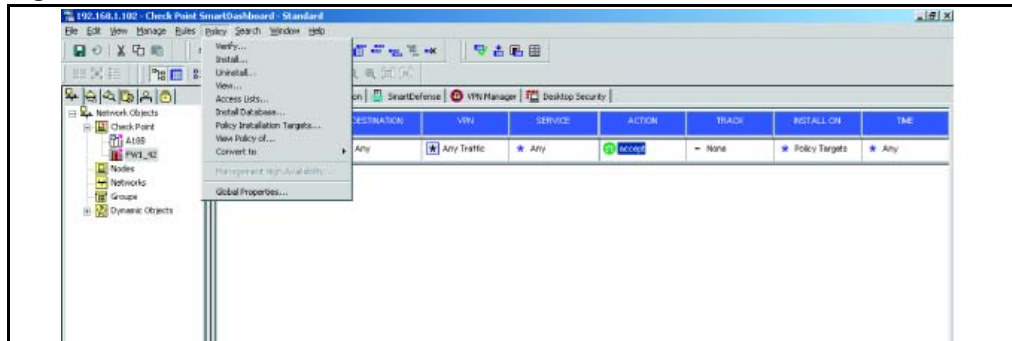


Also change the Track setting to **log** by right-clicking on the **none** setting and selecting **log** as the new track setting from the pop-up list.

7. Push the policies to the firewall iSD.

From the menu bar, select **Policy > Install**. When the Install Policy window appears, select the firewall iSD object and click on OK. See [Figure 2-36](#).

Figure 2-36

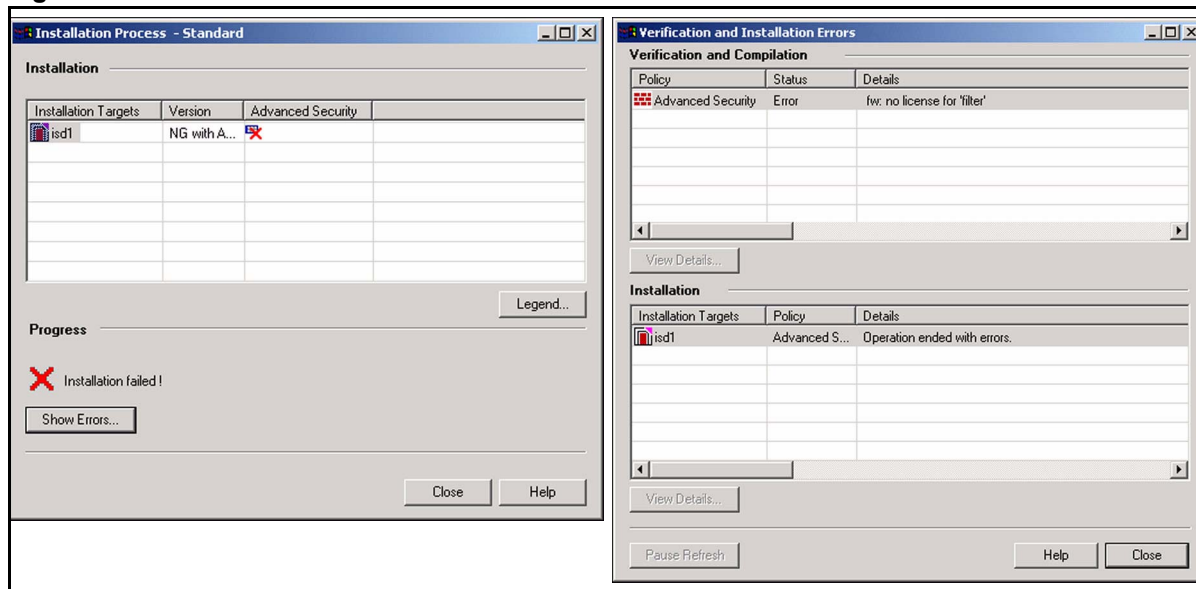


NOTE – If your system has an HA configuration, go to **Policy > Global Properties > NAT - Network Address Translation** and deselect **Automatic ARP configuration** before you push policies for the first time. Otherwise the Proxy ARP module will not work properly.

If the Check Point anti-spoofing feature is not enabled, a warning message appears. See your Check Point documentation to determine whether anti-spoofing is necessary for your firewall.

8. If the effort to push policies fails, click Show Errors... (see [Figure 2-37](#), left).

Figure 2-37



A common cause of errors is an expired license ([Figure 2-37](#) right). If this is the case, update the license on the SmartCenter Server using SmartUpdate and push policies again.

9. Use the SmartView Tracker program to confirm proper operation of the firewall iSD.

The SmartView Tracker lists all traffic being processed, accepted, dropped, and so on. To confirm that the firewall iSD is properly configured, select the SmartView Tracker Active Mode. Use a client station to ping the iSD. If the SmartView Tracker displays an entry for the ping traffic, the configuration is good.

NOTE – The SmartView Tracker is an excellent tool for debugging and enhancing your security rules. See your Check Point documentation for complete details.

10. Use the SmartDashboard to remove the test rule generated in “[Creating a firewall policy test rule](#)” on page 86.

Creating and installing firewall iSD security rules

The rules you apply to your security policy will depend on the security needs of your network. In general, you should drop all traffic that is not specifically required. See the Check Point documentation for more information about creating and maintaining effective security policies.

Managing Check Point licenses

Installing central licenses with SmartUpdate

Installing Check Point central licenses is best done using the Check Point tools on your management client. The license will be automatically sent to the Check Point Management Console license repository and then installed to the Firewall Director. For detailed information on Check Point licenses or the tools such as the Smart Dashboard and SmartUpdate, see your complete Check Point documentation at

<http://www.checkpoint.com/support/technical/documents/index.html> (ID and password required).

Use the following procedure to install a central license onto the firewall iSD. Steps 1-5 is used to create a new Gateway object. If you have already created a Gateway object, then go to Step 5 to install a central license:

- 1. Launch the SmartDashboard management tool on the management client Start menu.**
- 2. Create a new gateway object for the firewall iSD.**
Select **Network Objects > New > Gateway** and assign its IP address.
- 3. Establish trusted communication.**
Click the **Communication** button and type the Check Point SIC one-time password.
- 4. Click OK to save the object.**
- 5. Launch the SmartUpdate program from the Start menu.**
- 6. Select the object, from the Managed Modules window, that represents the target firewall iSD.**
- 7. Import the license file.**
From the menu bar, select **Licenses > New License > Import File** and then choose the license file (for example, 172.21.9.200_module.lic).
- 8. Follow onscreen prompts until the installation is complete.**

NOTE – If the license does not attach to the firewall iSD, then select **Licenses > View repository**. The **View repository** dialog box opens. Check for licenses for which the attached to column entry is empty. Double-click on each entry to find the matching IP address. To attach to the corresponding iSD, select **attach to**.

9. When the license is installed, load the firewall policy to the firewall iSD.

Re-installing an existing license

If the firewall iSD crashed and was re-imaged before the license was deleted from the firewall iSD, the management server will not allow you to install the same license remotely into the iSD. To work around the problem, have the original license file stored on a floppy disk (drive 'a'), and perform the following steps.

1. At the Check Point management station, enter the following command:

```
Rename c:\winnt\fw1\5.0\conf\licenses.c to licenses.old.
```

2. At the local terminal, enter the following commands:

```
>> Main# /cfg/fw/dis
>> Firewall Configuration# apply
>> Firewall Configuration# /cfg/fw/ena
>> Firewall Configuration# apply
```

Allow several minutes for FireWall-1 services to stop before entering `/cfg/fw/ena`.

NOTE – The 8660 SDM will automatically restart FireWall-1 services unless you use the `/cfg/fw/dis` command to disable the unit. For that reason, it is recommended that you do not use the `cpstop/cpstart` commands at the management station to disable/enable the firewall iSD.

3. At the Check Point management station enter the following command (make sure you have the license file on the floppy disk in drive 'a'):

```
cplic put <firewall name> -l a:ip_address_module.lic
```

Where `ip_address` is the IP address of the license; for example, `172.21.9.200_module.lic`.

Installing a license on an NT Workstation

Typically, you use SmartUpdate to maintain licensing on the SmartCenter Server. However, this procedure may be necessary if you are running the SmartCenter Server and SMART Client on an NT workstation.

NOTE – This procedure should not be needed if you are managing licenses from the SmartCenter server using SmartUpdate.

- 1. Click on your desktop Start button and select Run. When the Run window appears, specify `cmd` as the program to open and click on the OK button. In the command window, enter the license installation command in the following format:**

```
cplic put <firewall name> <Management Server IP address or name> <license expiration date> <license signature> <license string>
```

Use the firewall iSD name as entered in the `hosts` file (page 63). Be sure to enter the information exactly as shown on your specific Check Point license.

- 2. To verify that the local license is installed properly, login as `root` on the firewall iSD and enter the following command:**

```
cplic print -x -type
```

The output of this command should display the installed license information.



CHAPTER 3

Using JDM to configure firewall iSDs

This chapter describes how to configure the 8660 SDM firewall iSDs using JDM.

Overview of JDM tasks

To enable NAAP and configure SDM firewall iSDs using JDM, refer to the following sections:

- [“Configuring firewall iSD clusters” on page 93](#)
- [“Creating firewall VLANs” on page 97](#)
- [“Enabling and disabling NAAP” on page 104](#)
- [“Enabling and disabling a firewall iSD” on page 105](#)

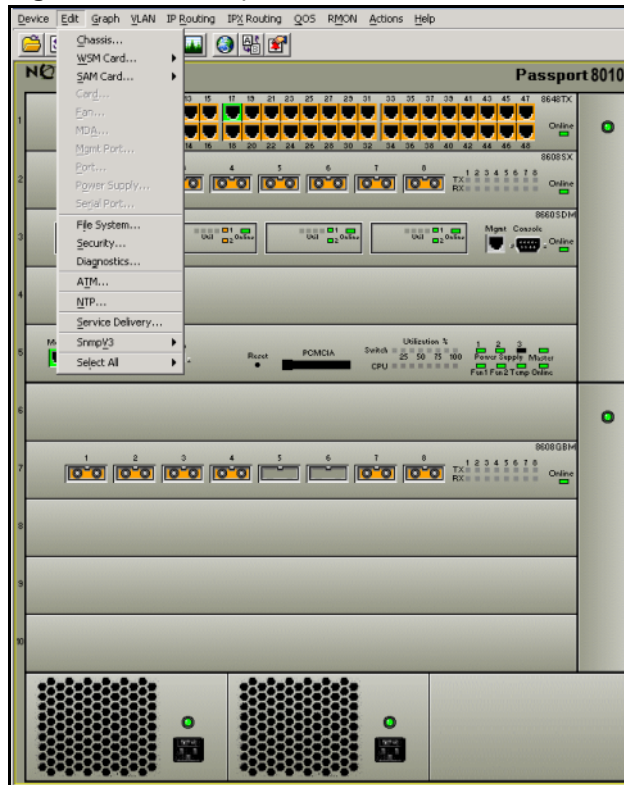
Configuring firewall iSD clusters

To increase the redundancy of firewall iSDs, two firewall iSDs can be aggregated together into one service delivery cluster. If an iSD is not aggregated with another iSD in a cluster, it must still be associated with a cluster ID to be enabled.

To configure a firewall iSD cluster:

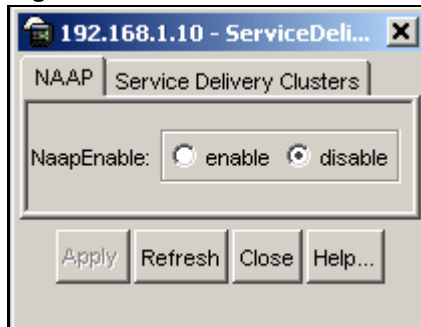
1. From the Device Manager menu bar, select **Edit > Service Delivery**. See [Figure 3-1](#).

Figure 3-1 Edit drop-down menu



The **ServiceDelivery** dialog box opens with the **NAAP** tab displayed. See [Figure 3-2](#).

Figure 3-2 NAAP tab



2. Click the **Service Delivery Clusters** tab.

The **Service Delivery Clusters** tab opens. See [Figure 3-3](#).

Figure 3-3 Service Delivery Clusters tab



[Table 3-1](#) describes the **Service Delivery Clusters** tab fields.

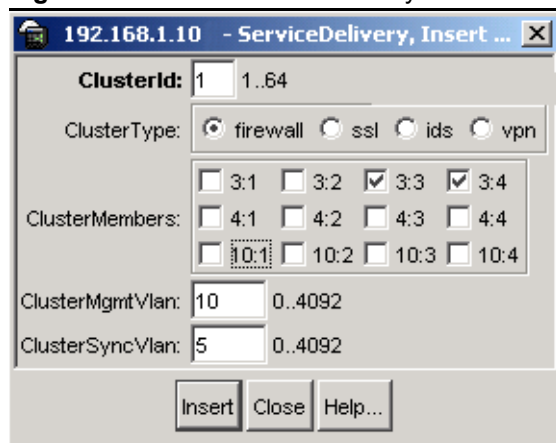
Table 3-1 Service Delivery Clusters tab fields

Field	Description
ClusterId	A unique ID assigned to a firewall iSD or an aggregation of firewall iSDs in a firewall configuration.
ClusterType	A specific cluster application selected when creating a cluster. The valid type is firewall. SSL, IDS, and VPN are not supported in the current software release.
ClusterSize	The number of iSDs in a cluster (maximum is 2).
ClusterMembers	The firewall iSDs that belong to a cluster, listed by 8600 Series Switch chassis slot and 8660 mini-slot.
ClusterMgmtVlan	This VLAN is created for the purpose of managing the cluster. Port 1 of each firewall iSD is used for the Management VLAN.
ClusterSyncVlan	This VLAN is created when you are configuring clusters to operate in High Availability (HA) mode. The sync VLAN is used for synchronization of clustered firewalls in a redundant configuration. This VLAN must have the lowest assigned VLAN ID number on the firewall iSD.

3. To add a cluster, click **Insert**.

The **Insert Service Delivery Cluster** dialog box opens. See [Figure 3-4](#).

Figure 3-4 Insert Service Delivery Cluster dialog box



[Table 3-1](#) on [page 95](#) describes the **Insert Service Delivery Cluster** dialog box fields.

4. Populate the **Insert Service Delivery Cluster** fields as follows:

- a. Enter the Cluster Id.
- b. Select the cluster type (firewall).
- c. Select the cluster members.
- d. Enter the cluster management VLAN ID.
- e. Enter the cluster sync VLAN ID. This must be the lowest assigned VLAN ID number on the firewall iSD.
(Defining a sync VLAN is only required when a cluster contains two members).

5. When all required fields are populated, click **Insert**.

JDM creates the firewall iSD cluster with the associated cluster management VLAN and cluster sync VLAN. [Figure 3-5](#) shows the Service Delivery Clusters tab with a sample two-member cluster configuration.

Figure 3-5 Service Delivery Clusters tab



Creating firewall VLANs

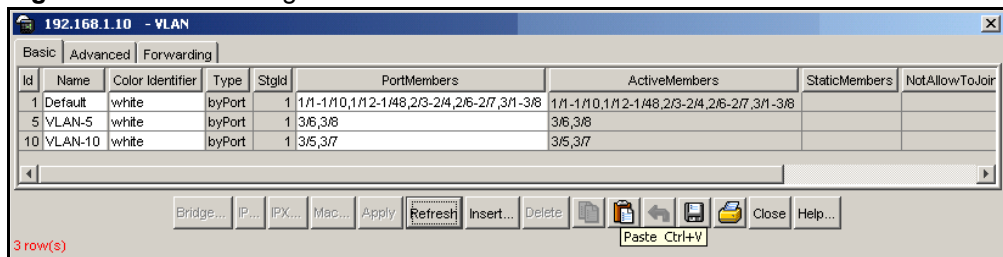
Once the firewall cluster(s) are defined, you must create VLANs for each interface to the firewalls and add them to the appropriate cluster. In addition, for each cluster, you can create a Peering VLAN to direct traffic in and out of the firewall iSD. It is also recommended to create a Check Point Management VLAN to provide access for Check Point Management. Finally, you must create a NAAP VLAN to provide system level management.

To create the VLANs:

1. From the Device Manager menu bar, select **VLAN > VLANs**.

The VLAN dialog box opens with the **Basic** tab displayed. See [Figure 3-6](#).

Figure 3-6 VLAN dialog box



2. Create the VLANs in the following order:

- a. Firewall VLANs (multiple can be created)
- b. Peering VLANs (maximum one per cluster)
- c. Check Point Management VLAN
- d. NAAP VLAN (one per 8600 switch)

[Table 3-2 on page 99](#) describes the required property values for the different VLAN types.

Table 3-2 Required property values for different VLAN types

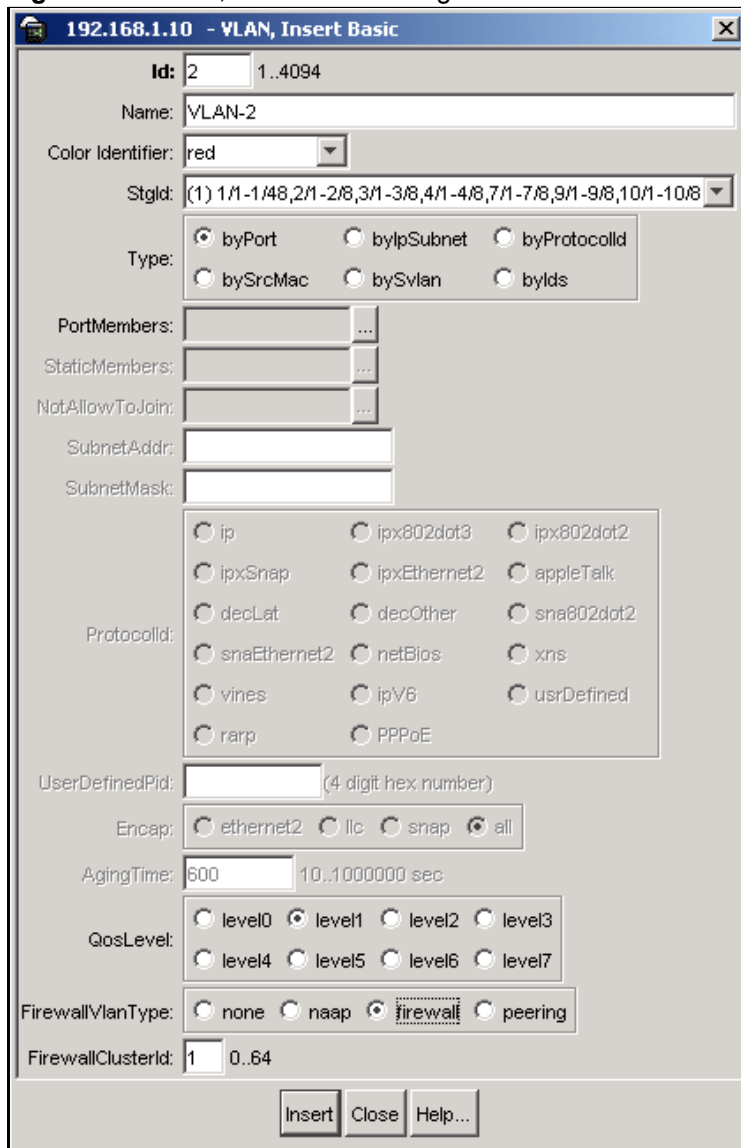
VLAN type/ Property	Firewall VLAN (Trusted network and Untrusted network)	Peering VLAN	Check Point VLAN	NAAP VLAN
ID	ID must be higher than sync VLAN ID	ID must be higher than sync VLAN ID	1-4092	must be 4094
Suggested Name (if default VLAN name is not desired)	Trusted VLANx or Untrusted VLANx	Peering VLAN	Check Point VLAN	NAAP VLAN
Type	byPort	byPort	byPort	byPort
PortMembers	Each Firewall VLAN must contain port 2* of each iSD in the cluster in addition to the desired 8600 ports.	The Peering VLAN contains only port 2* of each iSD in the cluster.	The Check Point VLAN must contain only the 8600 port connected to the Check Point SmartCenter Server.	The NAAP VLAN must contain port 1* of all iSDs in all clusters. When Interchassis Links (ICL) are required, (that is, when SDMs are in two different chassis) at least one 8600 port in each chassis must also be included in the NAAP VLAN to allow for inter-chassis communications.
FirewallVlanType	firewall	peering	none	NAAP
FirewallClusterID (see "Configuring firewall iSD clusters" on page 93)	appropriate cluster ID	appropriate cluster ID	Not applicable	Not applicable

*To add either iSD port 1 or port 2 to a VLAN membership, you must assign the matching logical ports on the 8600 switch.

3. To create each VLAN, perform the following steps:

- a. From the VLAN dialog box - **Basic** tab, click **Insert**.
The VLAN, **Insert Basic** dialog box opens. See [Figure 3-7](#).

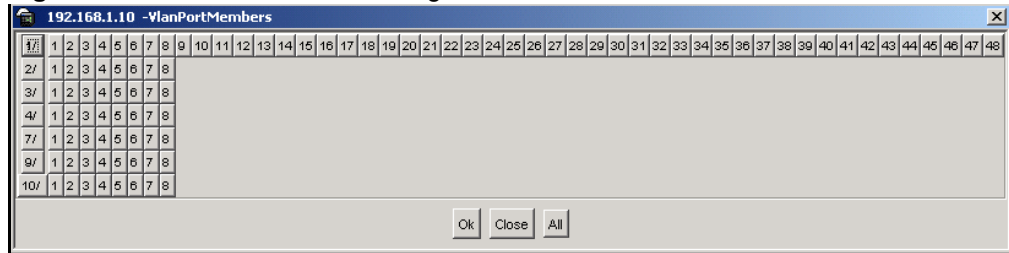
Figure 3-7 VLAN, Insert Basic dialog box



- b. In the **Id** field, enter the appropriate ID.
- c. In the **Type** field, select **byPort**.

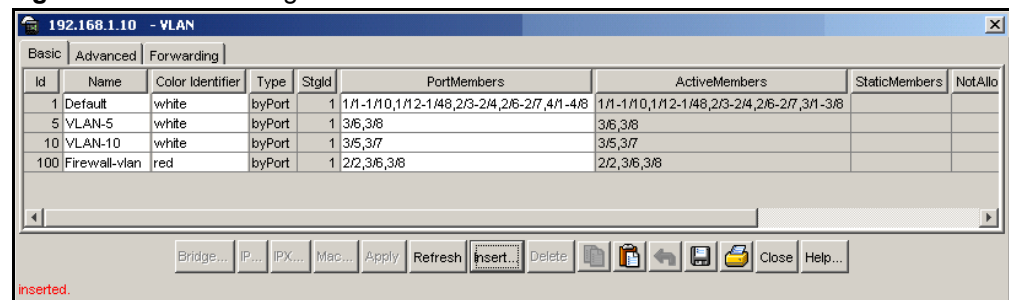
- d. In the **Name** field, if you wish to change the default VLAN name provided, enter a new VLAN name (for example, Firewall VLAN).
- e. (Optional) In the **Color Identifier** field, if you wish to change the default color provided, choose a color from the drop-down list.
- f. In the **Stgid** field, select the Spanning Tree Group ID of the VLAN from the drop-down list.
- g. In the **FirewallVlanType** field, select the appropriate VLAN-type radio button.
- h. In the **FirewallClusterID** field, enter the appropriate Cluster ID.
- i. In the **PortMembers** field, click the ellipsis (...).
The **VlanPortMembers** dialog box opens. (See [Figure 3-8](#).)

Figure 3-8 VlanPortMembers dialog box



- j. Select the port members as required and click **OK**.
- k. Click **Insert**.
The new VLAN appears in the Basic tab. [Figure 3-9](#) shows the VLAN-Basic tab with a sample firewall VLAN added.

Figure 3-9 VLAN dialog box



- l. Repeat Steps [a](#) to [k](#) for each of the required VLANs.
- 4. After you have added the VLANs, configure the IP addresses for the appropriate VLANs (see “[Configuring VLAN IP addresses](#)”).**

Configuring VLAN IP addresses

After you have created all VLANs, configure one IP address each for the cluster management VLAN, the Peering VLAN, and the Check Point VLAN.

To configure a VLAN IP address:

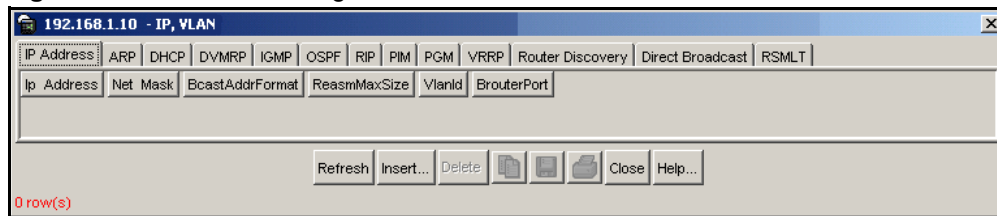
1. **From the Device Manager menu bar, select VLAN > VLANs.**

The VLAN dialog box opens with the **Basic** tab displayed. See [Figure 3-7 on page 100](#).

2. **Highlight the VLAN that requires an IP address.**
3. **Click IP.**

The IP, VLAN dialog box opens. (See [Figure 3-10](#).)

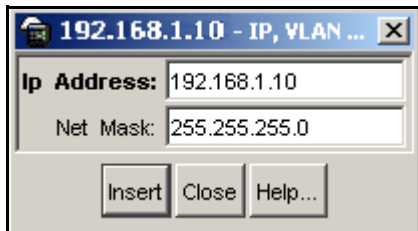
Figure 3-10 IP, VLAN dialog box



4. **Click Insert.**

The Insert IP Address dialog box opens. (See [Figure 3-11](#).)

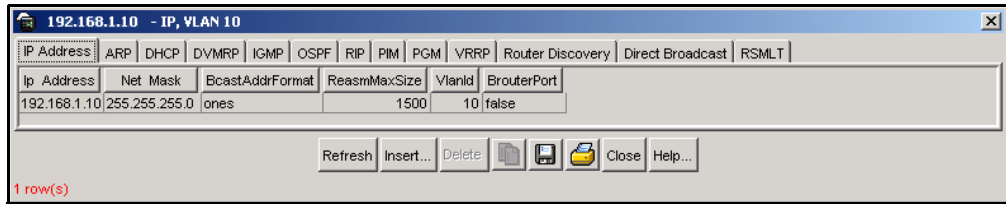
Figure 3-11 Insert IP Address dialog box



5. **Enter the IP address (in this example, 192.168.1.10).**
6. **Enter the Net mask (in this example, 255.255.255.0).**
7. **Click Insert.**

Figure 3-12 shows the IP Address tab with the sample IP configuration for the cluster management VLAN.

Figure 3-12 Management VLAN IP configuration



8. Click Close.
9. Repeat Steps 1 to 8 for each of the VLANs that require an IP address.
10. After you have configured the necessary IP addresses, enable the NAAP (see “[Enabling and disabling NAAP](#)”).

Enabling and disabling NAAP

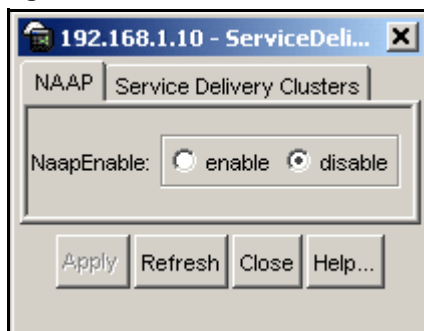
The Nortel Appliance Acceleration Protocol (NAAP) allows the firewall iSDs to communicate with the Passport 8600. As a result, enabling the NAAP enables the communication to the 8660 SDM module and disabling the NAAP disables the communication to the 8660 SDM module.

To enable NAAP:

1. From the Device Manager menu bar, select **Edit > Service Delivery**.

The **ServiceDelivery** dialog box opens, with the **NAAP** tab displayed. See [Figure 3-13](#).

Figure 3-13 NAAP tab



[Table 3-3](#) describes the NAAP tab field.

Table 3-3 NAAP tab field

Field	Description
NaapEnable	Select the enable option button to enable NAAP. Select the disable option button to disable NAAP.

2. After you enable the NAAP, if you have a new installation of the firewall iSD software image, you must connect to the firewall iSD console to initialize the unit. See [“Initializing the firewall iSD” on page 44](#).

Enabling and disabling a firewall iSD



CAUTION—Before disabling the firewall iSD, you must first halt it.

To halt the firewall iSD, perform the following:

- From the Passport console, use the following CLI command:
Set_console slot# mini slot#
(For example: `Set_console 3 1`).
- From the SDM console, enter the following:
/boot/halt.

To enable or disable a firewall iSD:

1. **Highlight a firewall iSD and right-click to open the shortcut menu.**
2. **From the shortcut menu, select Edit.**

The **Service Delivery** dialog box for the firewall iSD opens. See [Figure 3-14](#).

Figure 3-14 Firewall iSD Service Delivery dialog box

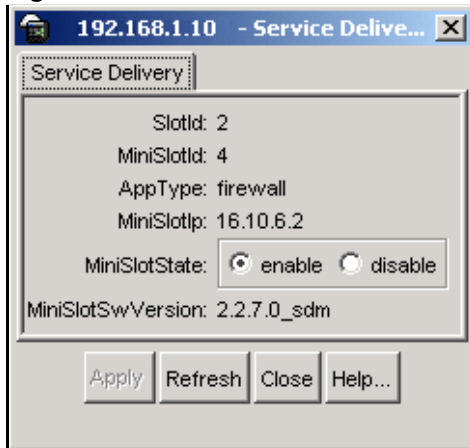


Table 3-4 describes the firewall iSD **Service Delivery** tab fields.

Table 3-4 Service Delivery fields

Field	Description
SlotId	The slot in which the 8660 SDM module resides within the 8600 Series Switch chassis.
MiniSlotId	The mini-slot position in which the firewall iSD resides within the 8660 SDM module.
AppType	The cluster application type. The valid type is firewall. SSL, IDS, and VPN are not supported in the current software release.
MiniSlotIp	The host IP address associated with the firewall iSD in that mini-slot.
MiniSlotState	<p>Select enable to power on the firewall iSD.</p> <p>NOTE – Before disabling the firewall iSD, you must halt it.</p> <p>To halt the firewall iSD, perform the following:</p> <ul style="list-style-type: none"> ■ From the Passport console, use the following CLI command: Set_console slot# mini slot# (For example: <code>Set_console 3 1</code>). ■ From the SDM console, enter the following: /boot/halt . <p>Select disable to shut down the firewall iSD.</p>
MiniSlotSwVersion	The software version of the firewall iSD running in the mini-slot.

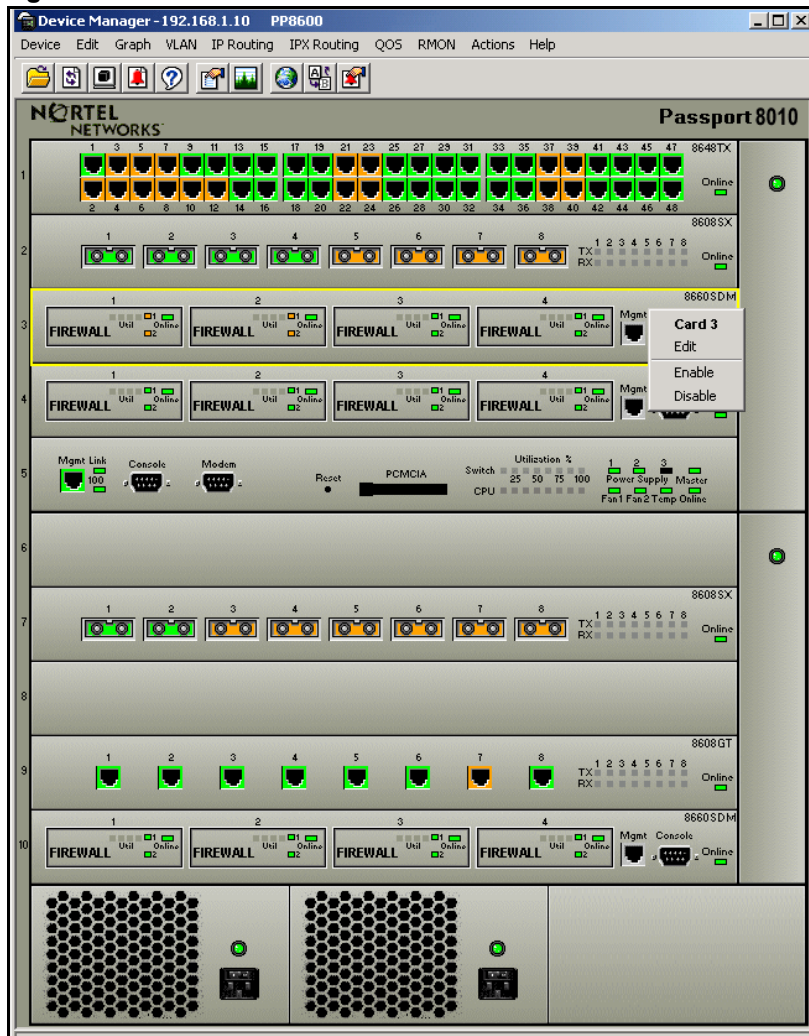
Viewing firewall iSD states

To view the state of all firewall iSDs on the SDM:

1. Perform one of the following:

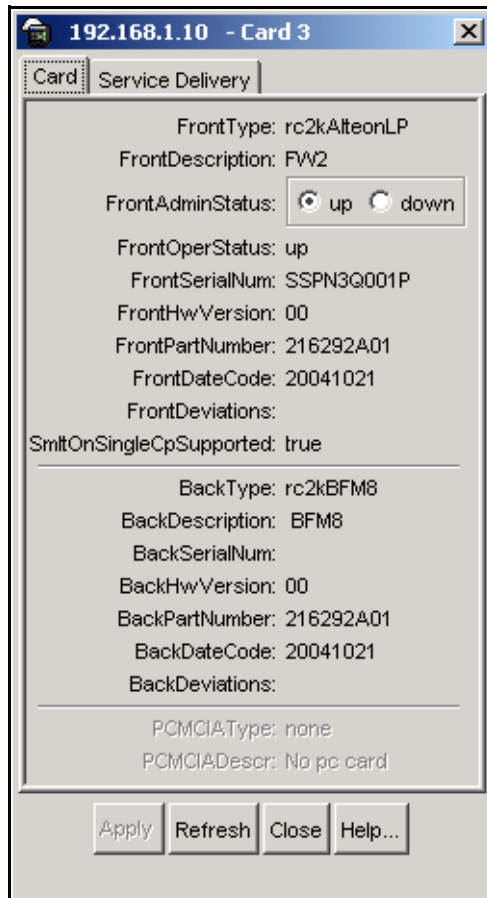
- Select the 8600 SDM, and from the Device Manager menu bar, select **Edit > Card**.
OR
- Select the 8660 SDM and right-click to open the shortcut menu.
From the shortcut menu, select **Edit**. See [Figure 3-15](#).

Figure 3-15 8660 SDM shortcut menu



The **Card** dialog box opens with the **Card** tab displayed. See [Figure 3-16](#).

Figure 3-16 Card tab



2. Click the **Service Delivery** tab.

The Service Delivery tab opens. See [Figure 3-17](#).

Figure 3-17 Service Delivery tab

SlotId	MiniSlotId	AppType	MiniSlotIp	MiniSlotState	MiniSlotSwVersion
3	1	firewall	16.10.5.1	enable	2.2.7.0_sdm
3	2	firewall	16.10.5.2	enable	2.2.7.0_sdm
3	3	firewall	16.10.5.3	enable	2.2.7.0_sdm
3	4	firewall	16.10.5.4	enable	2.2.7.0_sdm

For a description of the **Service Delivery** tab fields, see [Table 3-4](#) on page 106.

NOTE – To access the Browser-Based Interface (BBI) for a firewall iSD from the Service Delivery tab, highlight the firewall iSD and click **Open Service Home Page**. For more information on the BBI, see [Chapter 7, “Browser-Based Interface,”](#) on page 217 and [Chapter 8, “BBI forms reference,”](#) on page 233.

Accessing the Browser-Based Interface

Nortel Networks recommends that you create a secure port before using the Browser-Based Interface (BBI). To enable HTTPS access using SSL, see [“Enabling the Browser-Based Interface”](#) on page 218.

To access the Browser-Based Interface (BBI) for a firewall iSD using JDM:

1. **Highlight a firewall iSD and right-click to open the shortcut menu.**
2. **From the shortcut menu, select Open Service Home Page.**

If your firewall iSD host and browser are properly configured, the BBI login page appears.

For more information on the BBI, see [Chapter 7, “Browser-Based Interface,”](#) on page 217 and [Chapter 8, “BBI forms reference,”](#) on page 233.

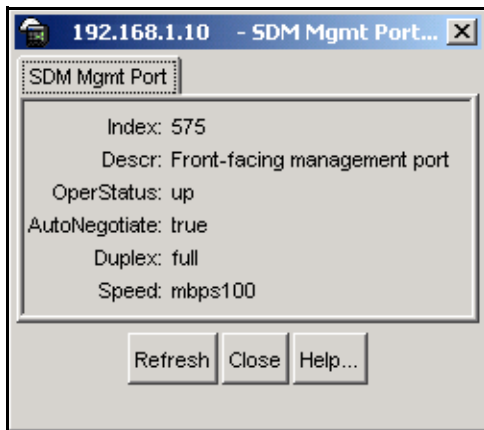
Viewing SDM Management Port properties

To view the SDM Management Port properties:

1. **Highlight the SDM Management Port.**
2. **From the Device Manager menu bar, select Edit > SDM Mgmt Port.**

The **SDM Mgmt Port** dialog box opens. (See [Figure 3-18](#).)

Figure 3-18 SDM Mgmt Port dialog box



For a description of the **SDM Mgmt Port** dialog box fields, see [Table 3-5](#).

Table 3-5 SDM Mgmt Port fields

Field	Description
Index	A unique value assigned to each interface.
Descr	The description of the SDM management port.
OperStatus	The operational status of the 8660 SDM device.
AutoNegotiate	The autonegotiate value for the SDM management port.
Duplex	The duplex setting for the SDM management port.
Speed	The speed setting for the SDM management port.

Example network configuration

The following procedure describes how to use JDM to create the required VLANs in the example network shown in [Figure 2-2 on page 34](#).

To create the VLANs:

1. **First, configure the firewall iSD cluster** (See [“Configuring firewall iSD clusters” on page 93](#) for details. [Figure 3-4 on page 96](#) shows the appropriate cluster configuration.)
2. **Once the firewall iSD cluster is created, create the necessary VLANs.** (For detailed instructions on creating VLANs, see [“Creating firewall VLANs” on page 97](#).)

[Table 3-6](#) describes the values for each of the VLANs required in this network example.

Table 3-6 VLAN properties for network example

VLAN/ Property	Untrusted Network VLAN	Trusted Network VLAN	Peering VLAN	Check Point VLAN	NAAP VLAN
ID	30	50	40	20	must be 4094
Name (optional)	Untrusted Network VLAN	Trusted Network VLAN	Peering VLAN	Check Point VLAN	NAAP VLAN
Type	byPort	byPort	byPort	byPort	byPort
PortMembers	1/4, 1/5 3/6, 3/8	1/7, 1/8 3/6, 3/8	3/6, 3/8	1/1	3/5, 3/7
FirewallVlanType	firewall	firewall	peering	none	NAAP
FirewallClusterID	1	1	1	Not applicable	Not applicable

Figures [3-19](#) through [3-23](#) starting on [page 112](#) show the required VLAN configurations, presented in the recommended order that they be created.

Figure 3-19 shows the Untrusted Network VLAN configuration.

Figure 3-19 Untrusted Network VLAN configuration

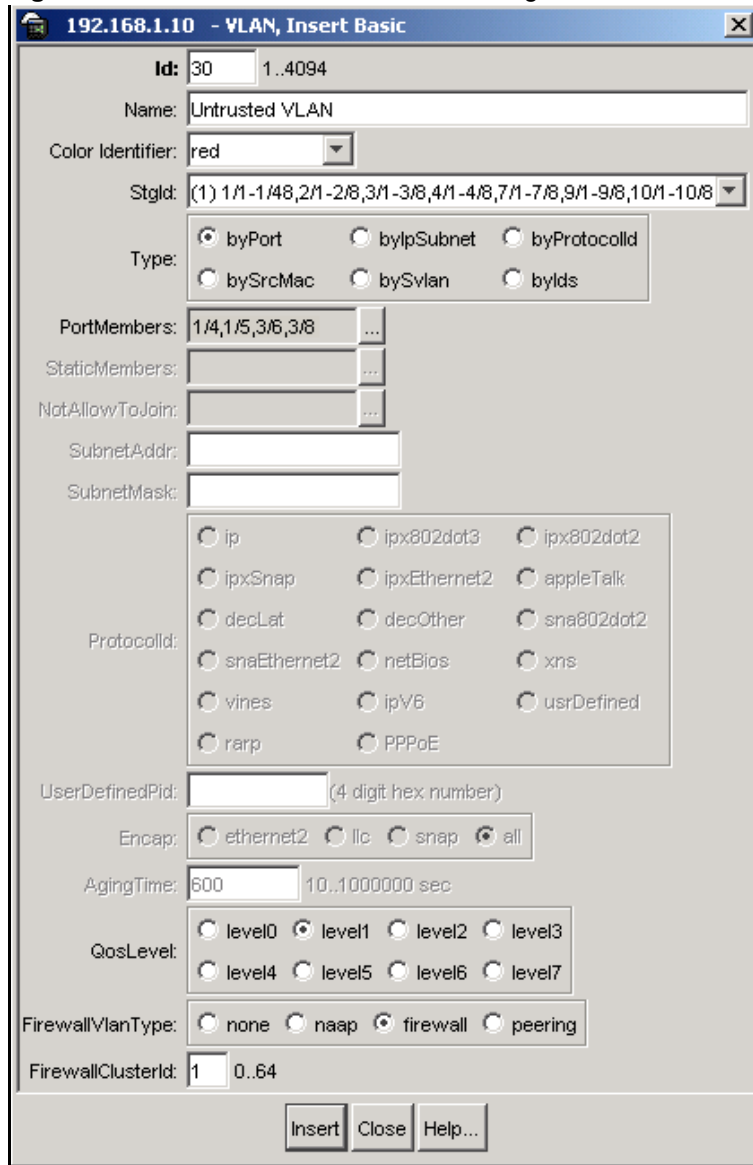


Figure 3-20 shows the Trusted Network VLAN configuration.

Figure 3-20 Trusted Network VLAN configuration

192.168.1.10 - VLAN, Insert Basic

Id: 50 1..4094

Name: Trusted VLAN

Color Identifier: red

StgId: (1) 1/1-1/48,2/1-2/8,3/1-3/8,4/1-4/8,7/1-7/8,9/1-9/8,10/1-10/8

Type: byPort byIpSubnet byProtocolId
 bySrcMac bySvlan byIids

PortMembers: 1/7,1/8,3/6,3/8 ...

StaticMembers: ...

NotAllowToJoin: ...

SubnetAddr: ...

SubnetMask: ...

ProtocolId: ip ipx802dot3 ipx802dot2
 ipxSnap ipxEthernet2 appleTalk
 decLat decOther sna802dot2
 snaEthernet2 netBios xns
 vines ipV6 usrDefined
 rarp PPPoE

UserDefinedPid: (4 digit hex number)

Encap: ethernet2 llc snap all

AgingTime: 600 10..1000000 sec

QosLevel: level0 level1 level2 level3
 level4 level5 level6 level7

FirewallVlanType: none naap firewall peering

FirewallClusterId: 1 0..64

Buttons: Insert Close Help...

Figure 3-21 shows the Peering VLAN configuration.

Figure 3-21 Peering VLAN configuration

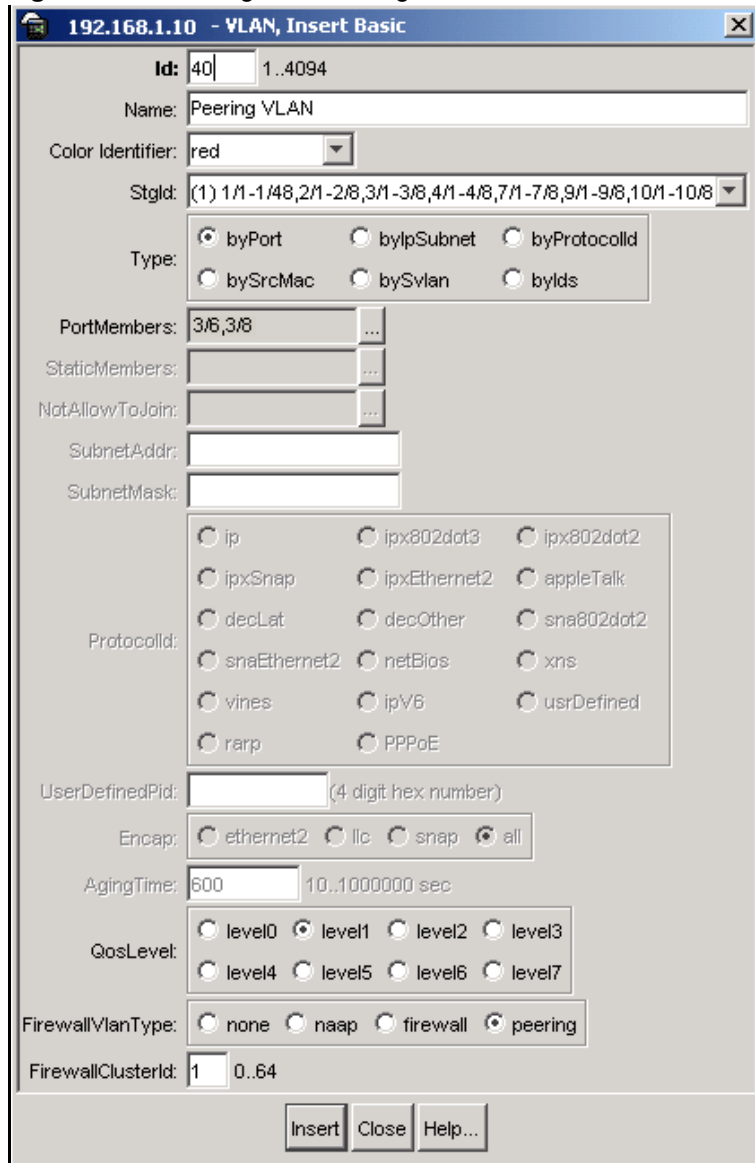


Figure 3-22 shows the Check Point VLAN configuration.

Figure 3-22 Check Point VLAN configuration

192.168.1.10 - VLAN, Insert Basic

Id: 20 1..4094

Name: Check Point VLAN

Color Identifier: red

StgId: (1) 1/1-1/48, 2/1-2/8, 3/1-3/8, 4/1-4/8, 7/1-7/8, 9/1-9/8, 10/1-10/8

Type: byPort byIpSubnet byProtocolId
 bySrcMac bySvlan byIids

PortMembers: 1/1

StaticMembers:

NotAllowToJoin:

SubnetAddr:

SubnetMask:

ProtocolId: ip ipx802dot3 ipx802dot2
 ipxSnap ipxEthernet2 appleTalk
 decLat decOther sna802dot2
 snaEthernet2 netBios xns
 vines ipv6 usrDefined
 rarp PPPoE

UserDefinedPid: (4 digit hex number)

Encap: ethernet2 llc snap all

AgingTime: 600 10..1000000 sec

QoSLevel: level0 level1 level2 level3
 level4 level5 level6 level7

FirewallVlanType: none naap firewall peering

FirewallClusterId: 1 0..64

Insert **Close** **Help...**

Figure 3-23 shows the NAAP VLAN.

Figure 3-23 NAAP VLAN configuration

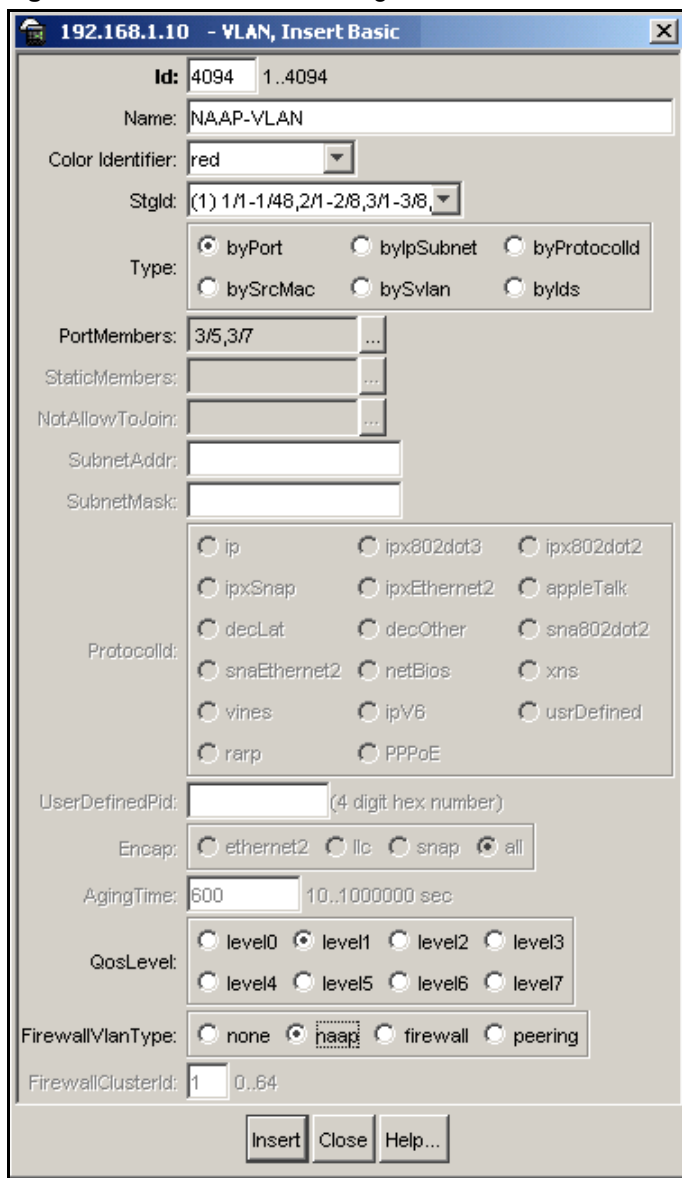


Figure 3-24 shows the VLAN - Basic tab with all required VLANs added.

Figure 3-24 Sample network VLAN configuration

Id	Name	Color Identifier	Type	StgId	PortMembers	ActiveMembers	StaticMembers	NotAllo
1	Default	red	byPort	1	1/1-1/10,1/12-1/48,2/3-2/4,2/6-2/7,3/1-3/8	1/1-1/10,1/12-1/48,2/3-2/4,2/6-2/7,3/1-3/8		
5	VLAN-5	red	byPort	1	3/6,3/8	3/6,3/8		
10	VLAN-10	red	byPort	1	3/5,3/7	3/5,3/7		
20	Check Point VLAN	red	byPort	1	1/1	1/1		
30	Untrusted VLAN	red	byPort	1	1/4,1/5,3/6,3/8	1/4,1/5,3/6,3/8		
40	Peering VLAN	red	byPort	1	3/6,3/8	3/6,3/8		
50	Trusted VLAN	red	byPort	1	1/7,1/8,3/6,3/8	1/7,1/8,3/6,3/8		
4094	NAAP-VLAN	red	byPort	1	3/5,3/7	3/5,3/7		

3. Configure the IP addresses for the Peering VLAN, the Check Point VLAN and the cluster management VLAN. (For detailed instructions on configuring IP addresses for VLANs, see “Configuring VLAN IP addresses” on page 102.)

Table 3-7 shows the required IP addresses for each VLAN.

Table 3-7 VLAN properties for network example

VLAN/ Property	Peering VLAN	Check Point VLAN	Cluster management VLAN
IP address	192.170.1.10	152.168.1.1	192.168.1.10
Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0

Figure 3-25 shows the VLAN dialog box - Basic tab after the required IP address configurations.

Figure 3-25 Sample Network IP configuration

Id	Name	Color Identifier	Type	StgId	PortMembers	ActiveMembers	StaticMembers	NotAllowToJoin	ProtocolId	SubnetAddr	SubnetMask
1	Default	red	byPort	1	1/1-1/10,1/12-1/48,2/3-2/4	1/1-1/10,1/12-1/48,2/3-2/4			none	N/A	N/A
5	VLAN-5	red	byPort	1	3/6,3/8	3/6,3/8			none	N/A	N/A
10	VLAN-10	red	byPort	1	3/5,3/7	3/5,3/7			none	192.168.1.10	255.255.255.0
20	Check Point VLAN	red	byPort	1	1/1	1/1			none	152.168.1.1	255.255.255.0
30	Untrusted VLAN	red	byPort	1	1/4,1/5,3/6,3/8	1/4,1/5,3/6,3/8			none	N/A	N/A
40	Peering VLAN	red	byPort	1	3/6,3/8	3/6,3/8			none	192.170.1.10	255.255.255.0
50	Trusted VLAN	red	byPort	1	1/7,1/8,3/6,3/8	1/7,1/8,3/6,3/8			none	N/A	N/A
4094	NAAP-VLAN	red	byPort	1	3/5,3/7	3/5,3/7			none	N/A	N/A

row(s)

4. Once all VLANs are created and the required IP addresses are configured, enable the NAAP (see [“Enabling and disabling NAAP” on page 104](#)).
5. Assuming this example is a new installation of the firewall iSD software image, after you enable the NAAP, you must connect to the firewall iSD console to initialize the unit. See [“Initializing the firewall iSD” on page 44](#).



CHAPTER 4

System management basics

This chapter explains how to access system management features on the firewall iSD. Management access is required for collecting system information, configuring system parameters beyond initial setup, establishing security policies, and monitoring policy effectiveness.

Management tools

The firewall iSD provides the following system management tools:

- The Command Line Interface (CLI)

The CLI offers a simple, text-based menu system for collecting system information and configuring system parameters. Use of the CLI is required for initial setup of the system. The CLI can be accessed locally at any 8660 SDM, or remotely using Telnet or Secure Shell (SSH) once access has been granted (see [“Defining the remote access list”](#) on page 124).

For additional details, see [“The Command Line Interface”](#) on page 123.

- The Browser-Based Interface (BBI)

The BBI allows management using your web browser. BBI access must be enabled through the CLI and Check Point SmartDashboard after initial setup is complete. Once enabled, the BBI provides a richly featured GUI that makes routine configuration and data collection easy.

For details, see [Chapter 7, “Browser-Based Interface,”](#) on page 217 and [Chapter 8, “BBI forms reference,”](#) on page 233.

- The Check Point FireWall-1 NG interface

The Check Point interface is used for managing firewall policies, and for viewing firewall logs and operational status. It is accessed through remote Check Point management stations or clients. A Check Point management station is required during initial system setup and for establishing firewall security policies, and monitoring policy effectiveness.

For details, see your Check Point documentation.

Users and passwords

Access to system functions is controlled through the use of unique usernames and passwords. Once you are connected to the system using local console, Telnet, SSH, or a web browser, you are prompted to enter a password. To enable better system management and user accountability, four levels of user access have been implemented on the firewall iSD. The default user names and password for each access level are listed in [Table 4-1](#). User names and passwords are case-sensitive.

NOTE – Nortel Networks recommends that you change all the default passwords after initial configuration and as regularly as required under your network security policies. For more information, see “[User Menu](#)” on [page 178](#) for CLI commands.

Table 4-1 User access levels (Part 1 of 2)

User Name	Password	Description and Tasks Performed
rwa	rwa	Default login for the Passport 8600 Series Switch.
oper	oper	The operator login is available through the CLI and BBI. The operator has no direct responsibility for system management. The operator can view all configuration information and operating statistics, but cannot make any configuration changes.
admin	admin	The administrator login is available through the CLI and BBI. The administrator has complete access to all menu, information, and configuration commands on the system, including the ability to add users and change passwords.
boot	ForgetMe	The boot login is available only through a local console terminal. The boot user can reinstall the firewall iSD software (see “ Reinstalling Software ” on page 345). To ensure that one avenue of access is always available in case all passwords are changed and lost, the boot user password cannot be changed.

Table 4-1 User access levels (Part 2 of 2)

User Name	Password	Description and Tasks Performed
root	ForgetMe	The root login is available only through a local console terminal. The root user has complete internal access to the operating system and software. Root user functions are outside the scope of this documentation.



CAUTION—The root login on this system is only intended for debugging and emergency repair, typically under the direction of support personnel. All modifications to the system, including configuration changes of any kind, must be made using the CLI available for the `admin` login. Modifications made through the root login can cause serious malfunction of the system, and can also be reversed by the system at any time.



CHAPTER 5

The Command Line Interface

The Command Line Interface (CLI) is the most direct method for viewing information about the firewall iSD. In addition, you can use the CLI for performing all levels of system configuration.

The CLI is text-based, and can be viewed using a basic terminal. The various commands are logically grouped into a series of menus and submenus. Each menu displays a list of commands and any submenus that are available, along with a summary of what each command does. Below each menu is a prompt where you can enter any command appropriate to the current menu.

This chapter describes how to access the CLI locally through any 8660 SDM serial port, or remotely using a Telnet or Secure Shell (SSH) client. It also provides a list of commands and shortcuts that are commonly available from all the menus within the CLI.

NOTE – Before the CLI can be used, a minimum configuration must be entered as discussed in Chapter 2, “Initial setup,” on page 31.

Accessing the CLI

Using the local serial port

The 8660 SDM has one front-facing serial port and one management port. These are shared among the iSDs on an SDM FW2, or SDM FW4. The serial port provides direct, local access for managing the firewall iSD.

Once the connection is initiated, you are prompted to log in and enter a valid password. For more information about different access levels and initial passwords, see [“Users and passwords” on page 120](#). When the login is validated, the Main Menu of the CLI displays (see [“The Main Menu” on page 130](#)).

Defining the remote access list

The firewall iSD can be managed remotely using Telnet, SSH, or the Browser-Based Interface (BBI). For security purposes, access to these features is restricted through the remote access list.

The remote access list allows the administrator to specify IP addresses or address ranges that are permitted remote access to the system. There is only one remote access list that is shared by all remote management features.

If a client whose IP address is not on the list requests remote management access, the request is dropped. By default, the access list is empty, meaning that all remote management access is initially disallowed.

When a client's IP address is added to the access list, that client is permitted to access all remote management features that have been enabled on the firewall iSD. For example, if only the Telnet feature is enabled, the client can use Telnet to reach the CLI. If the BBI is also enabled, the same client will be able to use the web browser to manage the system without any changes being made to the access list.

NOTE – When a remote management feature is enabled, access will not be allowed if the access list is left empty. It is important to add trusted management clients to the access list when initially enabling any remote management feature. It is also vital that you review the access list regularly and keep it up-to-date.

Displaying the access list

The following CLI command is used to view the access list:

```
>> # /cfg/sys/accesslist/list
```

Adding items to the access list

The following CLI commands are used to permit remote management access to a specific IP address or range of IP addresses.

1. Select the access list menu:

```
>> # /cfg/sys/accesslist
```

2. Add trusted remote IP addresses to the list:

```
>> Access List# add <base IP address to permit> <network mask for range>
```

The add command can be repeated for as many remote managers as required. For example, to allow IP addresses 201.10.14.7 and 214.139.0.0/24 to access remote management features, use the following commands:

```
>> # /cfg/sys/accesslist (Select access list menu)
>> Access List# add 201.10.14.7 255.255.255.255 (Add single address)
>> Access List# add 214.139.0.0 255.255.255.0 (Add range of addresses)
```

NOTE – Although each remote management feature (Telnet, SSH, and BBI) can be enabled or disabled independently, all share the same access list. All addresses on the access list are permitted to access any enabled management feature. You cannot enable SSH for some and Telnet for others.

3. Apply the changes:

```
>> Access List# apply
```

Using Telnet

A Telnet connection allows convenient management of the firewall iSD from any workstation connected to the network. Telnet access provides the same management options as those available through the local serial port.

NOTE – You cannot log in as `boot` or `root` using Telnet.

By default, Telnet access is disabled and all remote access is restricted. Depending on the severity of your security policy, you can enable Telnet and permit remote access to one or more trusted client stations (see [“Defining the remote access list” on page 124](#)).

NOTE – Telnet is not a secure protocol. All data (including the password) between a Telnet client and the firewall iSD is unencrypted and unauthenticated. If secure remote access is required, use SSH (see [“Using Secure Shell” on page 127](#)).

Enabling Telnet access

Before Telnet access is possible, you must perform the following configuration using the serial port:

1. **Log in as the administrator using the local serial port.**
2. **Ensure that the firewall iSD is configured with proper IP addresses.**

Each firewall iSD requires its own unique IP address, as well as one Management IP (MIP) address. These IP addresses are configured during the initial setup (see [Chapter 2, “Initial setup,”](#) on page 31).

3. **Enable Telnet.**

For security purposes, Telnet is initially disabled. To enable Telnet sessions on the firewall iSD, issue the following commands:

```
>> # /cfg/sys/adm/telnet/ena
>> Administration Applications# apply
```

4. **Use the access list to permit remote access to trusted clients.**

If you have already configured the access list for SSH or the BBI, there is no need to repeat the process for remote Telnet sessions. Otherwise, to permit remote access through Telnet, see [“Defining the remote access list”](#) on page 124.

5. **Use the Check Point SmartDashboard on your management client to add a security policy that allows Telnet traffic.**

The firewall policy should be constructed as follows:

- Source: The IP address of the Check Point SMART Client, or the IP address range of the management network
- Destination: The IP address of the firewall iSD (not the MIP address)
- Service: Telnet
- Action: Allow

Starting the Telnet session

Remote Telnet access requires a workstation with Telnet client software. To establish a Telnet session, run the Telnet client software and issue the Telnet command on your workstation:

```
telnet <host IP address>
```

Connect to the host IP address of the firewall iSD.

Once the Telnet session is initiated, you are prompted to log in and enter a valid password. For more information about access levels and initial passwords, see [“Users and passwords” on page 120](#).

When the login is validated, the Main Menu of the CLI will be displayed (see [“The Main Menu” on page 130](#)).

Using Secure Shell

An SSH connection allows convenient and secure management of the firewall iSD from any workstation connected to the network. SSH access provides the same management options as those available through the local serial port.

SSH access provides the following security benefits:

- server host authentication
- encryption of management messages
- encryption of passwords for user authentication

By default, SSH access is disabled and all remote access is restricted. Depending on the severity of your security policy, you can enable SSH and permit remote access to one or more trusted client stations (see [“Defining the remote access list” on page 124](#)).

Enabling SSH access on the firewall iSD

Before SSH access is possible, you must perform the following configuration using the serial port or enabled remote management feature:

- 1. Log in as the administrator.**
- 2. Check that the firewall iSDs are configured with proper IP addresses.**

Each firewall iSD requires its own unique IP address, as well as one MIP address. These IP addresses are configured during the initial setup (see [Chapter 2, “Initial setup,” on page 31](#)).

3. Enable SSH access.

For security purposes, SSH access is initially disabled. To explicitly enable SSH, issue the following commands:

```
>> # /cfg/sys/adm/ssh/ena  
>> SSH Administration# apply
```

4. Generate new SSH keys, where necessary.

During the initial setup of the firewall iSD, it was recommended that you select the option to generate new SSH host keys. This is required to maintain a high level of security when connecting to the firewall iSD using an SSH client.

If you think that your SSH host keys have been compromised, or if, at any time, your security policy dictates it, you can create new host keys using the following CLI command:

```
>> # /cfg/sys/adm/ssh/gensshkey  
>> SSH Administration# apply
```

When reconnecting to the firewall iSD after having generated new host keys, your SSH client will display a warning that the host identification (or host keys) has been changed.

5. Use the access list to permit remote access to trusted clients.

If you have already configured the access list for Telnet or the BBI, there is no need to repeat the process. Otherwise, to permit access to only trusted clients, see [“Defining the remote access list” on page 124](#).

6. Use the Check Point SmartDashboard on your management client to add a security policy that allows SSH traffic.

The firewall policy should be constructed as follows:

- Source: The IP address of the management client, or the IP address range of the management network
- Destination: The firewall iSD IP address
- Service: SSH
- Action: Allow

Starting the SSH session

Remote SSH access requires a workstation with SSH client software. To establish an SSH connection with the firewall iSD, run the SSH program on your workstation by issuing the following SSH command:

```
ssh -l <user name> <host IP address>
```

where the `-l` (lower case L) option is followed by the user name (`admin`, `oper`, and so on) being logged in, and the host IP address.

NOTE – You cannot log in as `boot` or `root` using SSH.

Once the SSH session is initiated, you will be prompted to log in and enter a valid password. For more information about different access levels and initial passwords, see [“Users and passwords” on page 120](#).

When the login is validated, the Main Menu of the CLI will be displayed (see [“The Main Menu” on page 130](#)).

Using the CLI

Basic operation

Using the CLI, firewall iSD administration is performed in the following manner:

- The administrator selects from a series of menu and submenu items, and modifies parameters to create the desired configuration.
- Most changes are considered pending and are not immediately put into effect or permanently saved. Only changes to users and passwords take effect when entered.
- To save changes, the administrator must use the global `apply` command. This allows the administrator to make a series of changes and put them into effect all at once.
- The global `diff` command can be used to view pending changes before they are applied.
- You can use the `“config naap connect 2”` command from the Passport 8600 CLI to access the firewall iSD CLI (similar to Telnet).

- To clear all pending changes, the administrator can use the global `revert` command, and then continue the configuration session, or the global `exit` command to log out of the system. Closing your remote session will also discard pending changes, though exiting manually is preferred.

NOTE – When multiple CLI or BBI administrator sessions are open at the same time, only pending changes made during your current session will be affected by the `diff`, `revert`, or `exit` commands. However, if multiple CLI or BBI administrators apply changes to the same set of parameters concurrently, the latest applied changes take precedence.

The Main Menu

After initial system setup is complete, and the user performs a successful connection and login, the Main Menu of the CLI is displayed. [Figure 5-1](#) shows the Main Menu with administrator privileges:

Figure 5-1 Administration Main Menu

```
[Main Menu]
info          - Information 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]

>> Main#
```

NOTE – If you are using the operator account, some menu options will not be available.

For more information about initial system setup, see [Chapter 2, “Initial setup,”](#) on page 31. For details about accessing the CLI, see [“Accessing the CLI”](#) on page 123.

Idle time-out

By default, the system will disconnect your CLI session after 5 minutes of inactivity. This function is controlled by the idle time-out parameter as shown in the following command:

```
>> # /cfg/sys/adm/idle <time-out period>
```

where the *time-out period* is specified in seconds, as an integer from 300-3600 seconds. Or you can specify time-out in minutes, from 5 minutes (5m) to 60 minutes (60m).

Multiple administration sessions

It is possible to have more than one CLI or BBI administrator session open simultaneously. Although each concurrent administrator session is independent, when configuration changes are saved to the Single Software Image (SSI) that is shared by the firewall iSD, the saved changes affect all users. However, if multiple CLI or BBI administrators apply changes to the same set of parameters concurrently, the latest applied changes take precedence.

Global commands

Some basic commands are recognized throughout the entire menu hierarchy. These commands are useful for obtaining online help, navigating through menus, and for applying and saving configuration changes. See [Table 5-1](#).

Table 5-1 Global CLI commands (Part 1 of 2)

Command	Action
help [<i><command></i>]	Provides more information about a specific command on the current menu. When used without the <i>command</i> parameter, a summary of the global commands is displayed.
.	Redisplay the current menu.
.. or up	Go up one level in the menu structure.
/	If placed at the beginning of a command, go to the Main Menu. Otherwise, this is used to separate multiple commands placed on the same line.
apply	Apply and save pending configuration changes.
diff	Show any pending configuration changes.
exit	Exit from the CLI and log out.

Table 5-1 Global CLI commands (Part 2 of 2)

Command	Action
lines <n>	Set the number of lines (<i>n</i>) that display on the screen at one time. The default is 24 lines. When used without a value, the current setting is displayed.
nslookup	Find the IP address or host name of a network device. The format is as follows: nslookup <host name IP address> To use this command, you must have configured the firewall iSD to use a Domain Name System (DNS) server. If you did not specify a DNS server during the initial setup procedure, you can add a DNS server at any time by using the <code>/cfg/sys/dns/add</code> command.
paste	Set a password for restoring a saved configuration dump file that includes encrypted private keys.
ping	Use this command to verify station-to-station connectivity across the network. The format is as follows: ping <address> [<tries> [<delay>]] Where <i>address</i> is the hostname or IP address of the device, <i>tries</i> (optional) is the number of attempts (1-32), and <i>delay</i> (optional) is the number of milliseconds between attempts. The DNS parameters must be configured if specifying hostnames (see “DNS Servers Menu” on page 151).
pwd	Display the command path used to reach the current menu.
revert	Cancel all pending configuration changes.
tracert	Use this command to identify the route used for station-to-station connectivity across the network. The format is as follows: tracert <address> [<max-hops> [<delay>]] Where <i>address</i> is the hostname or IP address of the target station, <i>max-hops</i> (optional) is the maximum distance to trace (1-16 devices), and <i>delay</i> (optional) is the number of milliseconds for wait for the response. As with <code>ping</code> , the DNS parameters must be configured if specifying hostnames.
verbose <n>	Sets the level of information displayed on the screen: 0 = Quiet: Nothing (including prompts) appears except errors. 1 = Normal: Prompts and requested output are shown, but no menus. 2 = Verbose: Everything is shown. When used without a value, the current setting is displayed.

Command line history and editing

Using the CLI, you can retrieve and modify previously entered commands with just a few keystrokes. [Table 5-2](#) lists options that are available globally at the command line.

Table 5-2 Command line history and editing options

Option	Description
history	Display a numbered list of the last ten previously entered commands.
!!	Repeat the last entered command.
!<i>n</i>	Repeat the <i>n</i> th command shown on the history list.
<Ctrl-p> (Also the up arrow key)	Recall the <i>previous</i> command from the history list. This can be used multiple times to work backwards through the last ten commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-n> (Also the down arrow key)	Recall the <i>next</i> command from the history list. This can be used multiple times to work forward through the last ten commands. The recalled command can be entered as is, or edited using the options below.
<Ctrl-a>	Move the cursor to the beginning of the command line.
<Ctrl-e>	Move cursor to the end of the command line.
<Ctrl-b> (Also the left arrow key)	Move the cursor back one position to the left.
<Ctrl-f> (Also the right arrow key)	Move the cursor forward one position to the right.
<Backspace> (Also the Delete key)	Erase one character to the left of the cursor position.
<Ctrl-d>	Delete one character at the cursor position.
<Ctrl-k>	Kill (erase) all characters from the cursor position to the end of the command line.
<Ctrl-l>	Redraw the screen.
<Ctrl-u>	Clear the entire line.
Other keys	Insert new characters at the cursor position.

Command line shortcuts

Command stacking

As a shortcut, you can type multiple commands on a single line separated by forward slashes (/). You can connect as many commands as required to access the a specific menu option. For example, the command stack to access the access list menu from the `Main#` prompt is as follows:

```
>> Main# cfg/sys/accesslist
```

Command abbreviation

Most commands can be abbreviated by entering the first characters that distinguish the command from the others in the same menu or submenu. For example, the command shown above could also be entered as follows:

```
>> Main# c/s/acc
```

Tab completion

By entering the first letter of a command at any menu prompt and pressing **Tab**, all commands in that menu beginning with the letter you typed are displayed. By typing additional letters, you can further refine the list of commands or options displayed. If only one command matches the letter or letters when **Tab** is pressed, that command will be supplied on the command line. You can then execute the command by pressing **Enter**. If the **Tab** key is pressed without any input on the command line, the currently active menu will be displayed.



CHAPTER 6

Command reference

/

Main Menu

After initial system setup is complete, and the user performs a successful connection and login, the Main Menu of the CLI is displayed. [Table 6-1 on page 136](#) identifies command syntax and usage for the Main Menu.

```
[Main Menu]
  info      - Information 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]
```

Table 6-1 Main Menu (Part 1 of 3)

Command Syntax and Usage

info

The Information Menu is used for displaying information about the current status of the firewall Alteon Firewall.

See [page 138](#) for menu items.

cfg

The Configuration Menu is used for configuring the firewall Alteon Firewall. Some commands are available only from an administrator login.

See [page 144](#) for menu items.

boot

The Boot Menu is used for upgrading firewall software and for rebooting, if necessary. The Boot Menu is accessible using an administrator or boot login.

See [page 210](#) for menu items.

maint

The Maintenance Menu is used for sending a technical support dump to a TFTP server.

See [page 212](#) for menu items.

diff

This global command is available from any menu or submenu. It displays the difference between the applied configuration (the configuration that the system is currently using) and the pending configuration (the changes that have not yet been applied).

Only pending changes made during your current administrator session are included. Pending changes being made by other CLI or BBI administrator sessions are not included.

Table 6-1 Main Menu (Part 2 of 3)

Command Syntax and Usage

apply

This global command is available from any menu or submenu. It is used to apply and save configuration changes made during your current administration session. Changes are considered pending and do not take effect until this command is issued. Pending changes being made by other CLI or BBI administrator sessions are not affected.

When issued, the `apply` command first validates the pending changes of your session. If problems are found, applicable warning and error messages are displayed. Errors are serious and will cause the `apply` command to fail before any changes are applied. If there are no errors (warnings are allowed), the changes are saved and put into effect. Warning messages can be turned off using the `/cfg/misc/warn` command (see [page 209](#)).

If multiple CLI or BBI administrators apply changes to the same set of parameters concurrently, the latest applied changes take precedence.

The global `revert` command clears pending changes and will not restore the configuration to previous settings once the `apply` command is issued.

revert y|n

This global command is available from any menu or submenu. It cancels all pending configuration changes made during your current administration session. Applied changes are not affected. Pending changes made by other open CLI or BBI sessions are also not affected.

paste [*<global key import password>*]

This global command is available from any menu or submenu. It lets you restore a saved configuration dump file that includes encrypted private keys.

If private keys were included when you created your configuration dump file (`/cfg/dump`), you were required to specify a password phrase for encrypting the private keys. When the `paste` command is issued, you will be prompted to supply the same password phrase. You can then open the configuration dump file in your text editor, copy the information, and paste it to the CLI window.

When pasted, the configuration content is batch processed by the firewall Alteon Firewall. The pasted commands are entered as pending, and any included private keys are decrypted. You can view the pending configuration changes resulting from the batch processing by using the global `diff` command. To apply the pending configuration changes, use the global `apply` command.

The `paste` password phrase remains in effect until cleared. To clear the password phrase, enter the `paste` command again.

Table 6-1 Main Menu (Part 3 of 3)

Command Syntax and Usage

help [*<menu command>*]

This global command is available from any menu or submenu. It provides brief information about any specific command in the current menu.

When used without a parameter, the `help` command displays a list of global commands.

exit

This global command is available from any menu or submenu. It exits the CLI and logs out the current session. Pending changes made during your current session will be lost if not applied. This command does not affect other open CLI or BBI sessions.

/info

Information Menu

```
[Information Menu]
  summary    - Show summary of all hosts and operational status
  clu        - Show runtime information of all hosts
  host       - Show runtime information of one host
  net        - Show network configuration
  fw         - Show firewall configuration
  lic        - Show all firewall licenses
  telnet     - Show Telnet configuration
  ssh        - Show SSH configuration
  web        - Show Web configuration
  log        - Show Log configuration
```

The Information Menu is used for displaying information about the current status of the firewall iSD. [Table 6-2](#) identifies command syntax and usage for the Information Menu

Table 6-2 Information Menu (/info) (Part 1 of 2)

Command Syntax and Usage

summary

This command displays the run-time information for the iSD host, including the host IP address, type (master), MIP, Local (all IP addresses in the local network route cache), cpu usage, mem (hard disk) usage of the log partition, and operational status (up/down).

clu

This command displays run-time information for all firewall Alteon Firewalls in the cluster. Information includes CPU usage, hard disk usage, status of important applications such as Web server, Check Point firewall, SNMP, and Inet server.

host

This command displays run-time information for the specified firewall Alteon Firewall host. Information includes run-time and application status, as well as the status of all network interface ports, and syslog messages.

To view menu items, see [page 140](#).

net

This command displays the current network configuration. This is the same information that is displayed using the `/cfg/net/cur` command.

To view menu items, see [page 141](#).

fw

This command displays the Alteon Firewall (firewall) status (enabled or disabled). This is the same information that is displayed using the `/cfg/fw/cur` command.

lic <Host IP Address>

This command displays the current Check Point license information for the selected host. Displayed information includes host IP address, license expiration date, signature string, and feature string. This is the same information available using the `/cfg/pnp/cur` command.

telnet

This command displays the current Telnet configuration settings: enabled or disabled. This is the same information available using the `/cfg/sys/adm/telnet/cur` command.

ssh

This command displays the current SSH configuration settings: enabled or disabled. This is the same information available using the `/cfg/sys/adm/ssh/cur` command.

Table 6-2 Information Menu (/info) (Part 2 of 2)**Command Syntax and Usage****web**

This command displays the current BBI configuration settings. Displayed information includes status (enabled or disabled) and service port number for HTTP and HTTPS (with Secure Socket Layer [SSL]), and certificate information for SSL. This is the same information available using the `/cfg/sys/adm/web/cur` command.

log

This command displays the configuration of the syslog, system log, ELA log, and log archiving.

/info/host

Info_host Menu

```
[info_host Menu]
  status      - Show runtime information
  link        - Show physical ports link status
  syslog      - Show syslog entries
```

This menu provides configuration, status, and statistics information on the run-time, link, ethernet, and syslog parameters of the host. [Table 6-3](#) identifies commands and usage for the Info_Host Menu.

Table 6-3 Info_Host Menu (/info/host)**Command Syntax and Usage****status** <Host number>

This command displays the run-time and application status for the specified host.

link

This command displays the status information for all network interface ports. The autonegotiate status and link status (UP or DOWN) are always displayed. If the link status is UP, the port speed (10, 100, or 1000 MHz) and the mode (full duplex or half duplex) are displayed.

syslog

This command displays the last 100 syslog messages. After each set of ten syslog messages is displayed, you are prompted to continue the display (enter **y**) or exit (enter **n**).

/info/net

Information Menu

```
[info_net Menu]
  if          - Show interface details
  route      - Show route configuration
  vrrp       - Show vrrp details
  parp       - Show parp configuration
```

The Information Menu shows the interface, route, and Virtual Router Redundancy Protocol (VRRP) details. [Table 6-4](#) identifies command syntax and usage for the Information Menu.

Table 6-4 Info_net Menu (/info/net)

Command Syntax and Usage

if

This command displays the interface details (ID, IP address and netmask, port assignment, operational status, VLAN number).

route

This command opens the info_net_route menu which has two options: `static` displays static route configuration details (destination IP address, destination mask, gateway IP address, interface number), and `ospf` opens the Open Shortest Path First (OSPF) Router Information Menu.

See [/info/net/route/ospf](#) below for menu items.

vrrp

This command opens the info_net_vrrp menu, which displays VRRP configuration and status information. See [page 143](#) for menu items.

parp

This displays the Proxy ARP status (enable = y/n) and the list of Proxy Address Resolution Protocol (ARP) entries (IP address in dotted decimal notation and group number).

/info/net/route

Route Information Menu

```
[info_net_route Menu]
  static     - Show static routes configuration
  ospf       - OSPF Router Menu
```

The Route Information Menu displays information on static and OSPF routes. [Table 6-5](#) identifies command syntax and usage for the Route Information Menu.

Table 6-5 Route Information Menu (/info/net/route)

Command Syntax and Usage

static

This command displays all static routes configured on the system.

ospf

This command opens the OSPF Router Information Menu. See [page 142](#) for menu items.

/info/net/route/ospf

OSPF Router Information Menu

[OSPF Router Information Menu]	
routes	- Display routes learned from OSPF
lsa	- Display OSPF LSA information
neigh	- Display OSPF neighbor information
if	- Display OSPF interface information
fib	- Display OSPF router FIB
ospf	- Show OSPF configuration

NOTE – ClusterXL and Floodgate-1 are not supported on this release.

The OSPF Router Information Menu displays status, configuration, and learned information on OSPF operation. [Table 6-6](#) identifies command syntax and usage for the OSPF Router Information Menu.

Table 6-6 OSPF Router Information Menu (/info/net/ospf) (Part 1 of 2)

Command Syntax and Usage

routes

This command displays all OSPF routes from the unicast table.

lsa

This command displays the OSPF Links State Advertisement (LSA) tables, which include the link ID, ADV router, age, sequence #, checksum, and link count.

Table 6-6 OSPF Router Information Menu (/info/net/ospf) (Part 2 of 2)**Command Syntax and Usage****neigh**

This command displays information about the OSPF neighbors of the cluster. *Neighbors* are routing devices that maintain information about each others' health.

if

This command displays status and configuration information about the configured OSPF interfaces.

fib

This command displays all OSPF routes contained in the Forwarding Information-Base (FIB) advertised by the firewall iSD. This includes routes which have been redistributed from other protocols.

ospf

Displays the current configuration for all of the OSPF setup parameters.

/info/net/vrrp

VRRP Information Menu

```
[info_net_vrrp Menu]
  status      - Show VRRP status
  cfg         - Show VRRP configuration
```

The VRRP Information Menu displays information on the status and configuration of VRRP. [Table 6-7](#) identifies command syntax and usage for the VRRP Information Menu.

Table 6-7 VRRP Information Menu (/info/net/vrrp)**Command Syntax and Usage****status**

This command displays the status for the VRRP Virtual Router ID (vrid).

cfg

This command displays the VRRP settings including high availability (enable/disable), VRRP advertisement interval, GARP delay interval, GARP broadcast interval, Port Healthcheck Interval, and Advanced Failover Check (AFC).

NOTE – ClusterXL was added to the command structure in Release 2.2.4, but was not fully tested in time for the software release to manufacturing. Please do not attempt to implement ClusterXL with Release 2.2.7 software.

/cfg Configuration Menu

```
[Configuration Menu]
  sys          - System-wide Parameter Menu
  net          - Network Configuration Menu
  pnp         - Firewall License Menu
  fw          - Firewall Configuration Menu
  ptcfg       - Backup current configuration to TFTP/FTP server
  gtcfg       - Restore current configuration from TFTP/FTP server
  misc        - Miscellaneous Settings Menu
  dump        - Dump configuration on screen for copy-and-paste
  cur         - Display current settings
```

The Configuration Menu is used for configuring the firewall Alteon Firewall. Some commands are available only from the administrator login. [Table 6-8](#) identifies command syntax and usage for the Configuration Menu.

Table 6-8 Configuration Menu (/cfg) (Part 1 of 3)

Command Syntax and Usage

sys

The System Menu is used for configuring system-wide parameters.

See [page 146](#) for menu items.

net

The Network Configuration Menu is used to configure the networks passing traffic through the firewall.

See [page 183](#) for menu items.

pnp

The Firewall License (Plug N Play) Menu is used for pre-configuring Check Point licenses.

See [page 204](#) for menu items.

Table 6-8 Configuration Menu (/cfg) (Part 2 of 3)

Command Syntax and Usage

fw

The Firewall Configuration Menu is used to enable the firewall or reset the Check Point Secure Internal Communications (SIC).

See [page 205](#) for menu items.

ptcfg *<TFTP/FTP server>* *<server host name/IP address>* *<file name>*

This command saves the current configuration, including private keys and certificates, to a file on the selected TFTP server. The information is saved in a plain-text file, and can later be restored by using the `gtcfg` command.

You are prompted to specify a password phrase before the information is sent to the TFTP server. The password phrase is used to encrypt all included private keys. If you later restore the configuration using the `gtcfg` command, you will be prompted to re-enter the password phrase.

gtcfg *<TFTP server>* *<file name>*

This command retrieves and applies a configuration file, including private keys and certificates, from the selected TFTP server. You will be prompted to enter the same password phrase specified when the file was created using the `ptcfg` command.

NOTE – You must reboot the firewall iSD after restoring a configuration using the `/cfg/gtcfg` command.

misc

The Miscellaneous Settings Menu is used to turn on or off configuration warning messages.

See [page 209](#) for menu items.

Table 6-8 Configuration Menu (/cfg) (Part 3 of 3)**Command Syntax and Usage****dump**

This command displays the current configuration parameters in CLI-compatible format. You can capture the screen display and save the configuration to a text editor file by performing a copy and paste operation. The configuration can later be restored by pasting the contents of the saved text file at any command prompt in the CLI.

When pasted, the content is batch processed by the firewall Alteon Firewall. To view the pending configuration changes resulting from the batch processing, use the `diff` command. To apply the configuration changes, use the `apply` command.

If you choose to include private keys in the configuration dump, you are required to specify a password phrase. The password phrase you specify will be used to encrypt all secret information. When restoring a configuration that includes secret information, use the global `paste` command. Before pasting the configuration, you will be prompted to reenter the password phrase.

cur

This command displays all current configuration settings. The output of the `cur` command is for viewing only. It cannot be captured to a file and later restored. If you wish to save the configuration for restoration later on, use the `dump` or `ptcfg` commands.

/cfg/sys

System Menu

```
[System Menu]
  backup      - Backup and Restore system configuration
  time        - Date and Time Menu
  dns         - DNS Servers Menu
  cluster     - Cluster Menu
  accesslist  - Access List Menu
  adm         - Administrative Applications Menu
  log         - Platform Logging Menu
  user        - User Access Control menu
  cur         - Display current settings
```

The System Menu is used for configuring system-wide parameters. [Table 6-9](#) identifies command syntax and usage for the System Menu.

Table 6-9 System Menu (/cfg/sys) (Part 1 of 2)

Command Syntax and Usage

backup

The Backup Menu is used to support configuration backup and restore on a remote TFTP/FTP server or to a folder on the firewall iSD host.

time

The Date and Time Menu is used to set the date, time, and time zone options.

See [page 149](#) for menu items.

dns

The DNS Servers Menu lets you change DNS parameters.

See [page 151](#) for menu items.

cluster

This command displays the Host Information menu, which allows you to configure the host IP and MIP address for the firewall iSD. It also lets you assign a physical port to that network.

See [page 152](#) for menu items.

accesslist

The Access List Menu is used to restrict remote access to firewall Alteon Firewall management features. You can add, delete, or list trusted IP addresses that are allowed Telnet, SSH, or BBI access to the system. If the access list is not configured, users will not be able to access remote management features, even when those features are otherwise enabled.

See [page 154](#) for menu items.

adm

The Administrative Applications Menu is used to configure idle timeout, as well as firewall Alteon Firewall remote management features such as Telnet, SSH, SNMP, and the BBI.

See [page 155](#) for menu items.

log

The Platform Logging Menu is used to configure system message logging features. Messages can be logged to the system console terminal, ELA facility, and archived to a file that can be automatically e-mailed.

See [page 173](#) for menu items.

Table 6-9 System Menu (/cfg/sys) (Part 2 of 2)**Command Syntax and Usage****user**

The User Menu is used to add, modify, delete, or list firewall Alteon Firewall user accounts, and change passwords.

See [page 178](#) for menu items.

cur

This command displays the current settings for items in the System Menu.

/cfg/sys/backup

Backup Menu

```
[Backup Menu]
  bcklocal   - Backup the system configuration to local folder
  bckremote  - Backup the system configuration to ftp/tftp server
```

The Backup Menu is used to support configuration backup and restoration to a remote TFTP/FTP server or to a folder on the firewall iSD host. Both commands store configuration, licenses, firewall policies, and SIC information, making it unnecessary to download firewall policy or reset SIC after a reboot or system crash recovery (`bcklocal`) or cloning (`bckremote`). [Table 6-10](#) identifies command syntax and usage for the Backup Menu.

Table 6-10 Backup Menu (/cfg/sys/backup)**Command Syntax and Usage****bcklocal**

This command stores the iSD host configuration, firewall policies, licenses, and SIC information in a default local file. This file image is automatically restored after a reboot.

bckremote

This command stores the iSD host configuration, firewall policies, licenses, and SIC information in a file on a remote FTP or TFTP server. Backup to an FTP server requires a server IP address, username (default *anonymous*), and configuration filename. Backup to a TFTP server does not require a username. However, the filename you use must pre-exist on the TFTP server.

The commands have been implemented to support host cloning when configuring the second iSD host in a cluster (see [“Cluster backup and clone procedures” on page 363](#) for usage information).

/cfg/sys/time

Date and Time Menu

```
[Date and Time Menu]
date      - Set system date
time      - Set system time
tzone     - Set Timezone
ntp       - Configure NTP servers
cur       - Display current settings
```

The Date and Time Menu is used to set the system date, time, and time zone options. [Table 6-11](#) identifies command syntax and usage for the Date and Time Menu.

Table 6-11 Date and Time Menu (/cfg/sys/time)

Command Syntax and Usage

date <YYYY-MM-DD>

This command sets the system date according to the specified format.

time <HH:MM:SS>

This command sets the system time using a 24-hour clock format.

NOTE – It is recommended that you reboot the iSD host after entering a time change that is greater than 1 minute.

tzone

This command sets the system time zone. When entered without a parameter, you will be prompted to select your time zone from a list of continents/oceans, countries, and regions (if applicable).

ntp

The NTP Settings Menu is used to synchronize system time with Network Time Protocol (NTP) servers.

See [page 150](#) for menu items.

cur

This command displays the current settings for items in the Date and Time Menu.

/cfg/sys/time/ntp

NTP Servers Menu

```
[NTP Servers Menu]
  list      - List all values
  del       - Delete a value by number
  add       - Add a new value
```

The NTP Servers Menu is used to add or delete Network Time Protocol (NTP) servers that synchronize system time. [Table 6-12](#) identifies command syntax and usage for the NTP Servers Menu.

Table 6-12 NTP Servers Menu (/cfg/sys/time/ntp)

Command Syntax and Usage

list

This command lists all configured NTP servers by their index number and IP address.

del <*index number*>

This command lets you remove an NTP server from the configuration by specifying the index number of the server. Use the `list` command to display the index numbers and IP addresses of configured NTP servers.

add <*NTP server IP address*>

This command lets you add an NTP server. The NTP server with the specified IP address will be added to the list of NTP servers used to synchronize the firewall iSD system clock. A number of NTP servers (at least three) should be available in order to compensate for any discrepancies among the servers.

/cfg/sys/dns

DNS Servers Menu

```
[DNS Servers Menu]
list          - List all values
del          - Delete a value by number
add          - Add a new value
insert       - Insert a new value
move        - Move a value by number
```

The DNS Servers Menu lets you change DNS parameters. [Table 6-13](#) identifies command syntax and usage for the DNS Servers Menu.

Table 6-13 DNS Servers Menu (/cfg/sys/dns)

Command Syntax and Usage

list

This command displays all DNS servers by their index number and IP address.

del <index number>

This command lets you remove a DNS server by index number. Use the `list` command to display the index numbers and IP addresses of added DNS servers.

add <DNS server IP address>

This command lets you add a new DNS server. The DNS server with the specified IP address will be added.

insert <index number> <IP address>

This command lets you add a new DNS server to the list at the specified index position. All existing items at the specified index number and higher are incremented by one position.

move <from index number> <to index number>

This command removes the DNS server of the specified *from* index number and inserts it at the specified *to* index number.

/cfg/sys/cluster

Cluster Menu

```
[Cluster Menu]
  mip          - Set MIP address
  port         - Management Port
  host         - iSD Host Menu
  cur          - Display current settings
```

The Host Information Menu allows you to configure the host IP address and MIP address of the firewall Alteon Firewall, and assign a port to the management network of the host. [Table 6-14](#) identifies command syntax and usage for the Cluster Menu.

Table 6-14 Cluster Menu (/cfg/sys/host)

Command Syntax and Usage

mip <Management IP address>

This command lets you change the MIP address. The MIP address must be unique on the network. Assign a MIP address that is on the same subnet as the firewall iSD host IP.

NOTE – The MIP address supports clustered firewalls in a redundant failover network. You must configure the MIP address even if you do not have redundant firewall iSDs.

port

This command lets you assign a physical port to the firewall iSD host. If the port you enter has been previously assigned (see “/cfg/net” on [page 183](#)), the system will not apply the assignment.

host <iSD host number>

This commands provides access to the iSD Host Menu for the specified host. For information on the iSD Host Menu, see [page 153](#).

cur

This command displays the current settings for items in the Network Menu.

`/cfg/sys/cluster/host` <*iSD host number*> iSD Host Menu

```
[iSD Host 1 Menu]
  ip          - Set IP address
  hwplatform - Display hardware platform
  halt       - Halt the iSD
  reboot     - Reboot the iSD
  delete     - Remove iSD Host
  cur       - Display current settings
```

This menu allows you to change host-specific parameters for a specified iSD host *number*. The host number can be found using the `/cfg/sys/cluster/cur` command. [Table 6-15](#) identifies command syntax and usage for the iSD Host Menu.

Table 6-15 iSD Host Menu (`/cfg/sys/cluster/host` <*iSD host number*>) (Part 1 of 2)

Command Syntax and Usage

`ip` <*host IP address*>

This command is used to set the IP address of the currently selected iSD host. Changing this address does not affect the MIP address which defines the cluster itself. The IP address is specified using dotted decimal notation.

NOTE – You will be logged out when you apply the new IP address.

`hwplatform`

Displays the specified host's hardware platform model number.

`halt` [*y|n*]

After confirmation, this command stops the currently selected iSD host. Always use this command before turning off the device, or removing the 8660 SDM card from the chassis.

If the iSD host you want to halt has become isolated from the cluster, you will receive an error message when performing the `halt` command. You can then try logging in to the specific iSD host using its local serial port (or a Telnet or SSH connection to the iSD host's individually assigned IP address) and use the `/boot/halt` command.

`reboot` [*y|n*]

After confirmation, this command reboots the currently selected iSD host. If the iSD host you want to reboot has become isolated from the cluster, you will receive an error message when performing the `reboot` command. You can then try logging in to the specific iSD host using its local serial port (or a Telnet or SSH connection to the iSD host's individually assigned IP address) and use the `/boot/reboot` command.

Table 6-15 iSD Host Menu (/cfg/sys/cluster/host <iSD host number>) (Part 2 of 2)**Command Syntax and Usage****delete**

After confirmation, this command lets you remove the currently selected iSD host from the cluster, and resets the removed iSD host to its factory default configuration. The other iSD host in the cluster is unaffected.

To ensure that you remove the intended iSD host, view the current settings by using the `cur` command. To view the host number, type, and IP address for both iSD hosts in a cluster, use the `/cfg/sys/cluster/cur` command.

Once you have removed an iSD host from the cluster using the `delete` command, you can only access the device through a console terminal attached directly to its local serial port. You can then log in using the administration account (`admin`) and the default password (`admin`) to access the Setup Menu.

When two iSD hosts are present in a cluster, you cannot delete a particular iSD host if it is the only one that has a health status “up.” If attempting to delete a firewall Alteon Firewall host in this scenario, you receive an error message when performing the `delete` command. To delete an iSD host from the cluster while the other cluster member is down, see the `/boot/delete` command on [page 211](#).

NOTE – After deleting a host, it is recommended that you get the topology using the SmartDashboard and push the policies to the operational iSD host. Then use the Setup utility to *join* the cluster.

cur

This command displays the current settings for items in the current iSD Host Menu.

/cfg/sys/accesslist

Access List Menu

```
[Access List Menu]
  list      - List all values
  del       - Delete a value by number
  add       - Add a new value
```

The firewall Alteon Firewall can be managed remotely using Telnet, SSH, or the BBI. For security purposes, access to these features is restricted through the access list.

The access list allows the administrator to specify IP addresses or address ranges that are permitted remote access to the system. There is only one access list that is shared by all remote management features.

NOTE – If you have configured Check Point User Authentication, the access list is ignored.

Requests for remote management access from any client whose IP address is not on the access list are dropped. By default, the access list is empty, meaning that all remote management access is initially disallowed. You can still ping the iSD host from an IP address not listed in the access list, however.

When a client's IP address is added to the access list, that client is permitted to access all enabled remote management features.

Table 6-16 identifies command syntax and usage for the Access List Menu.

Table 6-16 Access List Menu (/cfg/sys/accesslist)

Command Syntax and Usage

list

This command displays all index and IP address information for all trusted clients that can access enabled remote management features.

del <index number>

This command lets you remove an access entry by index number. Use the `list` command to display the index numbers and IP addresses of access entries.

add <user network IP address> <IP subnet mask>

This command lets you add a new IP address or range of addresses to the access list. Any added clients are considered trusted and may access any enabled remote management features.

/cfg/sys/adm

Administrative Applications Menu

```
[Administrative Applications Menu]
idle          - Set CLI idle timeout
telnet        - Telnet Administration Menu
ssh           - SSH Administration Menu
web           - Web Administration Menu
snmp          - SNMP Administration Menu
cur           - Display current settings
```

The Administrative Applications Menu is used to configure firewall Alteon Firewall remote management features such as Telnet, SSH, SNMP, and the BBI. [Table 6-17](#) identifies command syntax and usage for the Administrative Application Menu.

Table 6-17 Administrative Application Menu (/cfg/sys/adm)

Command Syntax and Usage

idle <CLI time-out period in seconds (300-3600)>

This command sets amount of time that a local or remote CLI session can remain inactive before being automatically logged out. The time period is specified in seconds, from 300 to 3600. The default is 300 seconds (5 minutes).

NOTE – If you make changes to the firewall iSD configuration and do not apply them before the CLI times out, all changes will be lost.

telnet

The Telnet Administration Menu is used to enable or disable Telnet sessions for remote access to the firewall Alteon Firewall management CLI.

NOTE – Enabling Telnet is not enough to provide access for remote Telnet sessions. The Telnet user's IP address must also appear in the access list (see “[Defining the remote access list](#)” on page 124 and “[/cfg/sys/accesslist](#)” on page 154 for details).

See [page 157](#) for menu items.

ssh

The SSH Administration Menu is used to enable or disable SSH for remote access to the firewall Alteon Firewall management CLI. This menu is also used for generating SSH host keys.

See [page 158](#) for menu items.

web

The Web Administration Menu is used to configure the BBI. The BBI provides HTTP or Secure Socket Layer (SSL) access for remote management of the firewall Alteon Firewall using a web browser.

See [page 159](#) for menu items.

snmp

The SNMP Administration Menu is used to control Simple Network Management Protocol (SNMP) read access and to enable or disable SNMP event and alarm messages for the firewall Alteon Firewall.

See [page 166](#) for menu items.

cur

This command displays the current settings for items in the Administrative Applications Menu.

/cfg/sys/adm/telnet

Telnet Administration Menu

```
[Telnet Administration Menu]
  ena      - Enable Telnet
  dis      - Disable Telnet
  cur      - Display current settings
```

The Telnet Administration Menu is used to enable or disable remote Telnet access to the firewall iSD CLI. By default, Telnet access is disabled. Depending on the severity of your security policy, you can enable Telnet access and restrict it to one or more trusted clients.

[Table 6-18](#) identifies command syntax and usage for the Telnet Administration Menu.

NOTE – Telnet is not a secure protocol. All data (including the password) between a Telnet client and a firewall iSD is unencrypted and unauthenticated. If secure remote access is required, see [“Using Secure Shell” on page 127](#). For more information on the Telnet feature, see [“Using Telnet” on page 125](#).

Table 6-18 Telnet Administration Menu (/cfg/sys/adm/telnet)

Command Syntax and Usage

ena

This command enables the Telnet management feature. When enabled, Telnet access to the host IP address is allowed for trusted clients that have been added to the access list (see [“Defining the remote access list” on page 124](#)).

dis

This command disables the Telnet management feature. This is the default. When disabled, all active Telnet administration sessions will be terminated, and all net Telnet requests sent to the host IP address will be dropped.

NOTE – The firewall iSD uses *iptables* to implement access control to its management interfaces (SSH, Telnet, HTTP, and HTTPS). *Iptables* inspects packets above FireWall-1 in the TCP/IP stack, which allows the firewall iSD to limit external access to internal system management software that uses sockets to communicate.

cur

This command displays the current Telnet settings.

/cfg/sys/adm/ssh

SSH Administration Menu

```
[SSH Administration Menu]
ena          - Enable SSH
dis         - Disable SSH
gensshkeys  - Generate new SSH host keys
cur         - Display current settings
```

The SSH Administration Menu is used to enable or disable SSH for remote access to the firewall Alteon Firewall management CLI. This menu is also used for generating SSH host keys.

An SSH connection allows secure management of the firewall Alteon Firewall from any workstation connected to the network. SSH access provides server host authentication, encryption of management messages, and encryption of passwords for user authentication. By default, SSH is disabled. [Table 6-19](#) identifies command syntax and usage for the SSH Administration Menu.

For more information on the SSH feature, see [“Using Secure Shell” on page 127](#).

Table 6-19 SSH Administration Menu (/cfg/sys/adm/ssh)

Command Syntax and Usage

ena

This command enables the SSH management feature. When enabled, SSH access to the host IP address is allowed for trusted clients that have been added to the access list (see [“Defining the remote access list” on page 124](#)).

dis

This command disables the SSH management feature. This is the default. When disabled, all active SSH administration sessions will be terminated, and all net SSH requests sent to the host IP address will be dropped.

gensshkeys

This command generates new SSH host keys.

cur

This command displays the current SSH settings.

/cfg/sys/adm/web

Web Administration Menu

```
[Web Administration Menu]
  http      - HTTP Configuration Menu
  ssl       - SSL Configuration Menu
  cur       - Display current settings
```

The Web Administration Menu is used to configure the BBI. The BBI allows for refined, intuitive remote management of the firewall Alteon Firewall using a Web browser. The BBI can be configured to use HTTP (non-secure), HTTPS with SSL, or both. [Table 6-20](#) identifies command syntax and usage for the Web Administration Menu.

For more information, see [Chapter 7, “Browser-Based Interface](#) and [Chapter 8, “BBI forms reference](#).

Table 6-20 Web Administration Menu (/cfg/sys/adm/web)

Command Syntax and Usage

http

The HTTP Configuration Menu is used to configure BBI access using HTTP (non-secure).

See [page 160](#) for menu items.

ssl

The SSL Configuration Menu is used to configure BBI access using HTTPS with SSL. For security reasons, Nortel Networks recommends using SSL with the BBI.

See [page 161](#) for menu items.

cur

This command displays the current settings for items in the Web Administration Menu.

/cfg/sys/adm/web/http

HTTP Configuration Menu

```
[HTTP Configuration Menu]
port      - Set HTTP Port number
ena       - Enable HTTP
dis       - Disable HTTP
cur       - Display current settings
```

The HTTP Configuration Menu is used to configure BBI access using HTTP. By default, HTTP access is enabled, but restricted to trusted clients. Depending on the severity of your security policy, you can disable HTTP access and refine the list of trusted clients. [Table 6-21](#) identifies command syntax and usage for the HTTP Configuration Menu.

NOTE – HTTP is not a secure protocol. All data (including passwords) between an HTTP client and a firewall iSD is unencrypted and unauthenticated. If secure remote access is required, see the “[SSL Configuration Menu](#)” on page 161.

For more information, see [Chapter 7, “Browser-Based Interface](#) and [Chapter 8, “BBI forms reference](#).

Table 6-21 HTTP Configuration Menu (/cfg/sys/adm/web/http)

Command Syntax and Usage

port <HTTP port number>

This command sets the logical HTTP port that is used by the built-in BBI web server. By default, the web server uses HTTP port 80. This can be changed to use any port number, but ensure you set it to a port that is not being used by other services.

ena

This command enables HTTP access to the BBI. This is the default. When enabled, HTTP access to the host IP address is allowed for trusted clients that have been added to the access list (see “[Defining the remote access list](#)” on page 124).

dis

This command disables HTTP access to the BBI. When disabled, HTTP requests to the host IP address are dropped.

cur

This command displays the current HTTP settings.

/cfg/sys/adm/web/ssl

SSL Configuration Menu

```
[SSL Configuration Menu]
port      - Set SSL port number
ena       - Enable SSL
dis       - Disable SSL
tls       - Set TLS
sslv2     - Set SSL version 2
sslv3     - Set SSL version 3
certs     - Certificate Management Menu
cur       - Display current settings
```

The SSL Configuration Menu is used to configure BBI access using HTTPS. HTTPS uses SSL to provide server host authentication, encryption of management messages, and encryption of passwords for user authentication. Nortel Networks recommends that you use SSL with the BBI for security reasons. By default, SSL is disabled.

In addition to enabling and disabling the HTTPS feature, this menu allows you to set the HTTPS port, set SSL version, and access menus for generating SSL certificates. [Table 6-22](#) identifies command syntax and usage for the SSL Configuration Menu.

For more information, see [Chapter 7, “Browser-Based Interface](#) and [Chapter 8, “BBI forms reference](#).

Table 6-22 SSL Configuration Menu (/cfg/sys/adm/web/ssl) (Part 1 of 2)

Command Syntax and Usage

port <HTTPS port number>

This command sets the logical HTTPS port that is used by the built-in BBI web server. By default, the web server uses HTTPS port 443. This can be changed to use any port number, but ensure you set it to a port that is not being used by other services.

ena

This command enables HTTPS access to the BBI. When enabled, HTTPS access to the host IP address is allowed for trusted clients that have been added to the access list (see [“Defining the remote access list” on page 124](#)).

NOTE – An SSL certificate must be generated using the Certificate Management Menu (*certs*) before HTTPS will function.

dis

This command disables HTTPS access to the BBI. This is the default. When disabled, HTTPS requests to the host IP address will be dropped.

Table 6-22 SSL Configuration Menu (/cfg/sys/adm/web/ssl) (Part 2 of 2)**Command Syntax and Usage****tls** *y|n*

This command enables or disables Transport Level Security (TLS) for SSL.

sslv2 *y|n*

This command enables or disables SSL Version 2.

sslv3 *y|n*

This command enables or disables SSL Version 3.

certs

The Certificate Management Menu is used to configure server certificates and external Certificate Authority certificates required for SSL.

See [page 162](#) for menu items.**cur**

This command displays the current settings for items in the SSL Administration Menu, including security certificates.

/cfg/sys/adm/web/ssl/certs

Certificate Management Menu

```
[Certificate Management Menu]
serv      - Server Certificate Management Menu
ca        - Certificate Authority Management Menu
cur       - Display current settings
```

The Certificate Management Menu is used to add or remove server certificates and external Certificate Authority certificates required for SSL. [Table 6-23](#) identifies command syntax and usage for the Certificate Management Menu.

Table 6-23 Certificate Management Menu (/cfg/sys/adm/web/ssl/certs)

Command Syntax and Usage

serv

The Server Certificate Management Menu is used to generate a certificate request or create a self-signed certificate.

See [page 164](#) for menu items.

ca

The Certificate Authority Management Menu is used to manage intermediate Certification Authority (CA) certificates. This is required if server certificates from external CAs are being used.

See [page 165](#) for menu items.

cur

This command displays the current settings for items under the Certificate Management Menu.

/cfg/sys/adm/web/ssl/certs/serv

Server Certificate Management Menu

```
[Server Certificate Management Menu]
gen          - Generate certificate request - this erases old key
exp          - Export certificate request
list         - List server certificates
del          - Delete a server certificate
add          - Add a server certificate
cur          - Display current settings
```

The Server Certificate Management Menu is used to administer SSL server certificates. [Table 6-24](#) identifies command syntax and usage for the Server Certificate Management Menu.

Table 6-24 Server Certificate Management Menu (/cfg/sys/adm/web/ssl/certs/serv)

Command Syntax and Usage

gen <Common Name> <Country Code> <Key Size>

This command will generate a certificate request or a self-signed certificate.

exp

This command is used for exporting certificate requests to an external CA. This command produces output that can be copied and pasted into a text file and sent to the CA to be signed. Do not use this if creating a self-signed certificate. Once the CA has responded with a PEM encoded certificate, use the **add** command to enter the certificate into the system.

list

This command displays a list of configured server certificates.

del

This command is used for deleting a server certificate.

add

This command is used for adding a signed server certificate. After you have entered this command, the system will expect you to paste the PEM encoded certificate into the CLI. When done pasting the certificate, add three periods (. . .) and press **Enter** to return to the CLI.

cur

This command displays the current server certificate settings.

/cfg/sys/adm/web/ssl/certs/ca

CA Certificate Management Menu

```
[CA Certificate Management Menu]
  list      - List CA certificates
  del       - Delete a CA certificate
  add       - Add a CA certificate
  cur       - Display current settings
```

The CA Certificate Management Menu is used to administer SSL external CA certificates.

[Table 6-25](#) identifies command syntax and usage for the CA Certificate Management Menu.

Table 6-25 CA Certificate Management Menu (/cfg/sys/adm/web/ssl/certs/ca)

Command Syntax and Usage

list

This command lists all configured CA certificates.

del

This command is used to remove a CA certificate from the configuration.

add

This command is used to add an intermediate CA certificate. After you have entered this command, the system will expect you to paste the PEM encoded certificate into the CLI. When you have finished pasting the certificate, add three periods (. . .) and press **Enter** to return to the CLI.

cur

This command displays the current CA certificate settings.

/cfg/sys/adm/snmp

SNMP Administration Menu

```
[SNMP Administration Menu]
ena          - Enable SNMP
dis          - Disable SNMP
model       - Set security model
level       - Set usm security level
access      - Set read access control
events      - Set trap events
alarms      - Set trap alarms
rcomm       - Set v2c read community
users       - SNMP USM Users Menu
hosts       - Trap Hosts Menu
system      - SNMP System Information Menu
adv         - Advanced SNMP Options Menu
cur         - Display current settings
```

The firewall iSD software supports elements of SNMP. If you are running an SNMP network management station on your network, you can read firewall iSD configuration information and statistics using the following SNMP Managed Information Bases (MIBs):

- MIB II (RFC 1213)
- Ethernet MIB (RFC 1643)
- Bridge MIB (RFC 1493)

[Table 6-26](#) identifies command syntax and usage for the SNMP Administration Menu.

Table 6-26 SNMP Administration Menu (/cfg/sys/adm/snmp) (Part 1 of 3)

Command Syntax and Usage

ena

This command enables the SNMP features.

dis

This command disables the SNMP features. This is the default.

model v2c|usm

This command is used to specify the form of SNMP security to be used by a firewall iSD:

- v2c: Use the SNMP version 2C security model.
 - usm: Use the SNMP version 3 User-based Security Model (USM).
-

Table 6-26 SNMP Administration Menu (/cfg/sys/adm/snmp) (Part 2 of 3)

Command Syntax and Usage

level auth|priv

This command is used only when `usm` is selected. It is used to specify the degree of SNMP USM security:

- `auth`: Verify the SNMP user password before granting SNMP access. SNMP information is transmitted in plain text.
- `encrypt`: Verify the SNMP user password before granting SNMP access and encrypt all SNMP information with the user's individual key.

USM user names, along with their passwords and encryption keys, are defined in the SNMP Users Menu (/cfg/sys/adm/snmp/users)

access d|r

This command is used to enable read (r) or disable read (d) access for the read community.

events y|n

This command is used to enable or disable sending event messages to the SNMP trap hosts. When enabled, messages regarding general occurrences (for example, detection of a new component) are sent.

alarms y|n

This command is used to enable or disable sending alarm messages to the SNMP trap hosts. Alarm messages indicate serious conditions that can require administrative action.

rcomm

Displays the current read community value (the default is "public") and allows you to change it. There is no restriction on the input string.

users

The SNMP Users Menu is used to list, add, and remove USM users. When `usm` is selected as the security model, SNMP access is granted only for user/password combinations that are defined in both the SNMP Users Menu and in the Access List Menu (/cfg/sys/adm/accesslist).

See [page 168](#) for menu items.

hosts

The Trap Hosts Menu is used to add, remove, or list hosts that receive event or alarm messages.

See [page 170](#) for menu items.

Table 6-26 SNMP Administration Menu (/cfg/sys/adm/snmp) (Part 3 of 3)

Command Syntax and Usage

system

The SNMP System Information Menu is used to configure basic identification information such as support contact name, system name, and system location.

See page 215 for menu items.

adv

The Advanced SNMP Settings Menu is used to configure less common SNMP options.

See [page 216](#) for menu items.

cur

This command displays the current SNMP Administration Menu settings.

/cfg/sys/adm/snmp/users

SNMP Users Menu

[SNMP Users Menu]	
list	- List all users
del	- Delete a user by name
add	- Add a new user

The SNMP Users Menu is used to list, add, and remove USM users. When `usm` is selected as the security model (`/cfg/sys/adm/snmp/model`), SNMP access is granted only for user/password combinations defined both in this menu and in the Access List Menu (see [page 154](#)). [Table 6-27](#) identifies command syntax and usage for the SNMP Users Menu.

Table 6-27 SNMP Users Menu (/cfg/sys/adm/snmp/users (Part 1 of 2))

Command Syntax and Usage

list

This command lists all configured USM users.

Table 6-27 SNMP Users Menu (/cfg/sys/adm/snmp/users (Part 2 of 2))

Command Syntax and Usage

del <user name>

This command lets you remove a USM user from the configuration. Use the `list` command to display the configured USM users.

add <user name>

This command lets you add a USM user. When the command is initiated, you will be prompted to enter the following:

- `get` or `trap`, or both: specify whether the user is authorized to perform SNMP `get` requests or receive enabled `trap` event and alarm messages. Enter `get trap` to specify that both are allowed.
 - authorization password (and confirmation): password the user must enter for access.
 - encryption string (and confirmation): if the `level encrypt` option is used on the SNMP Administration Menu (/cfg/sys/adm/snmp), the encryption string is used to encode SNMP traffic between the user and the 8660 SDM.
-

/cfg/sys/adm/snmp/hosts

Trap Hosts Menu

```
[Trap Hosts Menu]
list          - List all values
del           - Delete a value by number
add           - Add a new value
insert        - Insert a new value
move          - Move a value by number
```

The Trap Hosts Menu is used to add, remove, or list hosts that will receive SNMP event or alarm messages from the firewall iSDs. [Table 6-28](#) identifies command syntax and usage for the Trap Hosts Menu.

Table 6-28 Trap Hosts Menu (/cfg/sys/adm/snmp/hosts)

Command Syntax and Usage

list

This command lists all configured trap hosts that will receive SNMP event or alarm messages from the firewall iSDs.

del <index number>

This command lets you remove an SNMP trap host from the configuration by specifying the index number of the trap host. Use the `list` command to display the index numbers and IP addresses of configured trap hosts.

add <trap host IP address> <port number> <community string> <trap user>

This command lets you add an SNMP trap host. The trap host with the specified IP address will receive any enabled SNMP messages from a firewall iSD. Event messages and alarm messages can be independently enabled or disabled in the SNMP Administration Menu (see [page 166](#)). You will be prompted to enter port number, community string, and trap user information.

insert <index number> <IP address>

This command lets you add a new trap host IP address to the access list at the specified index position. All existing items at the specified index number and higher are incremented by one position.

move <from index number> <to index number>

This command removes the trap host IP address of the specified “from” index number and inserts it at the specified “to” index number in the access list.

/cfg/sys/adm/snmp/system

SNMP System Information Menu

```
[SNMP System Information Menu]
contact      - Set Contact
name         - Set Name
loc          - Set Location
cur          - Display current settings
```

The SNMP System Information Menu is used to configure basic identification information such as support contact name, system name, and system location. [Table 6-29](#) identifies command syntax and usage for the SNMP System Information Menu.

Table 6-29 SNMP System Information Menu

Command Syntax and Usage

contact *<new string, maximum 64 characters>*

Configures the name of the system contact. The contact can have a maximum of 64 characters.

name *<new string, maximum 64 characters>*

Configures the name for the system. The name can have a maximum of 64 characters.

loc *<new string, maximum 64 characters>*

Configures the name of the system location. The location can have a maximum of 64 characters.

cur

This command displays the current SNMP System Information settings.

/cfg/sys/adm/snmp/adv

Advanced SNMP Settings Menu

```
[SNMP Advanced Settings Menu]
trapsrcip   - Set set source ip of traps
cur         - Display current settings
```

The Advanced SNMP Options Menu is used to configure less common SNMP options. [Table 6-30](#) identifies command syntax and usage for the Advanced SNMP Settings Menu.

Table 6-30 Advanced SNMP Settings Menu

Command Syntax and Usage

trapsrcip auto | unique | mip

This command is used to configure the source IP address that is to be used with SNMP traps generated from the 8660 SDM.

- auto: The IP address of the outgoing interface is used. This is the default.
- unique: The IP address of an individual firewall iSD is used.
- mip: The IP address of the cluster MIP is used. This setting is useful with applications (for example, versions of HP OpenView) that expect devices to be limited to only one IP address.

cur

This command displays the current settings for all options in the Advanced SNMP Settings Menu.

/cfg/sys/log

Platform Logging Menu

```
[Platform Logging Menu]
  syslog      - Syslog Logging Menu
  ela         - ELA Logging Menu
  arch        - Log Archiving Menu
  debug       - Set syslog debugging
  srcip       - Set syslog source ip mode
  cur         - Display current settings
```

The Platform Logging Menu is used to configure system message logging features. Messages can be logged to the system console terminal, ELA facility, archived to a file which can be automatically e-mailed, and used for debugging. [Table 6-31](#) identifies command syntax and usage for the Platform Logging Menu.

Table 6-31 Platform Logging Menu (/cfg/sys/log) (Part 1 of 2)

Command Syntax and Usage

syslog

The System Logging Menu is used to configure syslog servers. The firewall iSD software can send log messages to specified syslog hosts.

See [page 174](#) for menu items.

ela

The ELA Menu is used to configure the Event Logging API (ELA) feature. ELA allows log messages to be sent to a Check Point SmartCenter Server for display through the Check Point SmartView Tracker.

See [page 175](#) for menu items.

arch

The Log Archiving Menu is used to archive log files when the file reaches a specific size or age. When log rotation occurs, the current log file is set aside or e-mailed to a specified address and a new log file is begun.

See [page 176](#) for menu items.

debug y|n

This command is used to enable or disable specialized debugging log messages. This is disabled by default and should be enabled only as directed by Nortel Networks technical support.

Table 6-31 Platform Logging Menu (/cfg/sys/log) (Part 2 of 2)**Command Syntax and Usage****srcip** auto|unique|mip

This command is used to configure which source IP address will be used with logs generated from the iSDs.

- auto: The IP address of the outgoing interface is used. This is the default.
- unique: The IP address of the individual iSD is used.
- mip: The IP address of the cluster MIP is used. This setting is useful with applications (such as some versions of HP OpenView) that expect devices to be limited to only one IP address.

cur

This command displays the current settings for all items in the Platform Logging Menu.

/cfg/sys/log/syslog

System Logging Menu

```
[System Logging Menu]
  list      - List all values
  del       - Delete a value by number
  add       - Add a new value
  insert    - Insert a new value
  move     - Move a value by number
```

The System Logging Menu is used to configure syslog servers. The firewall iSD software can send log messages to specified syslog hosts. [Table 6-32](#) identifies command syntax and usage for the System Logging Menu.

Table 6-32 System Logging Menu (/cfg/sys/log/syslog) (Part 1 of 2)**Command Syntax and Usage****list**

This command displays all configured syslog servers by their index number, IP address, and facility number.

del <syslog index number>

This command lets you remove a syslog server from the configuration by specifying the server's index number.

Table 6-32 System Logging Menu (/cfg/sys/log/syslog) (Part 2 of 2)**Command Syntax and Usage**

add <syslog server IP address> <severity level>

This command lets you add a new syslog server, including its IP address and local facility number. The local facility number can be used to uniquely identify syslog entries.

insert <index number> <IP address>

This command lets you add a new syslog server to the list at the specified index position. All existing items at the specified index number and higher are incremented by one position.

move <from index number> <to index number>

This command removes the syslog server of the specified *from* index number and inserts it at the specified *to* index number.

/cfg/sys/log/ela

ELA Logging Menu

```
[ELA Logging Menu]
  ena          - Enable ELA
  dis          - Disable ELA
  addr         - Set management station IP address
  sev          - Set minimum logging severity
  dn           - Set management station DN
  pull         - Pull SIC certificate
  cur          - Display current settings
```

The ELA Logging Menu is used to configure the Event Logging API (ELA) feature. ELA allows log messages to be sent to a Check Point SmartCenter Server for display through the Check Point SmartView Tracker.

ELA configuration requires steps at both the firewall iSD and at Check Point SmartCenter Server. For configuration details, see [Chapter 12, “Event Logging API,” on page 349](#).

Table 6-33 identifies command syntax and usage for the ELA Logging Menu.

Table 6-33 ELA Logging Menu (/cfg/sys/log/ela)

Command Syntax and Usage

ena

This command is used to enable the ELA feature. When enabled, system log messages will be sent to the Check Point SmartCenter Server.

dis

This command is used to disable ELA. This is the default.

addr <IP address>

This command is used to set the IP address of the Check Point SmartCenter Server to which log messages will be sent. Specify the IP address in dotted decimal notation.

sev **emerg|alert|crit|err|warning|notice|info|debug**

This command is used to set the minimum logging severity level. All messages at the specified level of severity or higher will be logged to the ELA

dn <OPSEC SIC name>

This command is used to set the Distinguished Name (DN) of the Check Point SmartCenter Server. The DN is defined in the Check Point SmartDashboard under the management server properties. The DN is found in the Secure Internal Communication (SIC) area.

pull

This command is used to obtain a certificate for secure communication from the Check Point SmartCenter Server.

cur

This command displays the current ELA settings.

/cfg/sys/log/arch

Log Archiving Menu

[Log Archiving Menu]	
email	- Set e-mail address to send log
smtp	- Set SMTP server address
int	- Set log archive interval
size	- Set maximum size of archived log
cur	- Display current settings

The Log Archiving Menu is used to archive log files when the file reaches a specific size or age. When log rotation occurs, the current log file is set aside or e-mailed to a specified address and a new log file is begun.

If the rotate size is set above 0, then log rotation occurs when the log surpasses the rotate size, or when the log rotation interval is reached, whatever occurs first. If the rotate size is set to 0, the file size is ignored and only the rotate interval is used. If an e-mail address and SMTP Server IP address are set, then the log file is e-mailed when rotated. [Table 6-34](#) identifies command syntax and usage for the Log Archiving Menu.

Table 6-34 Log Archiving Menu (/cfg/sys/log/arch)

Command Syntax and Usage

email <*e-mail address*>

This command is used in conjunction with `smtp` to set the e-mail address where log files will be sent when the log interval or maximum log size is reached.

smtp <*SMTP server IP address*>

This command is used to set the IP address of the SMTP mail server that holds the e-mail address specified in the `email` command. The IP address should be specified in dotted decimal notation.

NOTE – The specified SMTP server must be configured to accept messages from the firewall iSDs. Also, a Check Point policy should be present to allow these messages through the firewall.

int <*days*> <*hours*>

This command is used to set the time interval at which the log files are rotated. The interval is specified in number of days and number of hours.

size <*max size (kb)*>

This command is used to set the maximum size a log file is allowed to reach before triggering rotation. The size is specified in kilobytes. If set to 0, the file size is ignored and only the interval (`int`) is used to determine rotation.

cur

This command displays the current log archiving settings.

/cfg/sys/user

User Menu

```
[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
adv        - Advanced User Configuration Menu
edit       - Edit a user
```

The User Menu is used to add, modify, delete, or list firewall iSD user accounts, and change passwords.

There are four default user accounts which cannot be deleted: `admin`, `oper`, `root`, and `boot`. See “Users and passwords” on page 120 for information about default passwords and privileges. Only the Administrator can change the passwords.

The password for the `boot` user cannot be changed. This ensures that if you were to lose all system passwords, the `boot` user would be able to access the system through the local serial port and reset the passwords by reinstalling the system software. Table 6-35 identifies command syntax and usage for the User Menu.

Table 6-35 User Menu (/cfg/sys/user) (Part 1 of 2)

Command Syntax and Usage

passwd <admin password> <new admin password> <confirm new admin password>

This command lets you change the administrator password. The password can contain spaces and is case sensitive. There is no limitation on the number of characters.

Only the `admin` user can perform this action. You will be prompted to enter the current administrator password. Then, you will be prompted to enter and confirm the new administrator password.

expire <# of seconds>

This command is used to set password expiration time in seconds. If the value is set to zero (the default), password expiration is not activated. After a password has expired, the user will be prompted at login to enter the old password once, and the new password twice.

NOTE – This command is visible only to users in the `admin` group, and does not apply to the `root` user.

Table 6-35 User Menu (/cfg/sys/user) (Part 2 of 2)**Command Syntax and Usage****list**

This command lists all editable user accounts. The `boot` user is not listed because this account cannot be altered.

del <user name>

This command lets you delete user accounts. Only the `admin` user can perform this action. Of the four default users (`admin`, `oper`, `root`, and `boot`), only the `oper` user can be deleted.

add <user name>

This command lets you add a user account. Only the `admin` user can perform this action. After adding a user account, you must also assign the account to a group using the User Admin Menu (`edit`).

adv

This command opens the SSH User Menu, which provides options for administering SSH user access.

See [page 180](#) for menu items.

edit <user name>

This command opens the User Oper Menu, which lets you edit the user account passwords and group privileges for the specified user/

See [page 181](#) for menu items.

/cfg/sys/user/adv

SSH User Menu

```
[SSH User Menu]
  user          - SSH User Menu
```

The SSH User Menu opens the SSH User Admin Menu. You must specify a user name to open the menu.

/cfg/sys/user/adv/user <user name> SSH User Admin Menu

```
[SSH User admin Menu]
name          - Set Full name of User
pubkey        - Set RSA/DSA Public Key for User
ena           - Enable User Account
dis           - Disable User Account
del           - Remove SSH User
```

The SSH User Admin Menu allows you to create an SSH account on the 8660 SDM. This provides the specified user with SSH access to the OS shell of the iSDs. Changes do not take place until you apply them. [Table 6-36](#) identifies command syntax and usage for the SSH User Admin Menu.

Table 6-36 SSH User Admin Menu (/cfg/sys/user/adv/user <user name>)

Command Syntax and Usage

name

Allows you to enter a descriptive name (like a full name) for the SSH account.

pubkey

Allows you to specify the RSA/DSA (Rivest Shamir Adelman/Digital Signature Algorithm) public key for the SSH account.

NOTE – The public key you enter must conform to OpenSSH v2 RSA or DSA format.

ena

Enables the SSH account per the specified user name.

dis

Disables the SSH account per the specified user name.

del

Deletes the SSH account.

/cfg/sys/user/edit <user name>

User Menu

[User oper Menu]	
password	- Login password
groups	- Groups
cur	- Display current setting

The User (user name) Menu is used to change passwords and assign group privileges for the user account specified by the *user name*. [Table 6-37](#) identifies command syntax and usage for the User Oper Menu.

Table 6-37 User Oper Menu (/cfg/sys/user/edit)

Command Syntax and Usage

password <admin password> <new user password> <confirm new user password>

This command lets you change the password for the selected user. The password can contain spaces and is case sensitive. There is no limitation on the number of characters.

Only the `admin` user can perform this action. You will be prompted to enter the current administrator password. Then, you will be prompted to enter and confirm the new user password.

groups <group name>

This command lets you add or delete the selected user to or from a group. By default there are three predefined groups: `admin`, `oper`, and `root`. For the privileges of each group, see [“Users and passwords” on page 120](#).

To view menu items, see [“Groups Menu” on page 182](#).

cur

This command displays the current group settings for the selected user.

/cfg/sys/user/edit *<user name>* /groups

Groups Menu

[Groups Menu]	
list	- List all values
del	- Delete a value by number
add	- Add a new value

Table 6-38 identifies command syntax and usage for the Groups Menu.

Table 6-38 Groups Menu (/cfg/sys/user/edit/groups)

Command Syntax and Usage

list

This command lists all group members by index number and name: for example,

```
1: admin
2: oper
```

del *<Index number of entry to delete>*

This command is used to delete a member from the selected group. Specify the member by its index number.

add *<Index number of entry to add>*

This command is used to add a member to the selected group. Specify the member by its index number.

/cfg/net

Network Configuration Menu

[Network Configuration Menu]	
port	- Port Menu
if	- Interface Menu
vrrp	- VRRP Settings Menu
adv	- Advanced Settings Menu
cur	- Display current settings

Table 6-39 identifies command syntax and usage for the Network Configuration Menu.

Table 6-39 Network Configuration Menu (/cfg/net)

Command Syntax and Usage

port <port number [1-3]>

This command displays the Port menu for the selected port number. To view menu items, see [page 184](#).

if <interface number [1-255]>

This command displays the Interface menu for the selected Interface. To view menu items, see [page 185](#).

vrrp

This command displays the VRRP Settings Menu for the cluster. To view menu items, see [page 188](#).

adv

This command displays the Advanced Settings Menu for the cluster. To view menu items, see [page 188](#).

cur

This command displays the current configuration for all items in the Network Configuration Menu.

/cfg/net/port <port number>

Port Menu

[Port 1 Menu]	
name	- Set port name
autoneg	- Autonegotiate value for the SDM management port
speed	- Speed setting for the SDM management port
mode	- Duplex setting for the SDM management port
cur	- Display current settings

The Port Menu is used for configuring the port characteristics for a specified port. [Table 6-40](#) identifies command syntax and usage for the Port Menu.

Physical Port Connector Characteristics

The RJ-45 copper connector are for attaching 10/100/1000 Mbps Ethernet (10Base-T or 100Base-TX) segments.

For physical port specifications and LED behavior, see *Installing the 8660 Service Delivery Module (SDM) for the Passport 8600 Series Switch* (part number 217314-A).

Table 6-40 Port Menu (/cfg/net/port) (Part 1 of 2)

Command Syntax and Usage

name <port name>

This command sets a name for the port. The assigned port name appears next to the port number on some information screens. The default is set to None.

autoneg on|off

This command is used to turn link autonegotiation on or off. If set to off, the port will operate at the speed set in the port speed command.

NOTE – Turning autonegotiation on or off may cause temporary interruption to network traffic on all ports.

speed <port speed>

This command is used to set the link speed of the port. Enter the port speed as an integer representing Mb/second.

All ports on the firewall iSD are Gigabit Ethernet ports. Speed is 10/100/1000.

Table 6-40 Port Menu (/cfg/net/port) (Part 2 of 2)**Command Syntax and Usage****mode**

This command is used to set the port duplex mode to either full-duplex or half-duplex. The default setting is `full`.

cur

This command displays the current settings for the selected port.

/cfg/net/if <interface number>**Interface Menu**

```
[Interface 1 Menu]
  addr1      - Set IP address-1
  addr2      - Set IP address-2
  mask       - Set Subnet mask
  vlanid     - Set VLAN tag id
  port       - Set Port number
  vrrp       - VRRP Interface Menu
  ena        - Enable interface
  dis        - Disable interface
  del        - Remove Interface
  cur        - Display current settings
```

The Interface Menu is used to configure IP interfaces for each firewall iSD. Each IP interface should be configured to represent a network attached to a firewall iSD host. [Table 6-41](#) identifies command syntax and usage for the Interface Menu.

NOTE – A network device that is attached to a firewall port must be configured to use an IP interface as its default gateway. This will direct traffic through the firewall iSD.

NOTE – Do not use the host IP address or any IP address in the firewall iSD subnet as the default gateway for a network.

Table 6-41 Interface Menu (/cfg/net/if) (Part 1 of 2)

Command Syntax and Usage

addr1 <interface IP address (e.g., 192.4.17.101)>

This command configures the IP address of the interface using dotted decimal notation. Devices on the connected networks should use this IP address as their default gateway so that their outbound traffic is directed to the firewall. The firewall iSD will support up to 255 IP interfaces.

If the interface is part of a VRRP high availability network configuration, addr1 is the virtual router IP address (see “[VRRP Interface Menu](#)” on page 187).

addr2

Reserved for future use...

mask <IP subnet mask (such as 255.255.255.0)>

This command configures the IP subnet address mask for the IP interface using dotted decimal notation.

vlanid <id number (0-4095)>

This command allows you to enter the vlanid for traffic intended for a vlan member on this interface. Only one vlanid is allowed per interface. The default vlanid is 0, which disables VLAN tagging for the interface. The maximum number of vlanids allowed per system is 255.

port <port number>

This command is used to assign a port to this IP interface. Only one port may be assigned to an interface. One port may be assigned to multiple interfaces, but the interface IP addresses must be on different networks.

NOTE – A port must be configured before it can be assigned to an interface. To configure a port, see “[Port Menu \(/cfg/net/port\)](#)” on page 184.

vrrp

The VRRP Menu is used for configuring an interface for high-availability when redundant iSD hosts are in a cluster. Virtual Router Redundancy Protocol (VRRP) ensures that if the active iSD host fails, the redundant iSD host will take over. In a high-availability configuration, each participating IP interface must be configured separately for VRRP.

See [page 187](#) for menu items.

Table 6-41 Interface Menu (/cfg/net/if) (Part 2 of 2)**Command Syntax and Usage****ena**

This command enables this IP interface.

dis

This command disables this IP interface.

del

This command removes this IP interface from the Firewall configuration.

cur

This command displays the current settings for this IP interface.

/cfg/net/if *<interface number>* **/vrrp** **VRRP Interface Menu**

```
[VrrpInterface Menu]
  vrid      - Set virtual router ID
  ip1       - Set IP1
  ip2       - Set IP2
  cur       - Display current settings
```

The VRRP Interface Menu is used for configuring redundant interfaces when two iSD hosts are present in a cluster. Virtual Router Redundancy Protocol (VRRP) ensures that if the active iSD host fails, the backup iSD host will take over.

With VRRP, the redundant interfaces form a *virtual router*. The interface IP address (/cfg/net/if<interface number>/addr1) becomes the *virtual router IP address* for both iSD hosts, though it is only active on the active master. Two additional sub-addresses (ip1 and ip2) must be assigned to the interface: ip1 represents iSD host 1 and ip2 represents iSD host 2. Each sub-address must be on the same network as the virtual router IP address.

NOTE – Both iSD hosts in the cluster must have the same configuration.

Table 6-42 identifies command syntax and usage for the VRRP Interface Menu. For more information on VRRP see “Virtual Router Redundancy Protocol” on page 294, “High Availability firewall configuration” on page 299.

Table 6-42 VRRP Interface Menu (/cfg/net/if/vrrp)

Command Syntax and Usage

vrid <virtual router ID (1-255)>

This command assigns an ID for the virtual router interface. The vrid on this interface must be configured the same for both the active master and the backup. Separate interfaces must have unique vrids.

NOTE – Vrids must be at least one number apart (e.g., vrids 1 and 2 are not acceptable; vrids 1 and 3 are acceptable).

ip1 <IP address>

This command defines the IP address used to represent iSD #1 in this virtual router. The ip1 address must be in the same subnet as the interface IP address (see/cfg/net/if <interface number>/addr1 or addr2 on page 185) and is specified using dotted decimal notation.

ip2 <IP address>

This command defines the IP address used to represent iSD #2 in this virtual router. The ip2 address must be in the same subnet as the interface IP address (see/cfg/net/if <interface number>/addr1 or addr2 on page 185) and is specified using dotted decimal notation.

cur

This command displays the current interface settings for VRRP.

/cfg/net/vrrp

VRRP Settings Menu

```
[VrrpSettings Menu]
  ha          - Set high availability
  aa          - Set Active-Active
  clusterxl   - Set Cluster XL
  adint       - Set Vrrp Advertisement Interval
  garp        - Set Garp Delay interval
  gbcast      - Set Garp broadcast interval
  phcintvl    - Set Port Healthcheck Interval
  afc         - Set Advanced failover check
  cur         - Display current settings
```

NOTE – Active-active and ClusterXL are not supported in this release.

NOTE – ClusterXL was added to the command structure in Release 2.2.4, but was not fully tested in time for the software release to manufacturing. ClusterXL will not be fully tested until the release of version 2.3.0. Please do not attempt to implement ClusterXL with Release 2.2.7 software.

The VRRP Settings Menu is for setting the Virtual Router Redundancy Protocol (VRRP) parameters for the cluster. Valid addresses must be specified for /cfg/net/vrrp ip1 and /cfg/net/vrrp ip 2 before changes to the parameter values can be applied (see “[VRRP Interface Menu](#)” on page 187 for more information on VRRP). For example configurations, see “[High Availability firewall configuration](#)” on page 299. [Table 6-43](#) identifies command syntax and usage for the VRRP Settings Menu.

NOTE – Both iSD hosts in the cluster must have the same configuration.

Table 6-43 VRRP Settings Menu (/cfg/net/vrrp) (Part 1 of 2)

Command Syntax and Usage

ha *y|n*

This command is used to enable (*y*) or disable (*n*) high-availability VRRP. Two iSD hosts, must be installed and configured for you to enable HA and apply the setting. Neither AA or Cluster XL can be enabled.

aa *y|n*

Active-active configuration is not supported on the 8660 SDM at this time.

clusterxl *y|n*

ClusterXL is not supported on the 8660 SDM at this time.

adint <1-3600>

This command displays the current advertisement interval in seconds and provides the option to change it. A VRRP advertisement message is sent by the active master to the backup. Only the active master sends VRRP advertisement messages. If the backup does not receive a VRRP advertisement from the active master within the adint interval, VRRP will initiate [VRRP failover](#) (see “[VRRP failover](#)” on page 297). The default value is 3. It is also the lowest recommended value.

Table 6-43 VRRP Settings Menu (/cfg/net/vrrp) (Part 2 of 2)

Command Syntax and Usage

garp [1-600]

This command displays the current Gratuitous Address Resolution Protocol (GARP) value in seconds and allows you to set it. When the backup determines that the active master has failed, it immediately flashes a GARP message (an unsolicited ARP response) to all end-hosts on the virtual router interface. Then the backup delays a period of time set by the `garp` value before it begins sending continuous GARP messages (see the `gbcast` command). The flash GARP message forces end-hosts to update their ARP caches with the MAC address/IP address mapping for the newly active iSD host instead of waiting for end-hosts to learn it through periodic ARP requests.

The default value is 1.

gbcast <2-100>

This command displays the present Gratuitous Broadcast (`gbcast`) value and allows you to change it. The `gbcast` value sets the interval between GARP messages that are sent by the active master to ensure that all end-hosts have the correct MAC address/IP address mapping. Increasing the `gbcast` value cuts down on the `gbcast` traffic, but lengthens the interval between end-host ARP cache updates.

The `gbcast` value is multiplied by the `/cfg/net/vrrp/adint` value to determine the interval in seconds between GARP messages. For example, if your `adint` value is 10 and your `gbcast` value is 3, the interval between GARP messages will be 30 (10 x 3) seconds. The default `gbcast` value is 2.

phcintvl [2-3600]

This command displays the current healthcheck interval and allows you to change it. The interval determines how often the system checks for link failures on the virtual router interface. However, VRRP failover based on links is not supported on the firewall iSDs at this time.

afc *y|n*

This command is used to enable (*y*) or disable (*n*) Advanced Failover Checking (AFC). When AFC is enabled, the system ARPs before initiating a failover caused by missed VRRP advertisements.

cur

This command displays the current settings for VRRP.

/cfg/net/adv

Advanced Settings Menu

```
[Advanced Settings Menu]
  route      - Routing Settings Menu
  parp       - Proxy Arp Menu
```

The Advanced Settings Menu provides access to advanced configuration features on the 8660 SDM. [Table 6-44](#) identifies command syntax and usage for the Advanced Settings Menu.

Table 6-44 Advanced Settings Menu (/cfg/net/adv/)

Command Syntax and Usage

route

This command displays the Routing Settings Menu for the cluster. To view menu items, see [page 191](#).

parp

This command displays the Proxy ARP Menu for the cluster. To view menu items, see [page 202](#).

/cfg/net/adv/route

Routing Settings Menu

```
[Routing Settings Menu]
  ospf       - Open Shortest Path First (OSPF) Menu
  gateway    - Set default gateway address
  routes     - Routes Menu
```

The Routing Settings Menu provides access to advanced routing features on a firewall iSD. [Table 6-45](#) identifies command syntax and usage for the Routing Settings Menu.

Table 6-45 Routing Settings Menu (/cfg/net/adv/route)

Command Syntax and Usage

ospf

The OSPF Menu is used to configure Open Shortest Path First (OSPF) routing protocol. See [page 192](#) for menu items.

gateway <gateway IP address>

This command configures the IP address of the default gateway of an iSD, using dotted decimal notation. It should be set to the IP address of the network router interface that is adjacent to the iSD to allow remote administrative (Telnet, SSH, BBI) access.

routes

The Routes Menu is used to add, delete, or list static routes. The iSD uses these routes to route packets within the attached networks.

See [page 201](#) for menu items.

/cfg/net/adv/route/ospf

OSPF Menu

[OSPF Menu]	
aindex	- OSPF Area (index) Menu
if	- OSPF Interface Menu
redist	- Route Redistribute Menu
rtrid	- Set OSPF router ID
spf	- Set time interval between two SPF calculations
ena	- Enable OSPF
dis	- Disable OSPF
cur	- Display current settings

The OSPF Menu is used to configure OSPF routing protocol. OSPF creates a Link-State Database (LSDB) that is shared between routers in an OSPF *area*. Any change in routing information is flooded to all routers in the network.

The routers use a link-state algorithm (Dijkstra's algorithm) to calculate the shortest path to all known destinations, based on the cumulative *cost* required to reach the destination. The routers then select the least cost path for each routing request, which optimizes traffic speed and efficiency in the network. [Table 6-46](#) identifies command syntax and usage for the OSPF Menu.

For more information on OSPF, see [Chapter 10, “Open Shortest Path First.”](#)

Table 6-46 OSPF Menu (/cfg/net/adv/route/ospf)

Command Syntax and Usage

aindex <area index (1-16)>

The OSPF Area Index Menu is used for defining OSPF area numbers and parameters.

NOTE – The area index specified in this menu option does not represent the actual OSPF area number. It is an arbitrary index used only on an iSD. The actual area value is defined in the OSPF Area Menu using the *id* option.

See [page 194](#) for menu items.

if <IP interface number (1-255)>

The OSPF Interface Menu is used for attaching IP interface networks to OSPF areas.

See [page 195](#) for menu items.

redist

The Route Redistribution Menu is used to define how routes from other protocols are converted for use with OSPF.

See [page 197](#) for menu items.

rtrid <router ID (router IP address)>

This command sets a static router ID for this cluster. The router ID is expressed in dotted decimal IP address format. OSPF, when enabled, uses the router ID to identify the routing device. If no router ID is specified or if the router IP is set to 0.0.0.0 and the iSD is rebooted, the cluster dynamically selects one of the active IP interfaces on the cluster as the router ID.

spf <calculation interval (0-65535)> <calculation hold time (0-65535)>

This command sets the time interval, in seconds, between each calculation of the shortest path tree. The default for spf calculation interval is 5 seconds and the default for spf calculation hold time is 10 seconds.

ena

This command globally turns on OSPF.

dis

This command globally turns off OSPF.

cur

This command displays current settings for all items in the OSPF configuration.

/cfg/net/adv/route/ospf/aindex <area index>

OSPF Area Index Menu

```
[OSPF Area Index 1 Menu]
  id      - Set area ID
  type    - Set area type
  ena     - Enable area
  dis     - Disable area
  del     - Remove OSPF Area Index
  cur     - Display current settings
```

The OSPF Area Index Menu is used for defining OSPF area numbers and parameters. [Table 6-47](#) identifies command syntax and usage for the OSPF Area Index Menu.

For more information on OSPF, see [Chapter 10](#), “Open Shortest Path First.”

Table 6-47 OSPF Area Index Menu (/cfg/net/adv/route/ospf/aindex)

Command Syntax and Usage

id <area ID, such as 0.0.0.0>

This command sets the OSPF area number in dotted decimal notation. The area number can be set using the last octet format (0.0.0.1 for area 1) or using multi-octet format (1.1.1.1), though the same format should be used throughout an area.

type transit|stub

This command sets the area type:

- transit for the backbone.
- stub for any area that contains no external routes.

The default type is transit.

ena

This command enables this area.

dis

This command disables this area.

del

This command deletes this area index from the configuration.

cur

This command displays current settings for all items in the OSPF Area Menu.

`/cfg/net/adv/route/ospf/if` <interface number>

OSPF Interface Menu

```
[OSPF Interface 1 Menu]
aindex      - Set area index
prio        - Set interface router priority
cost        - Set interface cost
hello       - Set hello interval in seconds
dead        - Set dead interval in seconds
trans       - Set transmit delay in seconds
retra       - Set retransmit delay in seconds
auth        - Set authentication type
key         - Set password authentication key
md5key      - Set MD5 authentication key
ena         - Enable interface
dis         - Disable interface
cur         - Display current settings
```

The OSPF Interface Menu is used for attaching IP interface networks to OSPF areas. [Table 6-48](#) identifies command syntax and usage for the OSPF Interface Menu.

For more information on using OSPF, see [Chapter 10, “Open Shortest Path First.”](#)

NOTE – The hello interval (hello), dead interval (dead), transmit interval (trans) and retransmit interval (retra) must be the same on all OSPF routing devices within an area. Using incompatible values could keep adjacencies from forming and could stop or loop routing updates.

Table 6-48 OSPF Interface Menu (`/cfg/net/adv/route/ospf/if`>) (Part 1 of 3)

Command Syntax and Usage

aindex <area index (1-16)>

This command sets the OSPF area index to attach to the network for the current IP interface.

prio <priority value (0-127)>

This command sets the IP interface (IF) priority that is used when electing a Designated Router (DR) and Backup Designated Router (BDR) for the area. The default is 1 (lowest priority). A value of 0 specifies that the elected interface is DROTHER and cannot be used as a DR or BDR.

Table 6-48 OSPF Interface Menu (/cfg/net/adv/route/ospf/if>) (Part 2 of 3)

Command Syntax and Usage

cost <output cost (1-65535)>

This command sets the cost of output routes on this interface. Cost is used in calculating the shortest path tree throughout the AS. Cost is based on bandwidth. Low cost indicates high bandwidth. The default is 1.

hello <hello interval(1-65535)>

This command sets the hello interval in seconds. The switch sends hello messages to inform neighbors that the link is up. The default is 10 seconds. This value must be the same on all routing devices within the area.

dead <dead interval (1-65535)>

This command sets the router dead interval, in seconds. If the switch does not receive `hello` on the IP interface within the dead interval, the switch will declare the interface to be down. Typically, the dead value is four times the value of `hello`. The default is 40 seconds. This value must be the same on all routing devices within the area.

trans <transmit delay (1-65535)>

This command sets the transmit delay, in seconds. This is the estimated time required to transmit an LSA to adjacencies on this interface, taking into account transmission and propagation delays. The default is 1 second. This value must be the same on all routing devices within the area.

retra <time interval (1-65535)>

This command sets the time interval, in seconds, between each transmission of LSAs to adjacencies on this interface. The default value is five seconds. This value must be the same on all routing devices within the area.

auth none | password | md5

This command sets the authentication type for this interface:

- `none` turns off OSPF authentication.
- `password` turns on type 1 (plain text) password authentication. The password is set using the `key` option.
- `md5` turns on MD5 (strong encryption) password authentication. The password is defined using `md5key` option.

For more information, see [“Authentication” on page 321](#).

key <type 1 password>

This option is used with the OSPF `auth` option (see [page 169](#)). When the `auth` option is set to `password`, the `key` option sets the password to be used for OSPF authentication on this IP interface. Specify a type 1 (plain text) password of up to eight characters. To clear the key, specify `none` as the value.

Table 6-48 OSPF Interface Menu (/cfg/net/adv/route/ospf/if>) (Part 3 of 3)**Command Syntax and Usage**

md5key <MD5 key number (1-255)> <MD5 authentication key>

This option is used to define an MD5 password for OSPF authentication on this IP interface. Specify the key ID number of an MD5 password defined in the OSPF md5key Entry Menu (see [page 177](#)). Assigned passwords are ignored until MD5 authentication is enabled in the `auth` option.

ena

This command enables this interface.

dis

This command disables this interface.

cur

This command displays current settings for all items in the OSPF Interface Menu.

/cfg/net/adv/route/ospf/redist

Route Redistribution Menu

```
[Route Redistribution Menu]
  connected - Connected Route Redistribution Menu
  static    - Static Route Redistribution Menu
  defaultgw - Default Gateway Redistribution Menu
  cur       - Display current settings
```

The Route Redistribution Menu is used to redistribute static and default gateway routes through OSPF. If the routes are learned from a certain routing protocol, you have to enable that protocol for those routes to be redistributed into the network. [Table 6-49](#) identifies command syntax and usage for the Route Redistribution Menu.

Table 6-49 Route Redistribution Menu (/cfg/net/adv/route/ospf/redist) (Part 1 of 2)**Command Syntax and Usage**

connected

The Connected Route Redistribution Menu is used for advertising connected routes through OSPF.

See [page 198](#) for menu items.

Table 6-49 Route Redistribution Menu (/cfg/net/adv/route/ospf/redist) (Part 2 of 2)**Command Syntax and Usage****static**

The Static Route Redistribution Menu is used for advertising static routes through OSPF.

See [page 199](#) for menu items.

defaultgw

The Default Gateway Redistribution Menu is used for advertising default gateway routes through OSPF.

See [page 200](#) for menu items.

cur

This command displays current settings for all items in the OSPF Route Redistribution Menu.

/cfg/net/adv/route/ospf/redist/connected OSPF Connected Route Redistribution Menu

[OSPF Connected Route Redistribution Menu]	
metric	- Set Metric assigned to connected routes
ena	- Enable redistribution of connected routes
dis	- Disable redistribution of connected routes
cur	- Display current settings

The OSPF Connected Route Redistribution Menu is used to redistribute connected routes into OSPF. [Table 6-50](#) identifies command syntax and usage for the OSPF Connected Route Redistribution Menu.

Table 6-50 OSPF Connected Route Redistribution Menu
(/cfg/net/adv/route/ospf/redist/connected)

Command Syntax and Usage

metric

Sets metric of advertised connected routes. The metric cost range is 1 to 16777214 (0-none) and indicates the relative cost of this route. The larger the cost, the less preferable the route. The default is 10. The metric type is t1 or t2 (type 1 or type 2).

OSPF Type1 is defined in the same units as OSPF interface cost (that is, in terms of the link state metric). OSPF Type 2 external metrics are an order of magnitude larger; any Type 2 metric is considered greater than the cost of any path internal to the AS. This configuration parameter can be used to have an OSPF domain prefer type1 routes over type 2. OSPF Type 1 is default.

ena

Enables advertising of connected routes.

dis

Disables advertising of connected routes.

cur

Displays current settings for the OSPF Connected Route Redistribution Menu.

/cfg/net/adv/route/ospf/redist/static OSPF Static Route Redistribution Menu

[OSPF Static Route Redistribution Menu]	
metric	- Set Metric assigned to connected routes
ena	- Enable redistribution of connected routes
dis	- Disable redistribution of connected routes
cur	- Display current settings

The OSPF Static Route Redistribution Menu is used to redistribute static routes into OSPF. [Table 6-51](#) identifies command syntax and usage for the OSPF Static Route Redistribution Menu.

Table 6-51 OSPF Static Route Redistribution Menu
(/cfg/net/adv/route/ospf/redist/static)

Command Syntax and Usage

metric

Sets metric of advertised static routes. The metric cost range is 1 to 16777214 (0-none) and indicates the relative cost of this route. The larger the cost, the less preferable the route. The default is 10. The metric type is t1 or t2 (Type 1 or Type 2).

OSPF Type1 is defined in the same units as OSPF interface cost (that is, in terms of the link state metric). OSPF Type 2 external metrics are an order of magnitude larger; any Type 2 metric is considered greater than the cost of any path internal to the AS. This configuration parameter can be used to have an OSPF domain prefer Type1 routes over Type 2. OSPF Type 1 is default.

ena

Enables advertising of static routes.

dis

Disables advertising of static routes.

cur

Displays the current static routes configured for redistribution into OSPF.

/cfg/net/adv/route/ospf/redist/defaultgw OSPF Default Gateway Route Redistribution Menu

[OSPF Default Gateway Route Redistribution Menu]	
metric	- Set Metric assigned to connected routes
ena	- Enable redistribution of connected routes
dis	- Disable redistribution of connected routes
cur	- Display current settings

The OSPF Default Gateway Route Redistribution Menu is used to redistribute default gateway routes into OSPF. [Table 6-52](#) identifies command syntax and usage for the OSPF Default Gateway Route Redistribution Menu.

Table 6-52 OSPF Default Gateway Route Redistribution Menu
(/cfg/net/adv/route/ospf/redist/defaultgw)

Command Syntax and Usage

metric

Sets metric of advertised default gateway routes. The metric cost range is 1 to 16777214 (0-none) and indicates the relative cost of this route. The larger the cost, the less preferable the route. The default is 10.

OSPF Type1 is defined in the same units as OSPF interface cost (that is, in terms of the link state metric). OSPF Type 2 external metrics are an order of magnitude larger; any Type 2 metric is considered greater than the cost of any path internal to the AS. This configuration parameter can be used to have an OSPF domain prefer type1 routes over type 2. OSPF Type 1 is default.

ena

Enables advertising of default gateway routes.

dis

Disables advertising of static routes.

cur

Displays the current default gateway routes configured for redistribution into OSPF.

/cfg/net/adv/route/routes

Routes Menu

[Routes Menu]	
list	- List all values
del	- Delete a value by number
add	- Add a new value
insert	- Insert a new value
move	- Move a value by number

The Routes Menu is used to add, delete, or list static routes. An iSD uses these static routes to route packets to indirectly attached internal networks. You can configure up to 96 routes. [Table 6-53](#) identifies command syntax and usage for the Route Menu.

Table 6-53 Route Menu (/cfg/net/adv/route/routes)

Command Syntax and Usage

list

This command lists all configured routes (dynamic routes generated by OSPF as well as static routes) by their index number and IP address information.

del <index number>

This command lets you remove a route from the configuration by specifying the route index number. Use the `list` command to display the index numbers of configured routes.

add <destination IP address> <destination mask> <gateway IP address>

This command adds a static route based on destination IP address, destination subnet mask, and gateway IP address. Enter all addresses using dotted decimal notation.

NOTE – The gateway IP address should be a previously specified interface address and should not be within the range specified by the destination IP address and mask.

insert <index number> <destination IP address> <destination mask> <gateway IP address>

This command lets you add a new static route at a specific position (*index number*) in the index. Use the `list` command to display the index numbers of configured routes.

move <index number> <destination index number>

This command lets you move a static route from one position in the index to another.

/cfg/net/adv/parp

Proxy Arp Menu

[Proxy Arp Menu]	
list	- Proxy ARP List Menu
enable	- Set Proxy ARP enable/disable
cur	- Display current settings

The Proxy ARP Menu is used to configure IP addresses for which the cluster sends ARP messages. The feature allows the 8660 SDM to respond to ARP requests intended for devices behind the firewall, including VLAN and VRRP interfaces. [Table 6-54](#) identifies command syntax and usage for the Proxy ARP Menu.

Table 6-54 Proxy ARP Menu (/cfg/net/adv/parp)

Command Syntax and Usage

list

This command opens the Proxy ARP List Menu, which allows you add, delete and list IP addresses that the cluster ARPs for.

enable y|n

This command lets you enable (y) or disable (n) Proxy ARP for the cluster. Proxy ARP is disabled by default.

cur

This command displays the enable status for Proxy ARP and lists the IP addresses that have been configured for Proxy ARP.

Proxy Arp List Menu

[Proxy ARP List Menu]	
list	- List all values
del	- Delete a value by number
add	- Add a new value

The Proxy ARP List Menu is used to add, delete, or list IP addresses for which the cluster Proxy sends ARP messages. [Table 6-55](#) identifies command syntax and usage for the Proxy ARP List Menu.

Table 6-55 Proxy ARP List Menu (/cfg/net/adv/parp/list) (Part 1 of 2)

Command Syntax and Usage

list

This command displays all Proxy ARP addresses in order by their index number.

Table 6-55 Proxy ARP List Menu (/cfg/net/adv/parp/list) (Part 2 of 2)**Command Syntax and Usage****del** <index number>

This command lets you remove a Proxy ARP address by specifying its index number. Use the `list` command to display the Proxy ARP index numbers.

add <IP address> <group #>

This command lets you add an address to the Proxy ARP list. Use dotted decimal notation to specify the address. The maximum number of addresses is 2,048, however, the recommended limit is 256. Typically the IP addresses are on the Untrusted Network(s).

The group # indicates whether the entry is for a device on `addr1` or `addr2` (see “/cfg/net/if <interface number>” on page 185). If you have a VRRP HA configuration, enter 1. If you do not have a VRRP configuration, enter 1.

A typical Proxy ARP entry is a virtual IP address on the interface that faces the external network. Next, a route is required between the Proxy ARP address and the destination address (see “/cfg/net/adv/route/routes” on page 201).

Finally, you must open the Check Point SmartDashboard and enter Network Address Translation (NAT) rules and policies to allow the Firewall to Proxy ARP for incoming ARP requests.

/cfg/pnp

Firewall License Menu

```
[Firewall License Menu]
list      - List detailed status of current IPs and Licenses
del       - Delete firewall license
add       - Add firewall license
```

The Firewall License Menu is used for pre-configuring Check Point licenses for the firewall iSD. [Table 6-56](#) identifies command syntax and usage for the Firewall License Menu.

Table 6-56 Firewall License Menu (/cfg/pnp)

Command Syntax and Usage

list

This command is used to list the IP addresses and Check Point licenses currently in the Plug N Play resource pool. Listed data includes the expiration dates of the licenses.

Licenses configured using the Check Point central licensing mechanism will not be listed using this command.

del

This command is used to remove an IP address and/or Check Point license from the Plug N Play resource pool. You will be prompted to enter the IP address you wish to have removed from the pool. Only unused resources can be deleted.

add

This command is used to add a Check Point license. You will be prompted to enter Check Point license information.

NOTE – The add command is for adding a license that is bound to the IP address of the Firewall.

/cfg/fw

Firewall Configuration Menu

```
[Firewall Configuration Menu]
ena          - Enable Firewall
dis          - Disable Firewall
sic          - Reset Check Point SIC.
sync        - Sync Configuration Menu
client       - SMART Clients
smart        - Smart Update Configuration Menu
cur          - Display current settings
```

The Firewall Configuration Menu is used to enable the firewall or reset the Check Point Secure Internal Communications (SIC). [Table 6-57](#) identifies command syntax and usage for the Firewall Configuration Menu.

Table 6-57 Firewall Configuration Menu (/cfg/fw)

Command Syntax and Usage

ena

Enable the Check Point FireWall-1 NG processing on all healthy firewall iSDs.

dis

Disable the Check Point FireWall-1 NG processing on the firewall iSD and mark the iSD as down. The Check Point SmartCenter Server cannot be used to manage firewall policies in the disabled state. However, the current firewall policies are maintained.

NOTE – When /cfg/fw/dis is entered, remote access to the firewall iSD CLI or the BBI is lost. Be sure to use the command when you are accessing the iSD CLI at the [local console](#).

sic

This command is used to reset the Check Point Secure Internal Communication (SIC) state for a specific firewall iSD. You will be prompted to enter the IP address of the target firewall iSD in dotted decimal notation.

sync

The Sync Configuration Menu is used to enable/disable session state synchronization between clustered firewall iSDs in a redundant configuration.

See [page 207](#) for menu items.

client

The SMART Clients Menu allows you to edit the list of SMART Clients that can access a firewall iSD when the SmartCenter Server is enabled on that firewall iSD.

See [page 208](#) for menu items.

smart

The SmartUpdate Configuration Menu is used to enable/disable Check Point software updating using the SmartUpdate utility.

See [page 209](#) for menu items.

cur

This command displays the current Firewall Configuration Menu settings.

/cfg/fw/sync

Sync Configuration Menu

```
[Sync Configuration Menu]
  ena          - Enable Sync
  dis          - Disable Sync
  cur          - Display current settings
```

The Sync Configuration Menu is used to enable/disable session state synchronization for clustered iSDs in a redundant configuration. This allows for a stateful failover to the backup iSD when the active iSD fails. [Table 6-58](#) identifies command syntax and usage for the Sync Configuration Menu.

NOTE – Nortel Networks recommends that you turn off synchronization for services that do not benefit from it, such as http.

Table 6-58 Sync Configuration Menu

Command Syntax and Usage

ena

This command enables session state synchronization in a redundant configuration. For synchronization to work, there must be a redundant iSD in the cluster that is properly configured (see the [“VRRP Interface Menu”](#) on page 187 and the [“VRRP Settings Menu”](#) on page 188). For instructions on how to test the synchronization network, see the `/maint/diag/fw/sync` command on [page 213](#).

You must also update the firewall interface information for state synchronization at the Check Point SmartDashboard (see [Step 6](#) in the [“Example SmartDashboard configuration for HA”](#) on page 312).

dis

This command disables session state synchronization in a redundant configuration.

cur

This command displays the present configuration status for session state synchronization.

/cfg/fw/client

SMART Clients Menu

```
[SMART Clients Menu]
list          - List all values
del           - Delete a value by number
add           - Add a new value
insert        - Insert a new value
move          - Move a value by number
```

The SMART Clients Menu allows you to specify SMART Clients by IP address that may manage an iSD, when the SmartCenter Server is enabled on the management port. [Table 6-59](#) identifies command syntax and usage for the SMART Clients Menu.

Table 6-59 SMART Clients Menu (/cfg/fw/client)

Command Syntax and Usage

list

Displays the list of SMART Clients with access to the 8660 SDM management server.

del <index value>

Allows you to delete a specified member from the SMART Clients list.

add <client IP address>

Allows you to add a member to the SMART Clients list. New members are appended to the end of the list.

insert <index value> <client IP address>

Allows you to insert a new member at the specified point in the SMART Clients list.

move <index value> <destination index value>

Allows you to change the order of members in the SMART Clients list. This option is for display purposes only. The order of the list has no impact on SMART Client access.

/cfg/fw/smart

SmartUpdate Configuration Menu

```
[Smart Update Configuration Menu]
ena           - Enable Smart Update Mode
dis           - Disable Smart Update Mode
cur           - Display current settings
```


The SmartUpdate Configuration Menu is used to enable/disable support for Check Point software updating using the SmartUpdate utility. SmartUpdate is an optional module for VPN-1/FireWall-1 that automatically distributes software applications and updates for Check Point and OPSEC Certified products (such as the 8660 SDM). You can also use SmartUpdate to manage product licenses. [Table 6-60](#) identifies command syntax and usage for the SmartUpdate Configuration Menu.

Table 6-60 SmartUpdate Configuration Menu (/cfg/fw/smart)

Command Syntax and Usage

ena

Enables support for SmartUpdate on the iSDs.

dis

Disables support for SmartUpdate on the iSDs.

cur

Displays the current configuration for SmartUpdate support.

/cfg/misc

Miscellaneous Settings Menu

[Miscellaneous Settings Menu]	
warn	- Set warnings when configuration is applied
cur	- Display current settings

The Miscellaneous Settings Menu is used to turn on or off configuration warning messages. [Table 6-61](#) identifies command syntax and usage for the Miscellaneous Settings Menu.

Table 6-61 Miscellaneous Settings Menu (/cfg/misc)

Command Syntax and Usage

warn y|n

This command is used to turn on or off warning messages. When enabled (the default), whenever the global `apply` command is issued, applicable warning are displayed if problems are found in the pending configuration changes. Warnings will not cause the `apply` command to fail, but can be helpful for managing configuration issues.

cur

This command displays the current settings for items in the Miscellaneous Settings Menu.

/boot

Boot Menu

```
[Boot Menu]
  software - Software Management Menu
  halt     - Halt the iSD
  reboot   - Reboot the iSD
  delete   - Delete the iSD
```

The Boot Menu is used for upgrading firewall software and for rebooting, if necessary. The Boot Menu is only accessible using an administrator login. [Table 6-62](#) identifies command syntax and usage for the Boot Menu.

Table 6-62 Boot Menu (/boot) (Part 1 of 2)

Command Syntax and Usage

software

The Software Management Menu is used to load, activate, or remove firewall software upgrade packages.

See [page 211](#) for menu items.

halt

After confirmation, this command stops the firewall iSD to which you have connected using Telnet, SSH, or a console terminal. If using Telnet or SSH, use this command only when you have connected to a particular firewall iSD's individually assigned IP address.

WARNING! – If you do not enter the halt command before powering off the firewall iSD, all configurations will be lost and the iSD will be reset to factory default settings.

reboot

After confirmation, this command reboots the particular firewall iSD to which you have connected using Telnet, SSH or console terminal. When using Telnet or SSH, use this command only when you have connected to a particular firewall iSD's individually assigned IP address.

Table 6-62 Boot Menu (/boot) (Part 2 of 2)**Command Syntax and Usage****delete**

After confirmation, this command resets the firewall iSD to its factory default configuration.

If you are using Telnet or SSH, only use this command when you are connected to the firewall iSD host IP address.

Once you have reset the firewall iSD to factory defaults, you can access the device only through a console terminal attached directly to the local serial port. You can then log in using the administration account (`admin`) and the default password (`admin`) to access the initial Setup utility.

/boot/software

Software Management Menu

```
[Software Management Menu]
cur          - Display current software status
activate    - Select software version to run
download    - Download a new software package via TFTP/FTP
del         - Remove downloaded (unpacked) releases
```

The Software Management Menu is used to load, activate, or remove firewall software upgrade packages. [Table 6-63](#) identifies command syntax and usage for the Software Management Menu.

Table 6-63 Software Management Menu (/boot/software) (Part 1 of 2)**Command Syntax and Usage****cur**

This command displays the software status of the particular firewall iSD to which your current Telnet, SSH, or a console terminal is connected.

activate <software version>

This command activates a downloaded and unpacked firewall software upgrade package. The unpacked software package will be labeled as `permanent`.

If serious problems occur while running the new software version, you may revert to using the previous version by activating the software version labeled as `old`.

NOTE – You will be logged out after confirming the `activate` command.

Table 6-63 Software Management Menu (/boot/software) (Part 2 of 2)**Command Syntax and Usage**

download <host name or IP address> <file name>

This command lets you download a firewall software upgrade package from an FTP or TFTP server. When prompted, select either tftp or ftp server, provide the host name or IP address of the TFTP server, and enter the filename of the software upgrade package

del

After confirmation, this command lets you remove a software upgrade package that has been downloaded using the `download` command. This command deletes the most recently downloaded software upgrade package.

/maint**The Maintenance Menu**

```
[Maintenance Menu]
diag          - Diagnostic Tools Menu
tsdump       - Tech Support Dump Menu
ospf         - OSPF Debug Menu
```

The Maintenance Menu is used for administering OSPF logs and technical support dumps, loading firewall policies, and testing the synchronization network between iSD hosts in a cluster. [Table 6-64](#) identifies command syntax and usage for the Maintenance Menu.

Table 6-64 Maintenance Menu (/maint)**Command Syntax and Usage**

diag

The Diagnostic Tools Menu opens the Firewall Maintenance Menu. For details see [page 213](#).

tsdump

The Tech(nical) Support Menu provides options for creating dump files with configuration or log information. For details see [page 214](#).

ospf

The OSPF Debug Menu provides options for logging OSPF events. For details see [page 215](#).

Diagnostics logs or stats can only be done at the request of Nortel Networks technical support.

/maint/diag

Diagnostic Tools Menu

```
[Diagnostic Tools Menu]
fw           - Firewall Maintenance Menu
```

The fw option opens the Firewall Maintenance Menu.

/maint/diag/fw

Firewall Maintenance Menu

```
[Firewall maintenance Menu]
sync         - Test sync network
ldplcy       - Load CheckPoint Policy
unldplcy     - Unload CheckPoint Policy
```

[Table 6-65](#) identifies command syntax and usage for the Firewall Maintenance Menu.

Table 6-65 Firewall Maintenance Menu (/maint/diag/fw) (Part 1 of 2)

Command Syntax and Usage

sync

This command tests the session state synchronization network for redundant iSDs in a cluster. Session state synchronization allows for stateful failover in the event that the active unit fails and the backup takes over. The VRRP features and the *virtual router* must also be configured before you can test the synchronization network (see the “[VRRP Interface Menu](#)” on page 187 and the “[VRRP Settings Menu](#)” on page 188).

Table 6-65 Firewall Maintenance Menu (/maint/diag/fw) (Part 2 of 2)**Command Syntax and Usage****ldpolicy**

This command is used to load the firewall policies that were previously downloaded from the Check Point SmartDashboard. If no policies were previously downloaded, the default firewall policy, i.e., no access, is applied.

unldpolicy

This command is used to unload the current firewall policies.

NOTE – Unloading the firewall policies allows all traffic to pass through the iSDs. Remember to push your firewall policies from the Check Point SmartDashboard after you have re-established trust.

/maint/tsdump

Tech Support Dump Menu

```
[Tech Support Menu]
dump          - Create a tech support dump
ftp           - FTP tech support dump to an FTP server
cur           - Current Tech Support Information
```

The Tech Support Dump Menu is for creating tech support dumps that you can load on an FTP server. [Table 6-66](#) identifies command syntax and usage for the Tech Support Dump Menu.

Table 6-66 Tech Support Dump Menu (maint/tsdump)**Command Syntax and Usage****dump**

Dumps the current configuration (no logs) to the default file *tsdump.tgz*. The file size is typically small (less than 1 Mbyte).

NOTE – The previous contents of the file are overwritten each time you use this command.

```
ftp <ftp server address> <remote directory> [<ftp username>] [<ftp password>]
```

Loads the dump file *tsdump.tgz* onto the specified ftp server at the specified directory. You must enter the username and password previously selected for the ftp server.

cur

Displays the dump file system data, that is, the file name, creation date, size.

/maint/ospf

OSPF Debug Menu

```
[OSPF Debug Menu]
events      - Set log OSPF generic events
ism         - Set log OSPF ISM events
lsa         - Set log OSPF LSA events
nsm         - Set log OSPF NSM events
packets     - Set log OSPF packets
msgs        - View last 100 debug messages
cur         - Display current settings
```

The OSPF Debug Menu is for administering the log of OSPF events. By enabling generic OSPF events or specific (ism, lsa, nsm, packets) OSPF events, you can create a log of OSPF event messages that provides a useful picture of OSPF activity. Below are typical OSPF event messages:

```
2003/04/18 19:20:51 OSPF: LSA[Refresh]:ospf_lsa_refresh_walker(): start
2003/04/18 19:20:51 OSPF: LSA[Refresh]: ospf_lsa_refresh_walker(): next index 236
2003/04/18 19:20:51 OSPF: LSA[Refresh]: ospf_lsa_refresh_walker(): refresh index 235
2003/04/18 19:20:51 OSPF: LSA[Refresh]: ospf_lsa_refresh_walker(): end
```

[Table 6-67](#) identifies command syntax and usage for the OSPF Debug Menu.

Table 6-67 OSPF Debug Menu (maint/tsdump) (Part 1 of 2)

Command Syntax and Usage

events n|y

Enables logging of generic OSPF events.

ism n|y

Enables logging of interface state machine (ism) events.

lsa n|y

Enables logging of link state advertisements (lsa).

nsm n|y

Enables logging of neighbor state machine (nsm) events.

packets n|y

Enables logging of OSPF packets.

Table 6-67 OSPF Debug Menu (maint/tsdump) (Part 2 of 2)

Command Syntax and Usage

msgs

Displays the last 100 messages from the log file.

cur

Displays the current settings in the OSPF Debug menu.



CHAPTER 7

Browser-Based Interface

This chapter explains how to use the Browser-Based Interface (BBI) to access firewall iSD system management features from your web browser.

NOTE – You can start an https session to the BBI from the Passport 8600 Series Switch JDM.

Features

The BBI provides the following features:

- Intuitive and easy-to-use interface structure
- Configuration and monitoring functions that are similar to those available through the CLI
- Easy access using HTTP, or secure HTTPS using Secure Socket Layer (SSL)
- Nothing to install — the BBI is part of the firewall iSD OS software and can be upgraded with future software releases, as available
- Up to ten BBI sessions can run simultaneously
- Online context-sensitive help for each BBI page

Getting started

Requirements

- 8660 SDM installed according to directions in *Installing the 8660 Service Delivery Module (SDM) for the Passport 8600 Series Switch* (part number 217314-A)
- A Check Point policy to allow management station access for HTTP or HTTPS traffic.
- PC or workstation with network access to the IP address of a firewall iSD host.
- Frame-capable web browser software, such as the following:
 - Netscape Navigator 4.6 or higher
 - Internet Explorer 5.0 or higher
- JavaScript enabled in your web browser

Enabling the Browser-Based Interface

Before you can access the BBI, some configuration must be performed at the CLI. For information on accessing and using the CLI, see [Chapter 2, “Initial setup,” on page 31](#). For detailed CLI menus, see also [Chapter 5, “The Command Line Interface,” on page 123](#).

1. Enable the BBI.

By default, the BBI is enabled for HTTP access, and disabled for HTTPS access. The BBI can be enabled for either HTTP access, HTTPS access, or both. The BBI can also be fully disabled.

NOTE – HTTP is not a secure protocol. All data (including passwords) between an HTTP client and the firewall iSDs is unencrypted and is subject to weak authentication. If secure remote access is required, consider using HTTPS instead of HTTP.

To explicitly allow remote BBI access, enter the following commands in the CLI.

- To enable HTTP access:

```
>> # /cfg/sys/adm/web/http/ena
```

- To enable HTTPS access using SSL:

```
>> # /cfg/sys/adm/web/ssl/ena
```

2. If using HTTPS, generate a temporary certificate.

An SSL server certificate is required for HTTPS access to the BBI. The firewall iSD can generate a temporary, self-signed certificate. The commands to create a default certificate are as follows:

```
>> SSL configuration# certs/serv/gen <Name> <Country code> <Key size>
Do you want to generate a self-signed certificate with the generated
Key? y
```

where *Name* is the common name that appears on the certificate, *Country code* is a two-letter code (US for the United States of America, CA for Canada, JP for Japan, and so on), and *Key size* is 512, 1024, or 2048 bits. For example:

```
>> SSL configuration# certs/serv/gen Alteon US 1024
```

NOTE – When you log in to the BBI with the temporary certificate, you will be warned that the certificate is not signed or authenticated. This should be permitted only during initial configuration, where the system is not attached to active networks that could be a source of attack. Install a signed and authenticated certificate prior to connecting an untrusted network.

3. Apply the changes.

```
>> SSL configuration# apply
```

4. Use the access list to permit remote access to trusted clients.

If you have already configured the access list for Telnet or SSH, there is no need to repeat the process. Otherwise, to permit access to only trusted clients, see [“Access List Menu” on page 154](#).

5. Use the Check Point SmartDashboard on your SMART Client to add a security policy that allows BBI traffic.

The firewall policy should be constructed as follows:

- Source: The IP address of the SMART Client or IP address range of the management network
- Destination: The host IP address of the firewall iSD
- Service: HTTP for non-secure access, or SSL for HTTPS access
- Action: Allow firewall iSD

Setting up the web browser

Most web browsers have JavaScript enabled by default and require no additional configuration. However, it is advisable to ensure that JavaScript is enabled on your web browser before using the BBI.

NOTE – JavaScript is not the same as Java. Ensure that JavaScript is enabled in your web browser.

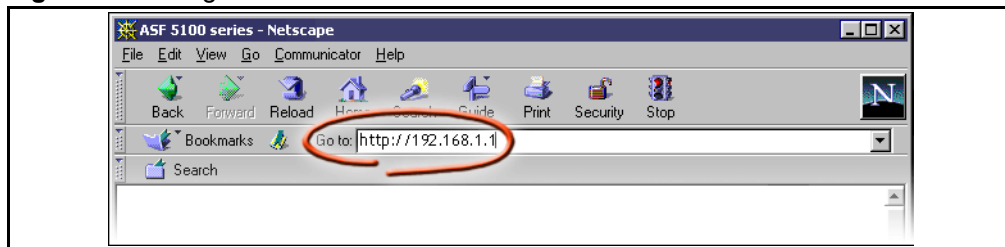
Starting the Browser-Based Interface

When the firewall iSD and browser setup is done, follow these steps to launch the BBI:

1. Start your web browser.
2. Enter the firewall iSD host IP address in the URL field of the web browser.

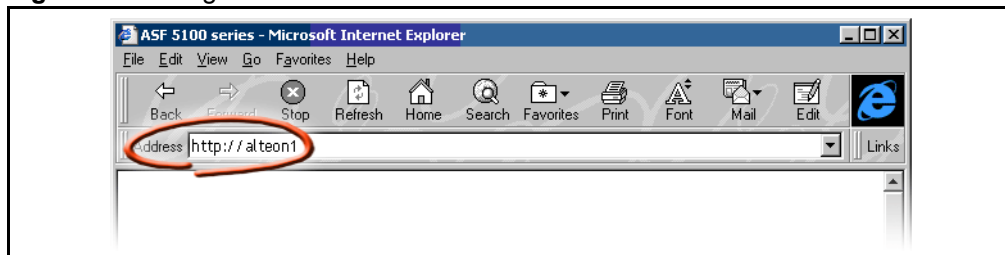
Figure 7-1 shows a host IP address of 192.168.1.1 entered in the Netscape Navigator URL field.

Figure 7-1 Using the firewall iSD host IP address



If the host IP address has a name on your local domain name server, you can enter that name instead. For example, see Figure 7-2.

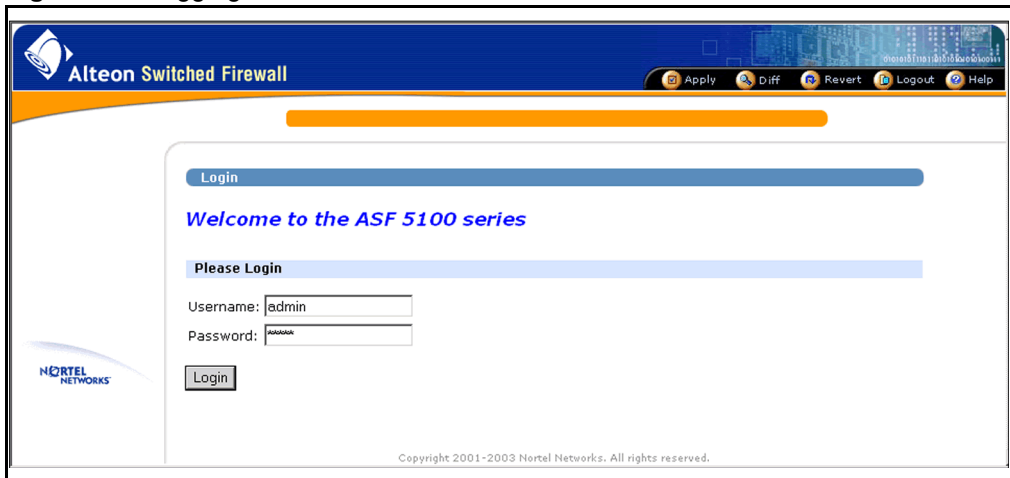
Figure 7-2 Using the firewall iSD host name



3. Log in.

If your firewall iSD host and browser are properly configured, you will be asked to enter a password. See [Figure 7-3](#).

Figure 7-3 Logging in to the BBI

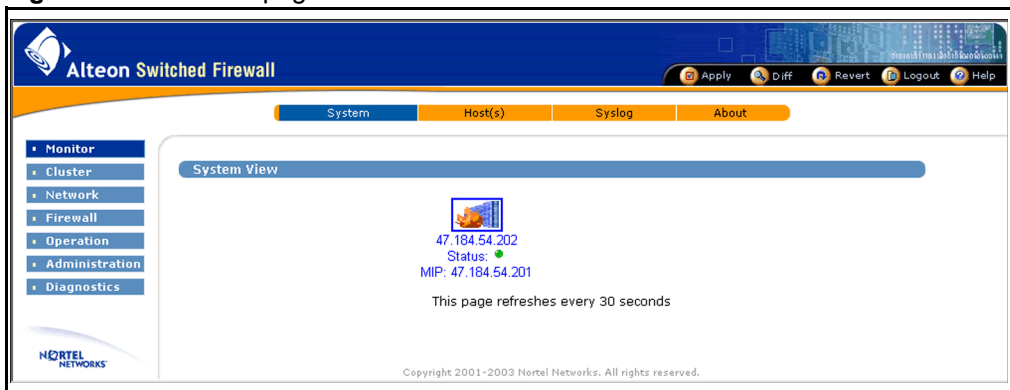


Enter the account name and password for the system administrator or operator account. For more login and password information, see [Chapter 4, “System management basics,”](#) on page 119.

4. Allow the main page to load.

If you enter the proper account name and password combination, the BBI main page opens in the viewing window of your browser. See [Figure 7-4](#).

Figure 7-4 BBI main page



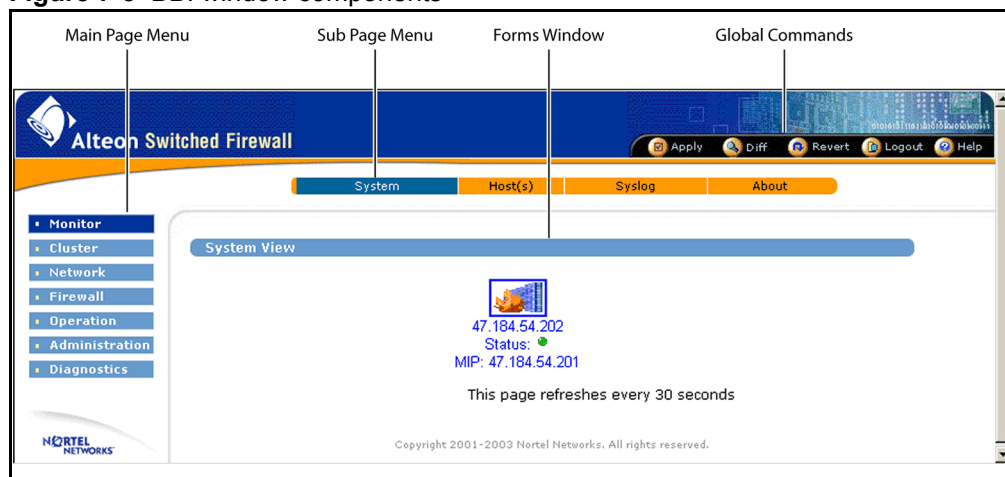
NOTE – There can be a few seconds delay while the default main page collects data. Do not stop the browser while loading is in progress.

Browser-Based Interface basics

Interface components

Figure 7-5 shows the main areas of the BBI window.

Figure 7-5 BBI window components



- **Main page menu**
The buttons in this area (Monitor, Cluster, and so on) represent the main categories of forms available for collecting information and configuring the system. Each main category contains a variety of sub-pages.
- **Sub-page menu**
These buttons represent the sub-categories under each main page. A different list of sub-pages is available for each main page. When a sub-page is selected, the appropriate information and configuration fields are displayed in the forms area.

The various pages are described in detail in [Chapter 8, “BBI forms reference,”](#) on page 233.

- Forms window

This area contains fields that display information or allow you to specify information for configuring the system. The fields are different for each sub-page.

- Global command buttons

These buttons are available from any page. The corresponding form displays when you click each button. Use these forms to save, examine or abort configuration changes, and to display help information for the current page.

Basic operation

NOTE – To access the full functionality of the BBI, you must log in as administrator.

NOTE – BBI sessions automatically close after five minutes of inactivity. This parameter cannot be changed.

Use the BBI to administer the firewall iSDs in the following manner:

- Select from a series of pages and sub-pages, and modify fields to create the desired configuration.
- Submit form changes using the appropriate Update buttons each time you finish making changes on a page.

If you select a new form or end the session without submitting the information, the changes are lost.

NOTE – Most submitted changes are considered pending and are not immediately put into effect, and are not permanently saved. The only changes that take effect as soon as the form is submitted are changes to users and passwords, and setting the time or time zone.

- Use the global **Apply** form to save changes and make them active. You can make updates on multiple forms, then make them all active simultaneously by clicking **Apply**. The **Apply** form validates the configuration changes before applying them. If the configuration changes contain invalid settings, the **Apply** command will fail.
- Use the global **Diff** form to view pending changes before they are applied.
- Use the global **Revert** form to clear pending changes. You can then either continue the configuration session, or log out.

- Use the global **Logout** form to exit from the system. Nortel Networks recommends that you log out using the **Logout** form; however, closing your browser manually or through inactivity will also discard pending changes.

See the “Global command forms” on page 224 for details on using Apply, Diff, Revert, Logout, and Help.

NOTE – Up to ten simultaneous browser connections are allowed. When multiple CLI or BBI administrator sessions are open at the same time, only pending changes made during your current session will be affected by the **Diff**, **Revert**, or **Logout** commands. However, if multiple CLI or BBI administrators apply changes to the same set of parameters concurrently, the latest applied changes take precedence.

Global command forms

The global command buttons are always available at the top of each form. See [Figure 7-6](#).

Figure 7-6 Global command buttons



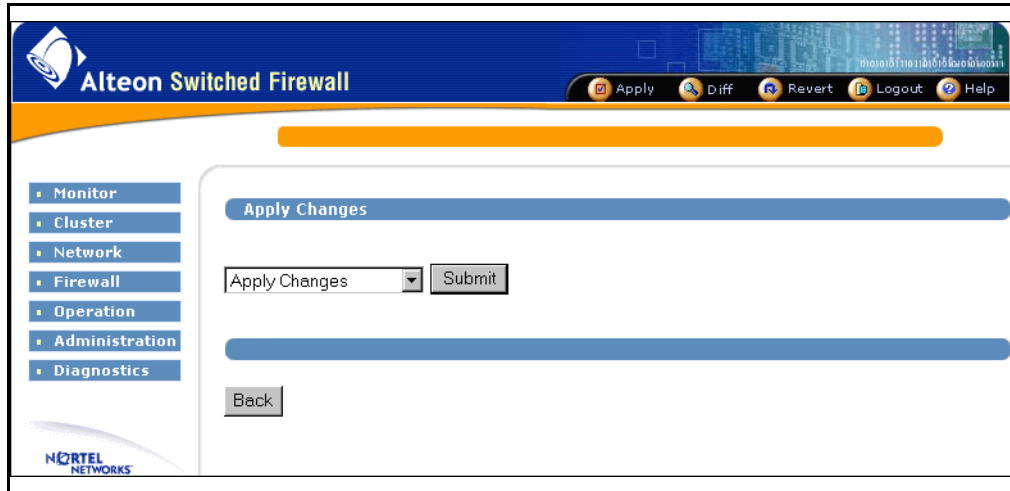
These buttons open pages that are used for logging out, saving, examining, or aborting configuration changes, and for displaying help information. Each global command page provides options to verify or cancel the command as appropriate.

Apply

Use the global **Apply** form to check the validity of the pending configuration changes for the current session, to save the configuration changes, and make configuration changes active.

[Figure 7-7](#) shows the **Apply Changes** form.

Figure 7-7 Apply Changes form



The global **Apply** form includes the following items:

- **Apply Changes** drop-down menu. To use this menu, select one of the following options, and click **Submit**:

- **Apply Changes**

When submitted, this action updates the firewall iSD with any pending configuration changes. Pending changes are first validated for correctness. If problems are found, applicable warning and error messages are displayed. If errors are found, the changes are not applied. If there are no errors (warnings are allowed), the changes are saved and made active.

This command has no effect on pending changes in other open CLI or BBI sessions.

NOTE – The global **Revert** command clears pending changes. It cannot be used to restore the old configuration after the **Apply Changes** command has been issued.

— **Validate Configuration**

When submitted, the pending changes of the current session are validated, but not applied. The pending configuration changes are examined to ensure that they are complete and consistent. If problems are found, the following types of messages are displayed:

- **Warnings** are in yellow. Warnings identify noteworthy conditions, but which will not cause errors or prevent the configuration from being applied.
- **Errors** are in red. Errors identify serious configuration problems that must be corrected before changes can be applied. Uncorrected errors will cause the **Apply Changes** command to fail.

If the configuration is valid, the administrator must still separately submit the **Apply Changes** command.

— **Run Security Audit**

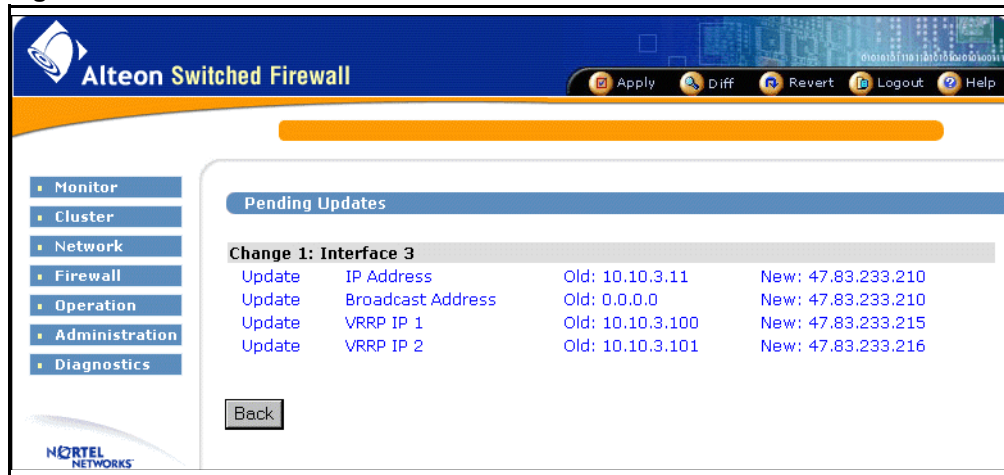
When submitted, **Run Security Audit** lists security information (for example, the status [enabled or disabled] for remote management tools such as Telnet, SSH, and the BBI for the cluster, as well as the IP addresses that can access them). It also lists the users (if any) who are still configured with default passwords. Nortel Networks recommends that you change all default passwords and make each unique.

- **Submit** button: This button performs the action selected in the **Apply Changes** drop-down menu.
- **Back** button: This button returns the previously viewed form without applying changes.

Diff

The global **Diff** form provides a list of the pending configuration changes for the current session. [Figure 7-8](#) shows the **Diff** form.

Figure 7-8 Diff form



The list displays a change record for each submitted update. Each record can consist of many modifications, depending upon the complexity of the form and the changes submitted. Modifications are color-coded as follows:

- **Green:** New items that will be added to the configuration when the global **Apply** command is submitted and verified.
- **Blue:** Existing items that will be modified.
- **Red:** Configuration items that will be deleted.

The **Diff** list is cleared when configuration changes are applied or reverted, or when you log out or close the browser window.

NOTE – The list generated on the **Diff** form does not include pending changes made in other concurrent CLI or BBI sessions.

Revert

Use the global **Revert** form to cancel pending configuration changes. [Figure 7-9](#) shows the **Revert** form.

Figure 7-9 Revert form



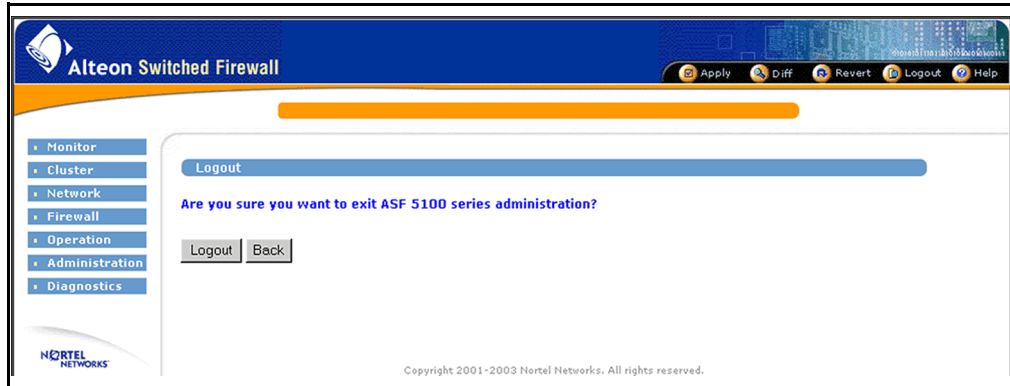
The **Revert** form includes the following items:

- **Revert Changes** button: This button cancels the pending configuration changes of the current session. Applied changes are not affected, nor are pending changes made in other open CLI or BBI sessions are not affected.
- **Back** button: This button returns the previously viewed form without cancelling pending changes.

Logout

Use the global **Logout** form to terminate the current user session. [Figure 7-10](#) shows the **Logout** form.

Figure 7-10 Logout form



The **Logout** form includes the following items:

- **Logout** button: This button terminates the current user session. Any configuration changes made during this session, and that you have not yet applied, will be lost. This command has no effect on pending changes in other open CLI or BBI sessions.
- **Back** button: This button returns to the previously viewed form without logging out.

NOTE – For thorough security, close all BBI windows (including help) after logging out.

Help

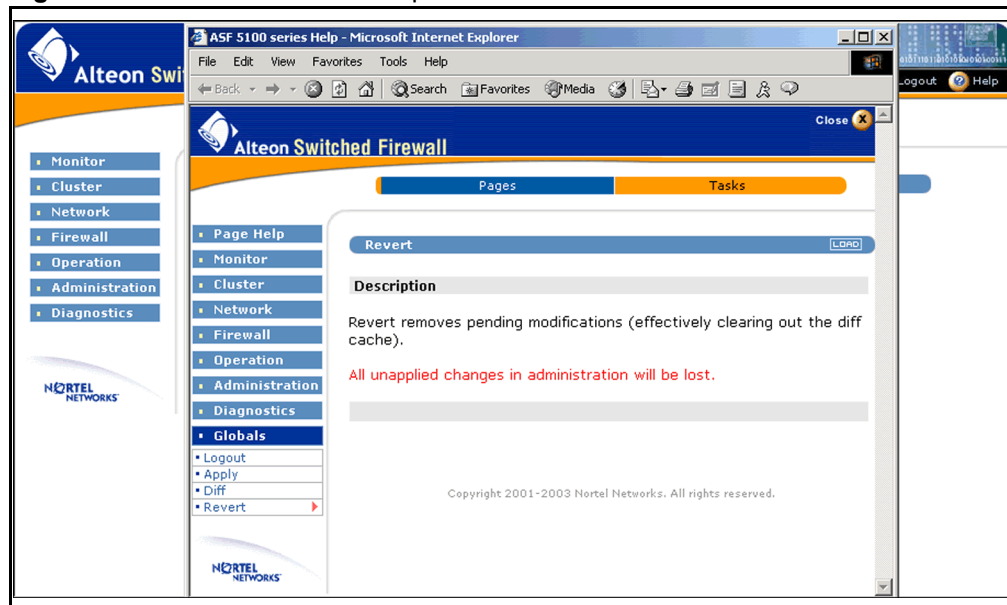
The global **Help** form provides assistance with forms and tasks in the BBI. There are two kinds of help:

- context-sensitive help
- task-based help.

Context-sensitive help

Context-sensitive help displays detailed information about the form that is currently displayed in the BBI forms area. When you click the global **Help** button, a new window appears with help information appropriate to your current options. [Figure 7-11](#) shows an example of the context-sensitive help.

Figure 7-11 Context-sensitive help form



The context-sensitive help window consists of the following areas:

- Sub-page menu: Click **Pages** to display help for the selected form. Click **Tasks** to activate the task-based help system.
- Help topic menu: Select a new help topic using the menu on the left side of the **Help** window. Each main menu item is listed, as well as sub-menu items under the current selection. Select a different menu item to display its sub-menu list. Select any sub-menu item to display help for the relevant form.

- **Load:** Click **Load** to display the form (**Revert** in the example) referenced on the bar.
- **Forms area:** Displays detailed information about the selected topic.
- **Close button:** Closes the context-sensitive help window.

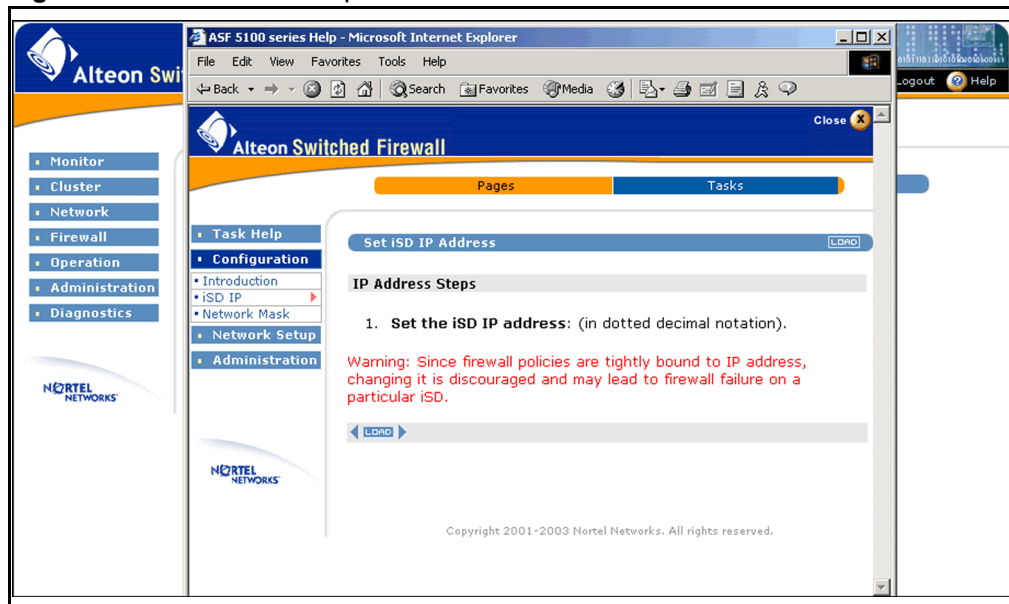
Task-based help

Task-based help leads the administrator through the steps of common procedures. To access task-based help:

1. Click the **global Help button**.
2. Click **Tasks** from the bar at the top of the page (see [Figure 7-12](#)).
3. Select the task for which you require additional information.

Tasks appear in a list on the left side of the page. The task help menu will be displayed in a new window with information appropriate to the current BBI form.

Figure 7-12 Task-based help form



The task-based help form consists of the following areas:

- **Sub-page menu:** Click on **Pages** to display help for the selected form. Click on **Tasks** to activate the task-based help system.

- Task topic menu: You can select from a list of tasks using the menu on the left side of the help window. Each main task item is listed, along with the sub-tasks under the current selection. Select a different sub-task to reveal the steps required to complete it.
- Forms area: Displays the step or steps required to complete the selected sub-task.
- ◀ (if appropriate): Displays the information for the previous sub-task.
- **Load**: Click **Load** to display the form referenced on the task topic menu (**iSD IP** in this example). If the sub-task has more than one step (as is common among the Network Setup tasks), the steps are enumerated on the form.
- ▶ (if appropriate): Displays the information for the next sub-task.
- **Close** button: Closes the task-based help window.



CHAPTER 8

BBI forms reference

Overview

This chapter describes each of the BBI forms. The forms are accessed by clicking a menu item from the left side of the BBI window. From the main page of each menu item, click a sub-page menu item to access all parameters available for that selected menu. See [“Interface components” on page 222](#) for more information on the BBI interface. The BBI menu items are the following:

- [“Monitor forms” on page 234](#)
- [“Cluster forms” on page 238](#)
- [“Network forms” on page 245](#)
- [“Firewall forms” on page 263](#)
- [“Operations forms” on page 268](#)
- [“Administration forms” on page 271](#)
- [“Diagnostics forms” on page 290](#)

Monitor forms

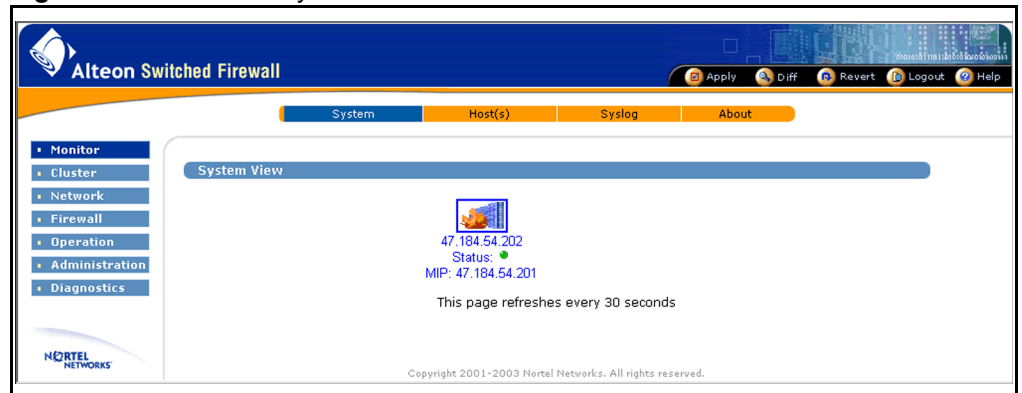
The Monitor sub-menu items are the following:

- “Monitor > System” on page 234
- “Monitor > Hosts” on page 235
- “Monitor > Syslog” on page 236
- “Monitor > About” on page 237

Monitor > System

Figure 8-1 shows the default Monitor form. It provides a summary status view of the cluster.

Figure 8-1 Monitor > System form



The firewall iSD icon is shown along with its individual host IP address and the MIP address.

A Green icon for **Status:** indicates the firewall iSD is up. A Red icon for **Status:** indicates the firewall iSD is down.

To obtain more information about a firewall iSD, click on the device icon (see “Monitor > Hosts” on page 235).

Monitor > Hosts

Figure 8-2 shows the **Monitor > Hosts** form. It displays iSD host details and application status.

Figure 8-2 Monitor > Hosts form

Alteon Switched Firewall

System ISDs Syslog About

Monitor Cluster Network Firewall Operation Administration Diagnostics

Host Details

List of iSD Hosts:

Host: 47.184.54.202

Host Name: isd@a47-184-54-202
 Management IP: 47.184.54.201
 MAC Address: 00:02:B3:BC:AD:CE
 System Uptime: 100:58:31
 Hard Disk Usage: 36%
 Memory Usage: 70%
 CPU Load: 22%

Application	Current Status	Uptime
Firewall	Running	100:56:53
Web Server	Running	100:56:50
SNMP	Disabled	00:00:00

The **Monitor > Hosts** form contains the following information:

- List of iSD Hosts: The drop-down menu lets you choose one or the other host (by IP address) or both (ALL). The **Update** button refreshes the screen according to the changed host details request.
- Host Name: The name of the firewall iSD host.
- Management IP: The MIP address of the firewall iSD.
- MAC Address: The MAC address of the firewall iSD.
- System Uptime: The time since the last boot of the firewall iSD, in Hours:Minutes:Seconds.
- Hard Disk Usage: The percentage of hard disk space being utilized on the firewall iSD.
- Memory Usage: The percentage of memory being utilized on the firewall iSD.
- CPU Load: The percentage of CPU being utilized on the firewall iSD.
- Application: The current applications that are running on the firewall iSD.
- Current Status: The current status of the application: running or disabled.

- Uptime: The time since the application started, in Hours:Minutes:Seconds.
- **Beep Host** button: Emits a beep at the specified host to identify it.

Monitor > Syslog

Figure 8-3 shows the **Monitor > Syslog** form. It displays the system logs of the firewall iSD based on your choice of search criteria.

Figure 8-3 Monitor > Syslog form

The screenshot shows the 'Monitor > Syslog' form in the Alteon Switched Firewall interface. The form is titled 'Syslog Messages' and contains the following elements:

- Host IP:** A dropdown menu showing '47.184.54.202'.
- Search String:** A text input field containing 'NOTICE' and a 'Quick Choice' dropdown menu.
- Messages Per Page:** A text input field containing '20'.
- Case Sensitive:** A checkbox that is currently unchecked.
- Note:** A small text note stating: 'Note: An empty search string displays the more recent messages. Search may take a while depending on syslog size and work load on system.'
- Search Button:** A button labeled 'Search'.
- Log Messages:** A list of log entries displayed in a table-like format:

May 19 23:50:51 a47-184-54-202 snmpagentd:	NOTICE: The SNMP subagent is starting.
May 19 23:50:49 a47-184-54-202 elalogd[1070]:	NOTICE: ELA logging daemon started.
May 16 09:17:49 localhost snmpagentd:	NOTICE: The SNMP subagent is starting.
May 16 09:17:48 localhost elalogd[2208]:	NOTICE: ELA logging daemon started.

The **Monitor > Syslog** form contains the following information:

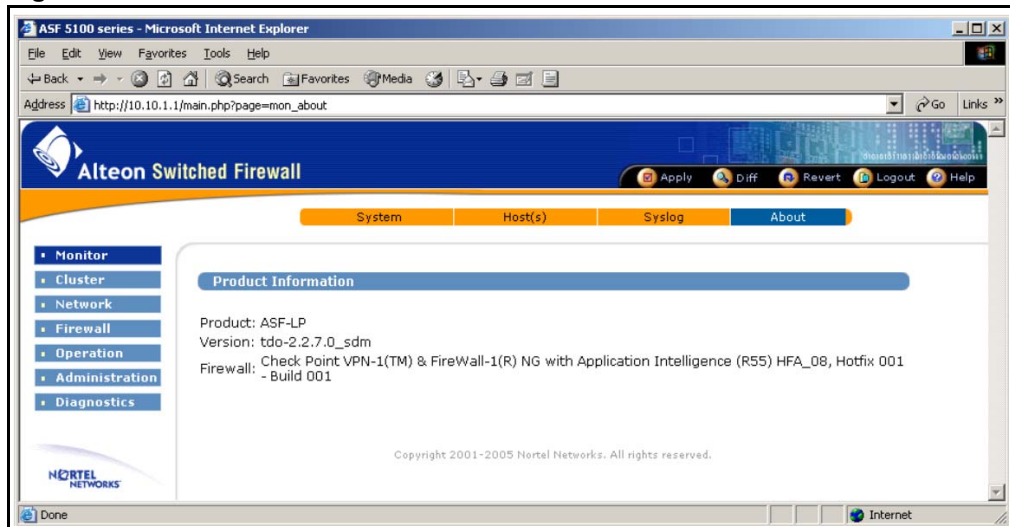
- **Host IP:** IP address of the firewall iSD from which to view logs.
- **Search String:** Search for this string in the message body. All messages that have a substring matching the characters in this field will be displayed when the **Search** button is selected.
- **Quick Choice** drop-down menu: Provides a predefined list of basic search strings. Select one of the following choices:
 - All critical messages (CRITICAL)
 - All error messages (ERROR)
 - All info messages (INFO)
 - All notice messages (NOTICE)
 - All warning messages (WARNING)
- **Messages Per Page:** Maximum number of messages displayed for each request.

- **Case Sensitive:** Check this box to make the search criteria case-sensitive. If unchecked, the capitalization of characters in the search string and message body is disregarded.
- **Search Button:** Execute the log search using the parameters defined on this form. When the search completes, it produces a list of messages at the bottom of the form that matches the search criterion.

Monitor > About

Figure 8-4 shows the **Monitor > About** form. It displays general product information about the host, including the model name, software version, and Check Point product and Feature Pack version.

Figure 8-4 Monitor > About form



The **Monitor > About** form contains the following information:

- **Product:** The model number of the cluster to which the BBI is connected.
- **Version:** The software version running on the cluster.
- **Firewall:** The Check Point software build and feature pack running on the cluster.

Cluster forms

The Cluster sub-menu items are the following:

- “Cluster > Time” on page 238
- “Cluster > iSDs” on page 239
- “Cluster > Logs > Syslog” on page 240
- “Cluster > Logs > ELA” on page 241
- “Cluster > Logs > Archive” on page 243
- “Cluster > Miscellaneous” on page 244

Cluster > Time

Figure 8-5 shows the **Cluster > Time** form. Use this form to set the date and time for the cluster.

Figure 8-5 Cluster > Time form

The **Cluster > Time** form contains the following information:

- **Current Time:** Displays the current system time. This field cannot be edited.
- **Date section:** Use these fields to set new date and time. Specified by month, day, year, hour, and minute.

- **Save** button: Submits the date changes to the pending configuration.
- **Timezone**: Select your region from the drop-down list.
- **Save** button: Submits the time zone change to the pending configuration.

Cluster > iSDs

Figure 8-6 shows the **Cluster > iSDs** form. It displays the cluster member IP interface settings.

Figure 8-6 Cluster > iSDs form

The screenshot displays the Alteon Switched Firewall web interface. At the top, there is a blue header with the Alteon logo and the text 'Alteon Switched Firewall'. To the right of the header are buttons for 'Apply', 'Diff', 'Revert', 'Logout', and 'Help'. Below the header is a navigation bar with tabs for 'Time', 'ISD(s)', 'Logs', and 'Miscellaneous'. The 'ISD(s)' tab is selected. On the left side, there is a vertical navigation menu with buttons for 'Monitor', 'Cluster', 'Network', 'Firewall', 'Operation', 'Administration', and 'Diagnostics'. The 'Cluster' button is highlighted. The main content area shows 'iSD Management' with a 'Management IP Address' field containing 'MIP: 47.184.54.201'. Below this is a 'General Settings: iSD 1' section with a list of hosts. The first host has the following details: Name: 'isd@a47-184-54-202' with a 'Delete' button next to it; IP: '47.184.54.202'; Netmask: '255.255.255.0'; and Port: '1'. At the bottom of the page, there is a copyright notice: 'Copyright 2001-2003 Nortel Networks. All rights reserved.'

The **Cluster > iSDs** form contains the following information:

- **MIP**: Displays the Management IP (MIP) address for the cluster.
- **Name**: Displays the internal name of the host.
- **Delete** button: Deletes the host and resets it to factory default configuration settings.
- **IP**: Displays the network IP address for the host.
- **Netmask**: Displays the network mask for the host in dotted decimal notation.
- **Port**: Displays the host management port number.

Cluster > Logs > Syslog

Figure 8-7 shows the **Cluster > Logs > Syslog** form. Use this form to specify remote system log daemons and turn on local log debugging.

Figure 8-7 Cluster > Logs > Syslog form

The screenshot shows the Alteon Switched Firewall web interface. The top navigation bar includes buttons for Apply, Diff, Revert, Logout, and Help. The main content area is titled "Cluster > Logs > Syslog" and contains the following sections:

- General:**
 - Debug Messages:
 - Source IP Mode:
 -
- Remote Servers:**
 - Current Remote Servers:**

IP Address	Logging Severity
No remote syslog servers configured.	
 - Add New Remote Server:**
 - New Server IP: (format: 10.10.1.75)
 - New Server Severity:
 -

The **Cluster > Logs > Syslog** form contains the following information:

- **Debug Messages:** Enables or Disables sending debug messages to the local system log.
- **Source IP Mode:** Configures which source IP address will be used with logs generated by the cluster.
 - Auto: The IP address of the outgoing interface is used (default).
 - Unique: The IP address of the individual firewall iSD is used.
 - MIP: The IP address of the cluster MIP is used. This setting is useful with applications (such as some versions of HP OpenView) that expect devices to be limited to only one IP address.
- **Update** button: Submits the debug message status change and the source IP mode change to the pending configuration.
- **IP Address:** IP address for the remote syslog server in dotted decimal notation.

- **Logging Severity:** Severity of messages logged. All messages of the selected severity and higher will be logged.
- **Delete button:** Deletes a remote server. This button is only present if a remote server is active.
- **New Server IP:** IP address for the remote syslog server in dotted decimal notation.
- **New Server Severity:** Severity of messages logged. All messages of the selected severity and higher will be logged.
- **Update button:** Submits the remote server changes to the pending configuration.

Cluster > Logs > ELA

Figure 8-8 on page 242 shows the **Cluster > Logs > ELA** form. Use this form to configure Event Logging API (ELA). ELA allows firewall iSD log messages to be sent to a Check Point SmartCenter Server for display through the Check Point SmartView Tracker.

NOTE – An ELA service must be configured on the Check Point Management Station, and a SIC Certificate for the service must be transferred to the firewall iSD before ELA logging can commence. For configuration details, see Chapter 12, “Event Logging API,” on page 349.

Figure 8-8 Cluster > Logs > ELA form

The screenshot shows the Alteon Switched Firewall web interface. The top navigation bar includes 'Apply', 'Diff', 'Revert', 'Logout', and 'Help'. The main menu on the left lists 'Monitor', 'Cluster', 'Network', 'Firewall', 'Operation', 'Administration', and 'Diagnostics'. The 'Cluster' menu is expanded, showing 'Time', 'ISD(s)', 'Logs', and 'Miscellaneous'. Under 'Logs', 'Syslog', 'ELA', and 'Archive' are visible. The 'ELA Log' page is displayed, featuring a 'General Settings' section with the following fields: Status (disabled), Management Station IP (0.0.0.0), Minimum Severity (err), and Management Station DN. Below this is an 'Update' button. The 'Pull SIC Certificate' section includes ISD IP (47.184.54.202), OPSEC Application Name, OPSEC Password, and OPSEC Password (again), with a 'Submit' button. A note at the bottom reads: 'Note: The certificate will need to be pulled again if the SIC status of the OPSEC application is reset.'

The **Cluster > Logs > ELA** form contains the following information:

- **Status:** Enables or Disables Check Point ELA logging.
- **Management Station IP:** The IP address of the Check Point SmartCenter Server to which the firewall iSD log messages will be sent.
- **Minimum Severity:** Severity of messages logged. All messages of the selected severity and higher will be sent to the ELA service.
- **Management Station DN:** Distinguished name of the Check Point SmartCenter Server.
- **Update** button: Submits the form changes to the pending configuration.

NOTE – The Management Station IP and Server DN must be configured and saved before updating the SIC certificate. If these values change, then a new certificate will need to be created.

- **iSD IP:** The IP address of the individual firewall iSD being updated (do not use the MIP address).

- OPSEC™ Application Name: Name of the ELA service that was configured on the Check Point SmartCenter Server. Use the same name specified when creating the OPSEC application in the Check Point SmartDashboard. Each firewall iSD should use a different OPSEC application.
- OPSEC Password: Password used to configure the above ELA service on the Check Point management station.
- OPSEC Password (again): Verify the password.
- **Submit** button: Submit the form and update the certificate on the specified firewall iSD.

Cluster > Logs > Archive

Figure 8-9 shows the **Cluster > Logs > Archive** form. Use this form to specify system log rotation/archiving parameters.

Figure 8-9 Cluster > Logs > Archive form

The screenshot shows the Alteon Switched Firewall web interface. The breadcrumb trail at the top reads: Time > ISD(s) > Logs > Miscellaneous > Syslog > ELA > Archive. The main content area is titled "Log Archiving" and contains the following fields:

- Email:
- SMTP Server IP:
- Rotate Size: (kb)
- Interval: Days: Hours:

An "Update" button is located below the interval fields. The left navigation menu includes: Monitor, Cluster, Network, Firewall, Operation, Administration, and Diagnostics. The Nortel Networks logo is visible in the bottom left corner.

Log files can be rotated when the file reaches a specific size or age. When rotation occurs, the rotated log file is set aside or e-mailed to a specified address and a new log file begins.

If the rotate size is set above 0, then log rotation occurs when the log surpasses the rotate size, or when the log rotation interval is reached, whichever occurs first. If the rotate size is set to 0, the file size is ignored and only the rotate interval is used. If an e-mail address and SMTP Server IP are set, then the log file is mailed when rotated.

The **Cluster > Logs > Archive** form contains the following information:

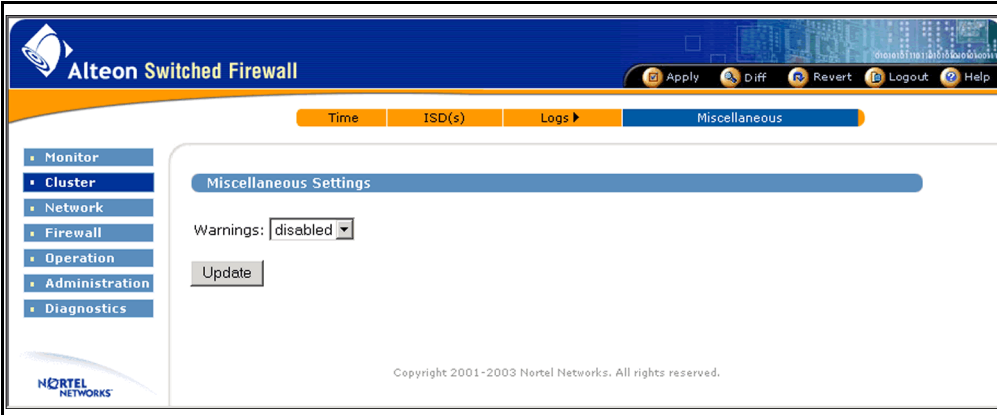
- E-mail: E-mail address of the administrator who will receive the log.

- SMTP Server IP: IP address of the SMTP server in dotted decimal notation. Note that this server must be configured to accept messages from the firewall iSD. Also, a Check Point policy should be present to allow these messages through the firewall.
- Rotate Size: Maximum size the log should reach before rotation. If 0, then the size is ignored and only the log rotate interval is used.
- Interval: The interval at which the system log file should be rotated, specified in days and hours.
- **Save Settings** button: Submits the form changes to the pending configuration.

Cluster > Miscellaneous

Figure 8-10 shows the **Cluster > Miscellaneous** form. Use this form to enable or disable configuration warning messages.

Figure 8-10 Cluster > Miscellaneous form



The **Cluster > Miscellaneous** form contains the following information:

- Warnings: Enables or Disables the display of warning messages that indicate the state of pending configuration changes when the global `apply` command is issued.
- **Update** button: Submits the Warning change to the pending configuration.

Network forms

The Network sub-menu items are the following:

- “Network > DNS” on page 246
- “Network > NTP” on page 247
- “Network > Ports” on page 248
 - “Network > Ports > Update (Add or Modify)” on page 249
- “Network > Interfaces” on page 250
 - “Network > Interfaces > Update (Add or Modify)” on page 251
- “Network > VRRP” on page 252
- “Network > Gateway” on page 254
- “Network > Routes > Static” on page 254
 - “Network > Routes > Static > Update (Add, Delete, or Modify)” on page 255
- “Network > Routes > Proxy ARP” on page 256
- “Network > Routes > OSPF > General” on page 257
- “Network > Routes > OSPF > Area Index” on page 258
 - “Network > Routes > OSPF > Area Index > Update (Add or Modify)” on page 259
- “Network > Routes > OSPF > Interface” on page 260
 - “Network > Routes > OSPF > Interface > Update (Modify)” on page 261

Network > DNS

Figure 8-11 shows the **Network > DNS** form. Use this form to specify the Domain Name Service (DNS) servers. Multiple servers are allowed.

Figure 8-11 Network > DNS form

The screenshot shows the 'DNS Servers' configuration page in the Alteon Switched Firewall web interface. The page has a blue header with the Alteon logo and 'Alteon Switched Firewall' text. Below the header is a navigation bar with tabs for DNS, NTP, Ports, Interfaces, VRRP, Gateways, and Routes. On the left is a sidebar menu with options: Monitor, Cluster, Network (selected), Firewall, Operation, Administration, and Diagnostics. The main content area is titled 'DNS Servers' and contains a table with the following data:

IP Address	Action
47.184.54.1	Delete

Below the table, there is a 'New DNS IP:' label followed by an input field and an 'Update' button. At the bottom of the page, there is a copyright notice: 'Copyright 2001-2003 Nortel Networks. All rights reserved.'

The **Network > DNS** form contains the following information:

- **IP Address:** Displays the IP address of a DNS server.
- **Delete Button:** Deletes the server. Only displayed if a DNS server is present.
- **New DNS IP:** Configure a new DNS server address using the dotted decimal notation.
- **Update button:** Submits the DNS server address changes to the pending configuration.

Network > NTP

Figure 8-12 shows the **Network > NTP** form. Use this form to specify the Network Time Protocol (NTP) servers.

Figure 8-12 Network > NTP form

The screenshot shows the Alteon Switched Firewall web interface. The main content area is titled "NTP Servers" and contains a table with the following data:

IP Address	Action
10.10.2.20	Delete

Below the table, there is a "New NTP IP:" label followed by an input field and an "Update" button. The interface also features a navigation menu on the left with options like Monitor, Cluster, Network, Firewall, Operation, Administration, and Diagnostics. The top navigation bar includes links for DNS, NTP, Ports, Interfaces, VRRP, Gateways, and Routes. The footer contains the Nortel Networks logo and copyright information: "Copyright 2001-2003 Nortel Networks. All rights reserved."

NTP servers are used by the NTP client on the firewall iSD to synchronize its clock. The system should have access to a number of servers (at least three) to compensate for discrepancies between the servers.

The **Network > NTP** form contains the following information:

- **IP Address:** Displays the IP address of an NTP server.
- **Delete Button:** Deletes the server. Only displayed if NTP server is present.
- **New NTP IP:** Configure a new NTP server using the dotted decimal notation.
- **Update button:** Submits the NTP server address changes to the pending configuration.

Network > Ports

Figure 8-13 shows the **Network > Ports** form. Use this form to configure network port settings.

Figure 8-13 Network > Ports form

Port#	Name	Autonegotiation	Speed	Mode	
1	Host Port	Yes	0	full	Modify
2	none	Yes	0	full	Modify
3	none	Yes	0	full	Modify

Add New Port

The **Network > Ports** form contains the following information:

- **Port#:** The port number on the firewall iSD.
- **Name:** The name for the port.
- **Autonegotiation:** On (autonegotiation is enabled) or Off (autonegotiation is disabled).
- **Speed:** The port data rate: 0, 10, 100, and 1000 options.
- **Duplex mode.** half or full.
- **Modify** button: Modify a displayed port. See the **Update** form on [page 249](#).
- **Add New Port** button: Add and configure a new port. See the **Update** form on [page 249](#).

Network > Ports > Update (Add or Modify)

Figure 8-14 shows the **Network > Ports > Update** form. Use this form to update network port settings.

Figure 8-14 Network > Ports > Update form

The screenshot displays the Alteon Switched Firewall web interface. The top navigation bar includes 'DNS', 'NTP', 'Ports', 'Interfaces', 'VRRP', 'Gateways', and 'Routes'. The 'Ports' tab is selected. On the left, a sidebar menu lists 'Monitor', 'Cluster', 'Network', 'Firewall', 'Operation', 'Administration', and 'Diagnostics'. The main content area is titled 'Add Port' and contains a 'General Settings' section with the following fields:

- Identifier: 5
- Name: (empty text box)
- Autonegotiation Status: enabled
- Speed: 0
- Mode: full

At the bottom of the form are 'Update' and 'Back' buttons.

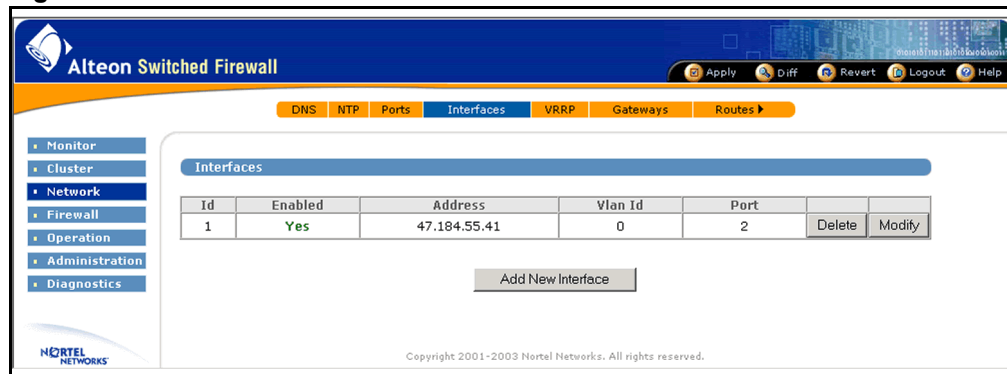
The **Network > Ports > Update** form contains the following information:

- **Identifier:** The port number on the firewall iSD.
- **Name:** Specify a name for the port.
- **Autonegotiation Status:** Enables/disables autonegotiation on the port.
- **Speed:** Sets the link speed. The choices include: 0, 10, 100, or 1000 Mbps.
- **Mode:** Sets the duplex operating mode. The choices are full (full-duplex) or half (half-duplex).
- **Update** button: Submits the changes to the pending configuration.
- **Back** button: Returns to the previously viewed form without saving changes to this form.

Network > Interfaces

Figure 8-15 shows the **Network > Interfaces** form. Use this form to view and configure the settings for individual interfaces.

Figure 8-15 Network > Interfaces form



The firewall iSD can be configured with up to 255 IP interfaces, each representing the firewall iSD on an IP subnet.

The **Network > Interfaces** form contains the following information:

- **Id**: Numerical ID for the interface (between 1 and 255). It can be used to specify the interface when configuring a new route.
- **Enabled**: Indicates whether the interface is enabled or disabled.
- **Address**: The IP address of the interface using the dotted decimal notation.
- **Vlan Id**: The numerical ID for a VLAN on this interface.
- **Port**: Associates the interface with a single port.
- **Delete** button: Delete an interface from the system. Only visible if interfaces are present.
- **Modify** button: Modify a displayed interface. Only visible if interfaces are present. See the **Update** form on [page 251](#).
- **Add New Interface** button: Adds a new interface to the configuration. See the **Update** form on [page 251](#).

Network > Interfaces > Update (Add or Modify)

Figure 8-16 shows the **Network > Interfaces > Update** form. Use this form to update interface settings.

Figure 8-16 Network > Interfaces > Update form

The screenshot displays the 'Add Interface' configuration page in the Alteon Switched Firewall web interface. The page has a blue header with the Alteon logo and navigation buttons (Apply, Diff, Revert, Logout, Help). Below the header is a navigation bar with tabs for DNS, NTP, Ports, Interfaces (selected), VRRP, Gateways, and Routes. On the left is a vertical menu with options: Monitor, Cluster, Network (selected), Firewall, Operation, Administration, and Diagnostics. The main content area is titled 'Add Interface' and contains two sections: 'General Settings' and 'Vrrp Settings'. The 'General Settings' section includes: Identifier (dropdown: 1), Status (dropdown: disabled), IP Address (text: 0.0.0.0, format: 10.10.1.75), IP Address2 (text: 0.0.0.0, format: 10.10.1.76), Subnet Mask (text: 0.0.0.0), Vlan Id (dropdown: 0), and Port (dropdown: 1). The 'Vrrp Settings' section includes: Vrid (dropdown: 1), Ip1 (text: 0.0.0.0, format: 10.10.1.73), and Ip2 (text: 0.0.0.0, format: 10.10.1.74). At the bottom are 'Save Interface' and 'Back' buttons.

The **Network > Interfaces > Update** form contains the following information:

- Identifier: Numerical ID for the interface (between 1 and 255). It can be used to specify the interface when configuring a new route.
- Status: Enables or disables the interface.
- IP Address: Configures the IP address of the interface using the dotted decimal notation.
- IP Address2: Configures the second IP address of the interface using dotted decimal notation. This address should not be configured unless the interface is part of a VRRP active-active network configuration. Active-active network configuration is not supported in software release 2.2.7.0.
- Subnet Mask: Configures the IP subnet address of the interface using the dotted decimal notation.
- Vlan Id: Numerical ID for the VLAN (between 0 and 4094).
- Port: Associates the interface with a single port.

- Vrid: Numerical ID for the Virtual Router on this interface.
- Ip1: Configures the IP sub-address representing iSD host 1 using dotted decimal notation.
- Ip2: Configures the IP sub-address representing iSD host 2 using dotted decimal notation.
- **Save Interface** button: Submits the form changes to the pending configuration.
- **Back** button: Returns to the previously viewed form without saving changes to this form.

Network > VRRP

Figure 8-17 shows the **Network > VRRP** form. Use this form to view and configure the VRRP parameters for the cluster.

Figure 8-17 Network > VRRP form

The screenshot shows the 'VRRP Settings' form in the Alteon Switched Firewall web interface. The form is titled 'VRRP Settings' and is part of the 'Network > VRRP' configuration page. The page header includes 'Alteon Switched Firewall' and navigation tabs for DNS, NTP, Ports, Interfaces, VRRP, Gateways, and Routes. A sidebar on the left contains menu items: Monitor, Cluster, Network, Firewall, Operation, Administration, and Diagnostics. The VRRP Settings form contains the following fields:

High Availability:	disabled
Active Active:	disabled
ClusterXL:	disabled
Advertisement Interval:	3
Garp Broadcast Interval:	2
Garp Delay Interval:	1
Port HealthCheck Interval:	2
Advance FailOver Check:	enabled

An 'Update' button is located at the bottom of the form.

The **Network > VRRP** form contains the following information:

- High Availability: Enables high availability VRRP.
- Active Active: Enables active-active VRRP. Active-active network configuration is not supported in software release 2.2.7.0.

NOTE – Only one of these VRRP settings can be enabled at a time. You cannot apply the enable setting for any of them unless there are two iSD hosts in the cluster.

- ClusterXL: Enables ClusterXL VRRP. ClusterXL configuration is not supported in software release 2.2.7.0.

NOTE – Do not attempt to implement ClusterXL with Release 2.2.7.0 software.

- Advertisement Interval: Sets the interval in seconds between advertisement messages (between 3 and 3600).
- GARP Broadcast Interval: Sets the value that, when multiplied by the Advertisement Interval, determines the interval between Gratuitous ARP (GARP) messages (between 2 and 100).
- GARP Delay Interval: This field displays the current Gratuitous Address Resolution Protocol (GARP) Delay Interval in seconds and allows you to set it. The delay interval is the period of time the backup iSD host waits after sending a flash GARP message (an unsolicited ARP response) to all end hosts on the virtual router interface before it begins sending continuous GARP messages. The flash GARP message forces end hosts to update their ARP caches with the MAC address/IP address mapping for the newly active iSD host, instead of waiting for end hosts to learn it through periodic ARP requests. The default value is 1 and the range is between 1 and 600.
- Port HealthCheck Interval: Sets the interval between port health checks that determine if a link on the port interface is up or down. The default value is 2 and the range is 2 - 3600.
- Advanced Failover Check: This command enables or disables Advanced Failover Checking (AFC). When AFC is enabled, the system ARPs before initiating a failover caused by missed VRRP advertisements.

Network > Gateway

Figure 8-18 shows the **Network > Gateway** form. Use this form to specify the default gateway for the Firewall.

Figure 8-18 Network > Gateway form



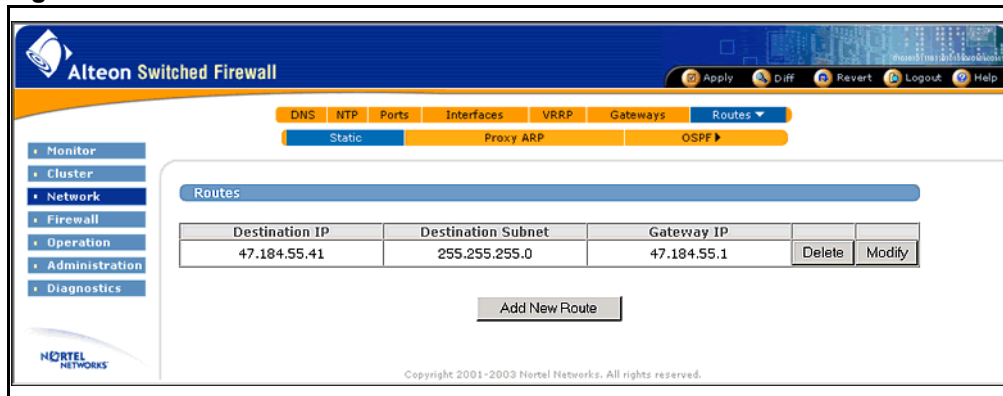
The **Network > Gateway** form contains the following information:

- Gateway: Configure the gateway for the system using dotted decimal notation.
- Update button: Submits the form changes to the pending configuration.

Network > Routes > Static

Figure 8-19 shows the **Network > Routes > Static** form. Use this form to view and configure static routes on the firewall iSD.

Figure 8-19 Network > Routes > Static form



The **Network > Routes > Static** form contains the following information:

- Destination IP: IP address of the route destination in dotted decimal notation.
- Destination Subnet: Subnet mask for the route destination in dotted decimal notation.
- Gateway IP: IP address of the gateway in dotted decimal notation.
- **Delete** button: Deletes a route from the system. Only visible if routes are present.
- **Modify** button: Modifies a displayed route. Only visible if routes are present. See the Update form on [page 255](#).
- **Add New Route** button: Adds a route to the configuration. See the Update form on [page 255](#).

Network > Routes > Static > Update (Add, Delete, or Modify)

[Figure 8-20](#) shows the **Network > Routes > Static > Update** form. Use this form to update static routes on the firewall iSD.

Figure 8-20 Network > Routes > Static > Update form

The screenshot displays the Alteon Switched Firewall configuration page. The top navigation bar includes 'Apply', 'Diff', 'Revert', 'Logout', and 'Help'. The main menu on the left lists 'Monitor', 'Cluster', 'Network', 'Firewall', 'Operation', 'Administration', and 'Diagnostics'. The central navigation tabs are 'DNS', 'NTP', 'Ports', 'Interfaces', 'VRRP', 'Gateways', and 'Routes'. Under 'Routes', there are sub-tabs for 'Static', 'Proxy ARP', and 'OSPF'. The 'Static' sub-tab is active, showing a 'Routes' table with one entry. Below the table are input fields for 'Destination IP' (47.184.55.41), 'Destination Subnet' (255.255.255.0), and 'Gateway IP' (47.184.55.1). A '(format: 10.10.1.75)' note is next to the Destination IP field. At the bottom are 'Save Route' and 'Back' buttons. The footer contains the Nortel logo and copyright information: 'Copyright 2001-2003 Nortel Networks. All rights reserved.'

The **Network > Routes > Static > Update** form contains the following information:

- Destination IP: IP address of the route destination in dotted decimal notation.
- Destination Subnet: Subnet mask for the route destination in dotted decimal notation.
- Gateway IP: IP address of the gateway in dotted decimal notation.
- **Save Route** button: Submits the form changes to the pending configuration.
- **Back** button: Returns to the previously viewed form without saving changes to this form.

Network > Routes > Proxy ARP

Figure 8-21 shows the **Network > Routes > Proxy ARP** form. Use this form to view and configure the Proxy ARP status and addresses. This allows the Firewall to respond to Proxy ARP requests.

Figure 8-21 Network > Routes > Proxy ARP form

The screenshot shows the Alteon Switched Firewall configuration page for Proxy ARP. The interface includes a navigation menu on the left with options like Monitor, Cluster, Network, Firewall, Operation, Administration, and Diagnostics. The main content area has tabs for DNS, NTP, Ports, Interfaces, VRRP, Gateways, and Routes. Under the Routes tab, there are sub-tabs for Static, Proxy ARP, and OSPF. The Proxy ARP section is active and contains a 'General' section with a dropdown menu for 'Proxy SFD Addresses and Cluster MIP Address' set to 'disabled' and an 'Update' button. Below this is a 'Proxy ARP Addresses' section with a table with columns for 'IP Address' and 'VRRP Group'. The table currently shows 'No proxy ARP addresses configured.' At the bottom, there are input fields for 'New Proxy ARP IP:' and 'VRRP Group:' (set to 1) with an 'Update' button.

The **Network > Routes > Proxy ARP** form contains the following information:

- Proxy Status: Enable or Disable Proxy ARP for this cluster.
- **Update** button: Submits the Proxy status change to the pending configuration.
- IP Address: Lists the IP addresses that the cluster proxy ARPs for.
- VRRP Group: Lists the VRRP group that the cluster proxy ARPs for (if VRRP is set up).
- **Delete** button: Deletes the IP address. Only visible if at least one Proxy ARP address is present.
- New Proxy ARP IP: Enter IP address in dotted decimal format.
- VRRP Group: Select VRRP group 1 or 2.
- **Update** button: Submits the IP address changes to the pending configuration.

Network > Routes > OSPF > General

Figure 8-22 shows the **Network > Routes > OSPF > General** form. Use this form to view and change the dynamic routing settings for OSPF.

Figure 8-22 Network > Routes > OSPF > General form

The screenshot shows the Alteon Switched Firewall configuration page for OSPF settings. The breadcrumb navigation is Network > Routes > OSPF > General. The page has a blue header with the Alteon logo and navigation buttons (Apply, Diff, Revert, Logout, Help). Below the header is a menu bar with tabs for DNS, NTP, Ports, Interfaces, VRRP, Gateways, and Routes. Under the Routes tab, there are sub-tabs for Static, Proxy ARP, and OSPF. The OSPF sub-tab is active, showing a 'General' sub-tab and an 'Area Index' sub-tab. The main content area displays 'Dynamic Routing Settings (OSPF)' with a 'Save Setting' button. The settings are: Status: enabled (dropdown), Spf Interval: 5 (text input, range 0 - 65535), Spf Hold Time: 10 (text input, range 0 - 65535), and Router Id: 33.2.1.1 (text input, format 10.10.1.75). A message 'Settings saved successfully' is displayed at the top of the form area.

The **Network > Routes > OSPF > General** form contains the following information:

- **Status:** Sets the status for OSPF (Enabled or Disabled).
- **SPF Interval:** Sets the time interval, in seconds, between each calculation of the Shortest Path Tree (SPF).
- **SPF Hold Time:** The minimum time OSPF keeps a shortest-path calculation result. This prevents another calculation from happening too soon.
- **Router ID:** Sets a static router id for the cluster. OSPF uses the router id to identify the routing device. If no router id is specified, or if the router id is set to 0.0.0.0 and the iSD host is rebooted, the cluster dynamically selects one of the active IP interfaces on the cluster as the router id.
- **Save Setting** button: Submits the changes made to the pending configuration.

Network > Routes > OSPF > Area Index

Figure 8-23 shows the **Network > Routes > OSPF > Area Index** form. Use this form to view and change the OSPF area index settings.

Figure 8-23 Network > Routes > OSPF > Area Index form

The screenshot shows the Alteon Switched Firewall web interface. The breadcrumb trail at the top reads: **Network > Routes > OSPF > Area Index**. Below the breadcrumb trail, there are several tabs: **DNS**, **NTP**, **Ports**, **Interfaces**, **VRRP**, **Gateways**, and **Routes**. Under the **Routes** tab, there are sub-tabs: **Static**, **Proxy ARP**, and **OSPF**. Under the **OSPF** sub-tab, there are further sub-tabs: **General**, **Area Index**, and **Interface**. The **Area Index** sub-tab is selected, showing the **OSPF Area index Settings** form. The form contains a table with the following data:

Id	Enabled	Area Id	Type	Delete	Modify
1	Yes	33.2.1.2	transit	Delete	Modify

Below the table is a button labeled **Add New Area Index**. The interface also includes a navigation menu on the left with options: **Monitor**, **Cluster**, **Network**, **Firewall**, **Operation**, **Administration**, and **Diagnostics**. The Alteon logo is visible in the bottom left corner.

The **Network > Routes > OSPF > Area Index** form contains the following information:

- **ID**: The index number for this area index, that is, its place in the list of area indexes attached to this firewall iSD.
- **Enabled**: Yes or No.
- **Area ID**: The IP address which identifies this area index.
- **Type**: Transit (default) or Stub.
- **Delete** button: Deletes the area index adjacent to the button. Only visible if an area ID is present.
- **Modify** button: Opens the form for modifying the area index adjacent to the button. See the **Update** form on [page 259](#).
- **Add New Area Index** button: Opens the form for configuring a new area index.

Network > Routes > OSPF > Area Index > Update (Add or Modify)

Figure 8-24 shows the **Network > Routes > OSPF > Area Index > Update** form. Use this form to update the OSPF area index settings.

Figure 8-24 Network > Routes > OSPF > Area Index > Update form

The screenshot shows the Alteon Switched Firewall configuration interface. The top navigation bar includes 'DNS', 'NTP', 'Ports', 'Interfaces', 'VRRP', 'Gateways', and 'Routes'. The 'Routes' menu is expanded to show 'Static', 'Proxy ARP', and 'OSPF'. The 'OSPF' menu is further expanded to show 'General', 'Area Index', and 'Interface'. The 'Area Index' sub-menu is selected, displaying the 'Modify Area Index' form. The form has a 'General Settings' section with the following fields:

- Identifier: 1
- Status: enabled
- Area Id: 33.2.1.2 (format: 10.10.1.75)
- Type: transit

At the bottom of the form are 'Update' and 'Back' buttons.

The **Network > Routes > OSPF > Area Index > Update** form contains the following information:

- **Identifier:** Sets the unique area ID (1-16).
- **Status:** Sets the area index status (enabled or disabled).
- **Area ID:** Sets the IP address that identifies this area index.
- **Type:** Sets the area index type (transit or stub).
- **Update** button: Submits the area index settings to the pending configuration.
- **Back** button: Returns to the **Network > Routes > OSPF > Area Index** form without submitting the changes.

Network > Routes > OSPF > Interface

Figure 8-25 shows the **Network > Routes > OSPF > Interface** form. Use this form to change the OSPF Interface settings, which are required to attach an IP network to an OSPF area.

Figure 8-25 Network > Routes > OSPF > Interface form

The screenshot shows the Alteon Switched Firewall web interface. The breadcrumb trail at the top reads: DNS > NTP > Ports > Interfaces > VRRP > Gateways > Routes > OSPF > Interface. The main content area is titled "OSPF Interface Settings" and contains a table with the following data:

Id	Enabled	Area Index	
2	No	0	Modify

The interface also features a left-hand navigation menu with options: Monitor, Cluster, Network, Firewall, Operation, Administration, and Diagnostics. The footer includes the Nortel Networks logo and the text "Copyright 2001-2003 Nortel Networks. All rights reserved."

The **Network > Routes > OSPF > Interface** form contains the following information:

- **Id**: Numerical id for the interface (between 1 and 255).
- **Enabled**: Enable/disable the interface.
- **Area Index**: Sets the OSPF area index to attach to the network for the current IP interface.
- **Modify** button: Modify a displayed interface. Only visible if interfaces are present. See the **Update** form on [page 261](#).

Network > Routes > OSPF > Interface > Update (Modify)

Figure 8-26 shows the **Network > Routes > OSPF > Interface > Update** form. Use this form to update the OSPF interface settings, which are required to attach an IP network to an OSPF area.

Figure 8-26 Network > Routes > OSPF > Interface > Update form

The screenshot displays the Alteon Switched Firewall web interface. The breadcrumb navigation path is **Network > Routes > OSPF > Interface > Update**. The page title is "Modify Interface". The "General Settings" section contains the following fields:

- Identifier: 2
- Status: disabled
- Area Index: 1
- Priority: 0
- Cost: 0 (1 - 65535, 0=none)
- Hello: 10 (1 - 65535)
- Dead: 40 (1 - 65535)
- Transmit: 1
- Retransmit: 5
- Authentication: none
- Key:
- MD5 Auth Key Number: 1
- MD5 Auth Key:

Buttons for "Update" and "Back" are located at the bottom of the form.

The **Network > Routes > OSPF > Interface > Update** form contains the following information:

- Identifier: Numerical id for the interface (between 1 and 255).
- Status: Enables or disables the interface.
- Area Index: Sets the OSPF area index to attach to the network for the current IP interface.
- Priority: Sets the IP interface (IF) priority that is used when electing a Designated Router (DR) and Backup Designated Router (BDR) for the area. The default is 1 (lowest priority). A value of 0 specifies that the elected interface is DROTHER and cannot be used as a DR or BDR.
- Cost: Sets the cost of output routes on this interface. Cost is used in calculating the shortest path tree throughout the AS. Cost is based on bandwidth. Low cost indicates high bandwidth.

- Hello: Sets the hello interval in seconds. The switch sends hello messages to inform neighbors that the link is up. The value must be the same on all routing devices within the area.
- Dead: Sets the router dead interval, in seconds. If the switch does not receive "hello" on the IP interface within the dead interval, the switch will declare the interface to be down. Typically, the dead value is four times the value of "hello". This value must be the same on all routing devices within the same area.
- Transmit: Sets the transmit delay, in seconds. This is the estimated time required to transmit an LSA to adjacencies on this interface, taking into account transmission and propagation delays. This value must be the same on all routing devices within the area.
- Retransmit: Sets the time interval, in seconds, between each transmission of LSAs to adjacencies on this interface. This value must be the same on all routing devices within the area.
- Key: When the "auth" option is set to "password", the "key" option sets the password to be used for OSPF authentication. Specify a type 1 (plain text) password of up to eight characters. When "auth" is set to "none", the "key" option is ignored.

Firewall forms

The Firewall sub-menu items are the following:

- “Firewall > Settings” on page 263
- “Firewall > License Management” on page 264
 - “Firewall > License Management > Update (Delete or Modify)” on page 265
- “Firewall > Synchronization” on page 267

Firewall > Settings

Figure 8-27 shows the **Firewall > Settings** form. Use this form to change the firewall iSD status and reset SIC.

Figure 8-27 Firewall > Settings form

The **Firewall > Settings** form contains the following information:

- **Status:** Enables or disables Check Point FireWall-1 NG processing on the firewall iSD.
- **Update** button: Submits the form changes to the pending configuration.

- Status: Enables or disables software updating with Check Point SmartUpdate.

NOTE – Once you have completed the software update, be sure to disable SmartUpdate management.

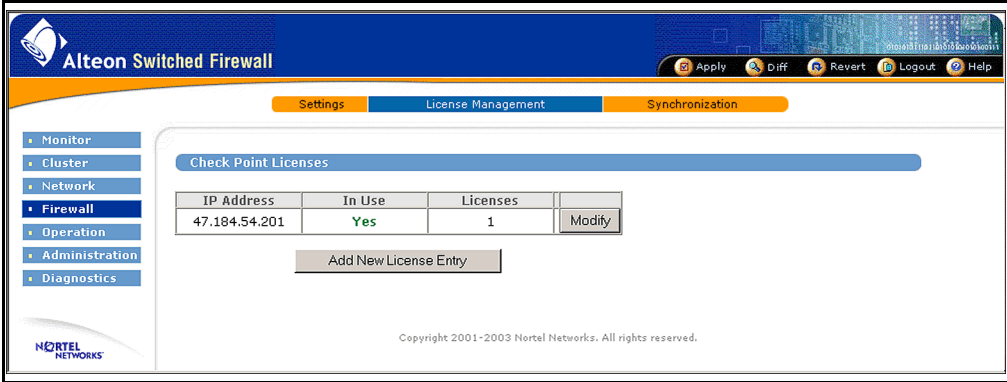
Use the Secure Internal Communication area of the form to establish SIC between the management station and the firewall iSD. This area of the form contains the following information:

- List of Hosts: Lists the firewall iSD hosts by IP address.
- Password: Enter the Check Point SIC password (different from the login password) in this field.
- Password (again): Re-enter the Check Point SIC password.
- **Reset SIC** button: Resets SIC for the firewall iSD.

Firewall > License Management

Figure 8-28 shows the **Firewall > License Management** form. Use this form to modify or install additional Check Point licenses on the firewall iSD.

Figure 8-28 Firewall > License Management form



IP Address	In Use	Licenses	
47.184.54.201	Yes	1	Modify

Add New License Entry

Copyright 2001-2003 Nortel Networks. All rights reserved.

NOTE – Plug N Play must be enabled for a firewall iSD to be brought into service with the selected license.

NOTE – In this release, you can only use this BBI form to add a license that is bound to the IP address of the firewall iSD.

The **Firewall > License Management** form contains the following information:

- **IP Address:** The IP address for the firewall iSD.
- **In Use:** Shows whether the IP address is currently assigned (Yes) to a firewall iSD, or whether it is available (No) to configure a new firewall iSD.
- **Licenses:** Shows the number of Check Point licenses currently configured for each IP address.
- **Modify** button: Allows you to modify or delete Check Point licenses for the IP address. See the **Update** form on [page 265](#).
- **Add New License Entry** button: Allows you to add Check Point licenses for the IP address. Clicking this button opens a form that looks like the **Update** form on [page 265](#), but with blank fields.

Firewall > License Management > Update (Delete or Modify)

[Figure 8-29](#) shows the **Firewall > License Management > Update** form. Use this form to update Check Point licenses on the firewall iSD.

Figure 8-29 Firewall > License Management > Update form

The screenshot shows the Alteon Switched Firewall web interface. The main content area is titled "Modify Check Point Licenses" and is divided into three sections:

- General Settings:** Shows the IP Address as 47.184.54.201.
- Current Licenses:** A table with the following data:

Expiration	Features	License	Delete
01Apr2003	CPMP-EVAL-1-DES-NG CK-CP	d9buCNLe9-ApJ9yv3pg-Agw8Gbpmq-xQM4LaGhp	<input type="checkbox"/>
- Add New License:** Three input fields for "Expiration Date", "Feature String", and "License String".

At the bottom of the form are "Save Page" and "Back" buttons. The left sidebar contains navigation links for Monitor, Cluster, Network, Firewall, Operation, Administration, and Diagnostics. The top navigation bar includes Settings, License Management, and Synchronization tabs, along with utility buttons for Apply, Diff, Revert, Logout, and Help.

The **Firewall > License Management > Update** form contains the following information:

- **IP Address:** Lists the IP address of the Firewall.
- **Shared Secret:** Enter the shared secret between the firewall iSD and the SmartCenter Server.

The shared secret establishes trust between the firewall iSD and the SmartCenter Server. If you are unable to establish trust, reset the SIC on the firewall iSD (through CLI or BBI) and the management station. This field does not appear if trust is already established.

- **Shared Secret (again):** Re-enter the shared secret.

The **Current Licenses** area of the form displays the licenses assigned to the selected IP address:

- **Expiration:** Expiration date of the Check Point license.
- **Features:** The features of the Check Point license.
- **License:** The Check Point license.
- **Delete:** When checked, prepares to delete this license from the Plug N Play resource pool.

The **Add New Licenses** area of the form is used to enter information for new Check Point licenses to be assigned to the current IP address.

- **Expiration Date:** Sets the expiration date of the Check Point license.
- **Feature String:** Sets the features of the Check Point license.
- **License String:** Sets the license string of the Check Point license.
- **Save Page** button: Submit the form changes to the pending configuration.
- **Back** button: Return to the **Firewall > License Management** form without saving changes.

Firewall > Synchronization

Figure 8-30 shows the **Firewall > Synchronization** form. This form displays the cluster synchronization status for the cluster and lets you enable it. Firewall synchronization provides for stateful failover of open sessions when a master is backed up by the backup master.

Figure 8-30 Firewall > Synchronization form

The screenshot shows the Alteon Switched Firewall web interface. The top navigation bar includes 'Settings', 'License Management', and 'Synchronization'. The left sidebar lists menu items: Monitor, Cluster, Network, Firewall, Operation, Administration, and Diagnostics. The main content area is titled 'Firewall Synchronization' and contains a 'Status' dropdown menu set to 'enabled' and a 'Save Setting' button. The footer includes the Nortel Networks logo and copyright information: 'Copyright 2001-2003 Nortel Networks. All rights reserved.'

The **Firewall > Synchronization** form contains the following information:

- Status: Enables or disables cluster synchronization.
- **Save Settings** button: Submits the form changes to the pending configuration.

Operations forms

The Operations sub-menu items are the following:

- “Operation > Configuration” on page 268
- “Operation > Update” on page 269

Operation > Configuration

Figure 8-31 shows the **Operation > Configuration** form. Use this form to export or import configuration files.

Figure 8-31 Operation > Configuration form

The **Operation > Configuration** form contains the following information:

- **Secret key:** The case-sensitive secret key is used to encrypt the settings and must be supplied again when the configuration is imported.
- **Export** button: Depending on the browser type, the administrator may have the option to output to a file or to the screen (allowing it to be captured using copy and paste functions).
- **Text input area:** Import a configuration by pasting it into the field provided. A configuration can be copied and pasted from a saved text file.

- **Secret Key:** The case-sensitive secret key used in the export must be supplied to decrypt the configuration settings.
- **Import button:** Replace the current configuration using the pasted configuration information. This takes effect immediately. No apply command is required.

NOTE – Importing a configuration will cause the BBI to restart. If the import is successful, any imported configuration overrides all prior configuration settings. All changes pending at the time of the import are lost. The **Revert** command cannot be used to recover the prior configuration.

Operation > Update

NOTE – The 8660 SDM ships with the most recent version of firewall OS software installed. You need to use the **Operation > Update** form only for future software upgrades.

Figure 8-32 shows the **Operation > Update** form. Use this form to update your firewall iSD software from your browser. A browser-based software update is a distinctly different process from a CLI-based software update (see [Note – on page 270](#)).

Figure 8-32 Operation > Update form

The screenshot shows the Alteon Switched Firewall web interface. The top navigation bar includes buttons for Apply, Diff, Revert, Logout, and Help. The main content area is titled 'Configuration' and 'Update'. On the left, there is a navigation menu with options: Monitor, Cluster, Network, Firewall, Operation (selected), Administration, and Diagnostics. The main content area contains a 'Packages' section with a table showing the current software version and a table with columns for Version, Name, Status, and Actions. Below the table is an 'Upload New Package' section with a 'File:' input field, a 'Browse...' button, and a 'Submit' button. A warning message at the bottom states: 'Warning: The time it takes to upload a package is dependent upon the speed of the Internet connection. Slow connections may take many minutes.'

Version	Name	Status	Actions
2.2.2.2	tdo	permanent	
2.2.0.14	tdo	old	Activate

The **Operation > Update** form contains the following information:

- **Version:** The firewall software version running on the cluster.
- **Name:** The name of the software package.

- **Status:** The software package status (permanent, old, unpacked). The permanent version is the one that is currently running. The previous (old) software version is displayed if it exists, that is, if you have uploaded at least one software version from a tftp/ftp server. The unpacked version has been downloaded, but never activated (part of the activation process is to unpack the code).
- **Actions buttons:** **Activate** reboots the iSD host so that it will come up with the selected software version. **Delete** removes the selected software version from storage.
- **Browse** button: Click this button and navigate to the file location to select a file for upload.
- **Submit** button: Uploads the software package you selected in the **File:** field.

NOTE – The advantage to using your browser to upload software is that a TFTP or FTP server is not required. For example, if you download the latest software update *.pkg* file from the Nortel Networks Customer Support site to your Windows Desktop, you can navigate to the Desktop location using the **Browse** button and upload the *.pkg* file from there to your firewall iSD. The disadvantage is that activating the version disables remote access. To restore remote access (that is, browser access), you must log in at your local console, reenter your Check Point license, and reload the remote access policy.

Administration forms

The administration forms allow administrators to control client and user access to the system, through Telnet, SSH, SNMP, SSL, and the web. Forms for administering certification and licensing are also here.

The Administration sub-menu items are the following:

- “Administration > Users” on page 272
- “Administration > Users > Add New User” on page 273
- “Administration > Access List” on page 274
 - “Administration > Access List > Update (Add or Modify)” on page 275
- “Administration > Telnet-SSH” on page 276
- “Administration > Web > General” on page 277
- “Administration > Web > Create Cert” on page 278
- “Administration > Web > Server Certs” on page 279
 - “Administration > Web > Server Certs > Update (Add or Modify)” on page 280
- “Administration > Web > CA Certs” on page 281
 - “Administration > Web > CA Certs > Update (Add or Modify)” on page 282
- “Administration > SNMP > General” on page 283
- “Administration > SNMP > System” on page 284
- “Administration > SNMP > Trap Hosts” on page 285
 - “Administration > SNMP > Trap Hosts > Update (Add or Modify)” on page 286
- “Administration > SNMP > USM Users” on page 287
 - “Administration > SNMP > USM Users > Update (Add or Modify)” on page 288
- “Administration > SNMP > Advanced” on page 289

Administration > Users

Figure 8-33 shows the **Administration > Users** form. Use this form to add, modify, delete, or list firewall user accounts, and change passwords.

Figure 8-33 Administration > Users form

The screenshot shows the Alteon Switched Firewall web interface. The top navigation bar includes 'Users', 'Access List', 'Telnet-SSH', 'Web', and 'SNMP'. The left sidebar has a menu with 'Administration' highlighted. The main content area is titled 'Administration Users' and contains a table with the following data:

Username	Group(s)	
root	root	Modify
admin	admin, oper	Modify
oper	oper	Modify

Below the table is an 'Add New User' button. Underneath is the 'Password Expire Time' section, which includes a text input field with the value '0' and the text '(in seconds, 0 = never)', followed by an 'Update' button.

The **Administration > Users** form contains the following information:

- **Administration Users:** You can change the passwords for the default user names (root, admin, oper) using the **Modify** buttons, but you cannot remove these names. The user names you add can be deleted or modified.
- **Add New Users** button: Opens the **Add New Users** form that allows you to add a new user name to a specified group and to set the password (see the “[Administration > Users > Add New User](#)” on page 273).
- **Password Expire Time:** You can set the time (in seconds) to any value by entering it in the **Password Expiration** field. The value applies to the current username. The default value “0” means the password will never expire.
- **Update** button: Confirms the value in the **Password Expiration** field for the current username.

Administration > Users > Add New User

Figure 8-34 shows the **Administration > Users > Add New User** form. Use this form to specify a new username.

Figure 8-34 Administration > Users > Add New User form

The screenshot shows the 'Add New User' form in the Alteon Switched Firewall web interface. The interface has a blue header with the Alteon logo and 'Alteon Switched Firewall' text. Below the header is a navigation bar with tabs for 'Users', 'Access List', 'Telnet-SSH', 'Web', and 'SNMP'. On the left is a sidebar menu with options: Monitor, Cluster, Network, Firewall, Operation, Administration (highlighted), and Diagnostics. The main content area is titled 'Add New User' and contains the following fields and controls:

- Username:** A text input field containing 'test'.
- Group:** Two list boxes. The 'Available' list contains 'admin' and 'oper'. The 'Selected' list is empty. Between the lists are '>>' and '<<' buttons.
- Set Password:** Three password input fields: 'Admin Password', 'Password', and 'Password (again)'. Each field contains a masked password 'AAAAAA'.
- Buttons:** 'Save User' and 'Back' buttons at the bottom of the form.

The **Administration > Users > Add New User** form contains the following information:

- **Username:** Enter the new user name in the **Username** field.
- **Group:** Select a group name from the **Available** field and add it to the **Selected** field by clicking the >> button. Deselect a group name in the **Selected** field by pressing the << button.
- **Admin Password:** Enter the administration password in the **Admin Password** field.
- **Password:** Enter the password for the new username in the **Password** field.
- **Password (again):** Confirm the password by re-typing it in the **Password (again)** field.
- **Save User** button: Click Save User to submit the new username and password.

NOTE – You must still apply and save the settings after pressing the **Save User** button.

- **Back** button: Click **Back** to return to the **Administration > Users** form without saving the new username and password.

Administration > Access List

Figure 8-35 shows the **Administration > Access List** form. Use this form to specify which clients are permitted to administer the system. For example, to access the BBI, the client must be matched by an entry in this form.

Figure 8-35 Administration > Access List form

Network Address	Subnet Mask		
47.184.177.0	255.255.255.0	Delete	Modify
47.102.147.0	255.255.255.0	Delete	Modify
47.184.54.0	255.255.255.0	Delete	Modify

Add New Access Control

Copyright 2001-2003 Nortel Networks. All rights reserved.

The **Administration > Access List** form contains the following information:

- Network Address: IP address of the client in dotted decimal notation.
- Subnet Mask: Subnet address used for matching. Uses dotted decimal notation.
- **Delete** button: Deletes an entry from the system. Only visible if access entries are present.

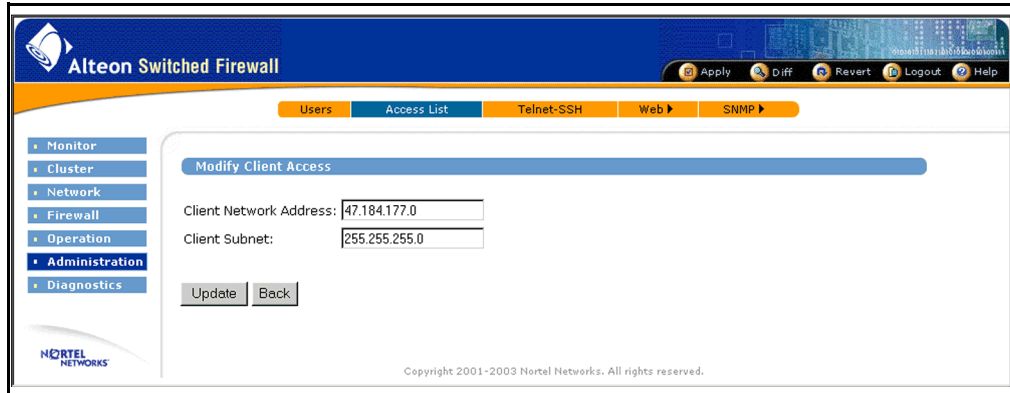
NOTE – Deleting the entry corresponding to the current client will terminate the connection when the change is applied.

- **Modify** button: Modifies an entry in the system. Only visible if access entries are present. See the **Update** form on [page 275](#).
- **Add New Access Control** button: Adds a new entry to the access list. See the **Update** form on [page 275](#).

Administration > Access List > Update (Add or Modify)

Figure 8-36 shows the **Administration > Access List > Update** form. Use this form to add or change client access information.

Figure 8-36 Administration > Access List > Update form



The **Administration > Access List > Update** form contains the following information:

- **Client Network Address:** IP address of the client in dotted decimal notation.
- **Client Subnet:** Subnet address used for matching. Uses dotted decimal notation.
- **Update** button: Submits the form changes to the pending configuration.
- **Back** button: Returns to the **Administration > Access List** form without saving changes.

Administration > Telnet-SSH

Figure 8-37 shows the **Administration > Telnet-SSH** form. Use this form to enable or disable Telnet or SSH administration.

Figure 8-37 Administration > Telnet-SSH form

The **Administration > Telnet-SSH** form contains the following information:

- Telnet: Enable administration through Telnet.
- SSH: Enable administration through SSH.
- CLI Timeout: Sets the number of seconds a Telnet or SSH session can remain idle before being automatically disconnected.

NOTE – If you make changes to the firewall iSD configuration, and do not apply them before the CLI times out, all changes will be lost.

- **Update** button: Submits the form changes to the pending configuration.

Administration > Web > General

Figure 8-38 shows the **Administration > Web > General** form. Use this form to specify BBI administration settings.

Figure 8-38 Administration > Web > General form

The screenshot displays the Alteon Switched Firewall web interface. At the top, there's a navigation bar with tabs for 'Users', 'Access List', 'Telnet-SSH', 'Web', and 'SNMP'. Below this, there are sub-tabs for 'General', 'Create Cert', 'Server Certs', and 'CA Certs'. The left sidebar shows a tree view with 'Administration' highlighted. The main content area is titled 'Web Settings' and contains the following configuration fields:

- HTTP Settings:**
 - Port:
 - Status:
- HTTP/SSL Settings:**
 - Port:
 - Status:
 - TLS:
 - SSL v2:
 - SSL v3:

An 'Update' button is located at the bottom of the form.

The **Administration > Web > General** form contains information for both HTTP settings and HTTP/SSL settings.

HTTP settings are the following:

- Port: Application port used for non-secure HTTP access to the BBI. The default is port 80.
- Status: Enables or disables HTTP access to the BBI.

HTTP/SSL (HTTPS) settings are the following:

- Port: Application port for secure HTTPS (using SSL) access to the BBI. The default is port 443.
- Status: Enables or disables HTTPS access to the BBI.
- TLS: Enable TLS protocol.
- SSL v2: Enable SSL v2 protocol.
- SSL v3: Enable SSL v3 protocol.
- **Update** button: Submits the form changes to the pending configuration.

Administration > Web > Create Cert

Figure 8-39 shows the **Administration > Web > Create Cert** form. Use this form to generate a self-signed certificate.

Figure 8-39 Administration > Web > Create Cert form

The screenshot shows the Alteon Switched Firewall web interface. The top navigation bar includes 'Users', 'Access List', 'Telnet-SSH', 'Web', and 'SNMP'. Below this, there are tabs for 'General', 'Create Cert', 'Server Certs', and 'CA Certs'. The 'Create Cert' tab is active, displaying the 'Generate Self-Signed Certificate' form. The form has three input fields: 'Common Name' with the value 'Lary', 'Two-Letter Country Code' with the value 'US', and 'Key Size' with a dropdown menu set to '512'. At the bottom of the form are 'Submit' and 'Back' buttons. The left sidebar contains a menu with options: Monitor, Cluster, Network, Firewall, Operation, Administration (highlighted), and Diagnostics. The bottom left corner features the Nortel Networks logo.

The **Administration > Web > Create Cert** form contains the following information:

- **Common Name:** Common name (cn) to be used with the certificate.
- **Two-Letter Country Code:** Country code to be used. For example, US for the United States of America, CA for Canada, JP for Japan, AU for Australia, and so on.
- **Key Size:** Size of the encryption key. Valid sizes are 512, 1024, or 2048 bits.
- **Submit button:** Submits the form changes to the pending configuration and opens the **Server Certificates** form (see [page 279](#)).
- **Back button:** Returns to the previously viewed form without saving changes.

Administration > Web > Server Certs

Figure 8-40 shows the **Administration > Web > Server Certs** form. Use this form to administer server certificates on the firewall iSD.

Figure 8-40 Administration > Web > Server Certs form

The screenshot shows the Alteon Switched Firewall web interface. The top navigation bar includes 'Users', 'Access List', 'Telnet-SSH', 'Web', and 'SNMP'. The 'Web' menu is expanded to show 'General', 'Create Cert', 'Server Certs', and 'CA Certs'. The 'Server Certs' page features a table with the following data:

Id	Issuer	Subject	Serial Number	Valid From	Valid To	Delete	Modify
1	CN=Larry C=US	CN=Larry C=US	00	Apr 4 20:34:34 2003 GMT	Apr 1 20:34:34 2013 GMT	Delete	Modify

Below the table is an 'Add New Server Certificate' button. At the bottom of the page, there are buttons for 'Generate Certificate Request' and 'Export Certificate Request'.

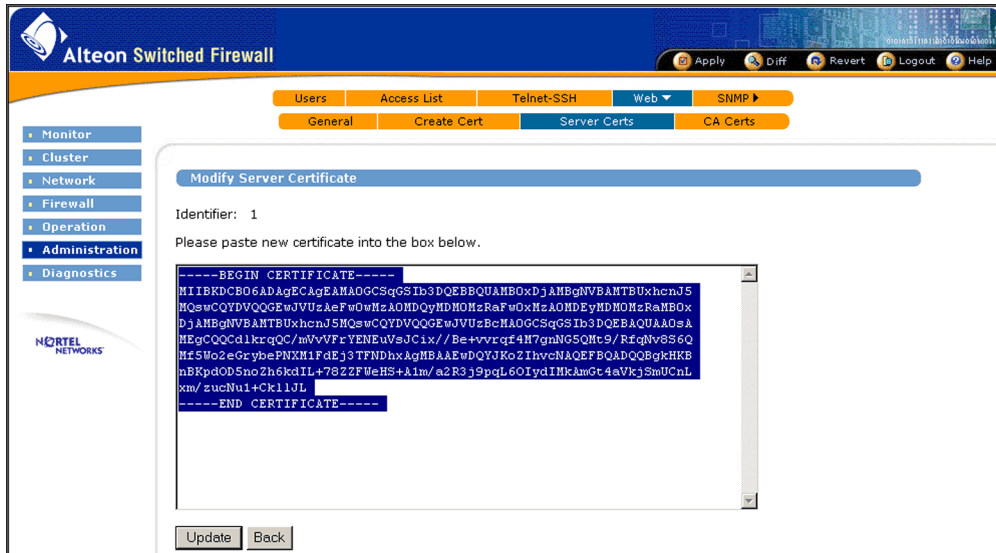
The **Administration > Web > Server Certs** form contains the following information:

- **Id:** Identifier for the certificate.
- **Issuer:** Issuer of the certificate.
- **Subject:** Subject of the certificate
- **Serial Number:** Serial number of the certificate.
- **Valid From:** Certificate valid start date.
- **Valid To:** Certificate valid end date.
- **Delete button:** Deletes a certificate from the system. Only visible if a certificate is present.
- **Modify button:** Modifies a displayed certificate. Only visible if a certificate is present. See the **Update** form on [page 280](#).
- **Add New Server Certificate button:** Displays a new form used for inputting a new certificate. Paste the certificate into the text area. The server certificate is used for a Secure Sockets Layer (SSL) connection the firewall iSD. See the **Update** form on [page 280](#).
- **Export Certificate Request button:** Exports a certificate created using the **Generate Certificate Request** button. Use these buttons to obtain a server certificate to be added. The **Export Certificate Request** form is identical to the “[Administration > Web > Create Cert](#)” form on [page 278](#).

Administration > Web > Server Certs > Update (Add or Modify)

Figure 8-41 shows the Administration > Web > Server Certs > Update form. Use this form to update server certificates on the firewall iSD.

Figure 8-41 Administration > Web > Server Certs > Update form



The Administration > Web > Server Certs > Update form contains the following information:

- Identifier: ID for the certificate.
- Text area: Paste a new certificate into the text area.
- **Update** button: Submits the form changes to the pending configuration.
- **Back** button: Returns to the Administration > Web > Server Certs form without saving changes.

Administration > Web > CA Certs

Figure 8-42 shows the **Administration > Web > CA Certs** form. Use this form to administer Certificate Authority (CA) certificates on the firewall iSD. This is required if server certificates from an external CA are being used.

Figure 8-42 Administration > Web > CA Certs form

The screenshot shows the Alteon Switched Firewall web interface. The top navigation bar includes 'Users', 'Access List', 'Telnet-SSH', 'Web', and 'SNMP'. The 'Web' menu is expanded to show 'General', 'Create Cert', 'Server Certs', and 'CA Certs'. The 'CA Certs' tab is active, displaying a table with the following columns: Id, Issuer, Subject, Serial Number, Valid From, and Valid To. The table is currently empty, with the text 'No CA certificates entered.' displayed below it. An 'Add New CA Certificate' button is located below the table. The Nortel logo and copyright information are visible at the bottom of the page.

The **Administration > Web > CA Certs** form contains the following information:

- **Id:** Identifier for the certificate.
- **Issuer:** Issuer of the certificate.
- **Subject:** Subject of the certificate.
- **Serial Number:** Serial number of the certificate.
- **Valid From:** Starting date upon which the certificate is valid.
- **Valid To:** Ending date upon which the certificate is valid.
- **Delete button:** Deletes a certificate from the system. Only visible if a certificate is present.
- **Modify button:** Modifies a displayed certificate. Only visible if a certificate is present. See the **Update** form on [page 282](#).
- **Add New CA Certificate button:** This opens the **Add New CA Certificate** form. See the **Update** form on [page 282](#).

Administration > Web > CA Certs > Update (Add or Modify)

Figure 8-43 shows the **Administration > Web > CA Certs > Update** form. Use this form to update a CA certificate.

Figure 8-43 Administration > Web > CA Certs > Update form

The screenshot shows the Alteon Switched Firewall web interface. The top navigation bar includes 'Alteon Switched Firewall' and several utility buttons: 'Apply', 'Diff', 'Revert', 'Logout', and 'Help'. Below the navigation bar, there are tabs for 'Users', 'Access List', 'Telnet-SSH', 'Web', and 'SNMP'. Under the 'Web' tab, there are sub-tabs for 'General', 'Create Cert', 'Server Certs', and 'CA Certs'. The 'CA Certs' sub-tab is selected. On the left side, there is a vertical menu with options: 'Monitor', 'Cluster', 'Network', 'Firewall', 'Operation', 'Administration', and 'Diagnostics'. The 'Administration' option is highlighted. The main content area is titled 'Add CA Certificate' and contains the following text: 'Identifier: 1' and 'Please paste new certificate into the box below.' Below this text is a large, empty text area with a vertical scrollbar. At the bottom of the form, there are two buttons: 'Update' and 'Back'.

The **Administration > Web > CA Certs > Update** form contains the following information:

- Identifier: ID for the certificate.
- Text area: Paste a new certificate into the text area.
- **Update** button: Submits the form changes to the pending configuration.
- **Back** button: Returns to the **Administration > Web > CA Certs** form without saving changes.

Administration > SNMP > General

Figure 8-44 shows the **Administration > SNMP > General** form. Use this form to enable or disable SNMP event and alarm messages for the firewall iSD.

Figure 8-44 Administration > SNMP > General form

The screenshot displays the 'Administration > SNMP > General' configuration page. The page title is 'Alteon Switched Firewall'. The navigation menu on the left includes: Monitor, Cluster, Network, Firewall, Operation, Administration (selected), and Diagnostics. The main content area is titled 'General' and contains the following settings:

- Status: disabled
- Security Model: v2c
- Access: disabled
- Events: disabled
- Alarms: disabled
- SNMPv2c Options: Read Community String (v2c): public
- SNMPv3 (USM) Options: Security Level (usm): auth

An 'Update' button is located at the bottom of the form.

The **Administration > SNMP > General** form contains the following information:

- **Status:** Enables or disables the SNMP features. This must be enabled for events and alarms to be sent to the trap hosts.
- **Security Model:** Choose either SNMP v2c or SNMP v3 (usm). SNMP v3 has enhanced security features such as protection against masquerade, message modification, replay, and disclosure.
- **Access:** Specify whether read access is allowed.
- **Events:** Enables or disables sending event messages to the SNMP trap hosts. When enabled, messages regarding general occurrences (such as detection of a new component) are sent.
- **Alarms:** Enable or disable sending alarm messages to the SNMP trap hosts. Alarm messages indicate serious conditions that require administrative action.
- **Read Community String (v2c):** Specify the community string used in an SNMP v2c read.
- **Security Level (usm):** Specify whether the level of security should be authentication only (auth) or authentication and encryption (priv). Authentication uses MD5 and encryption uses DES.

- **Update** button: Submits the form changes to the pending configuration.

Administration > SNMP > System

Figure 8-45 shows the **Administration > SNMP > System** form. Use this form to enter administrative information on behalf of the SNMP system.

Figure 8-45 Administration > SNMP > System form

The screenshot shows the 'Administration > SNMP > System' form in the Alteon Switched Firewall web interface. The form is titled 'System Settings' and contains the following fields and buttons:

- Email Contact:**
- Cluster Name:**
- Cluster Location:**
- Update** button

The interface also features a navigation menu on the left with 'Administration' selected, and a top navigation bar with 'SNMP' selected. The Alteon logo and copyright information are visible at the bottom.

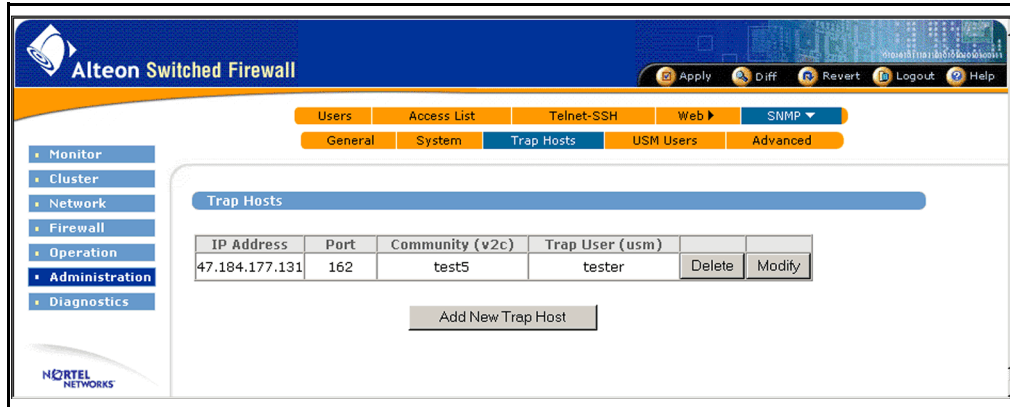
The **Administration > SNMP > System** form contains the following information:

- **Email Contact:** Email address of the SNMP administrator.
- **Cluster Name:** A name for referencing the cluster.
- **Cluster Location:** A name for referencing the cluster location.

Administration > SNMP > Trap Hosts

Figure 8-46 shows the **Administration > SNMP > Trap Hosts** form. This form lists all configured trap hosts that will receive SNMP event or alarm messages from the firewall iSD.

Figure 8-46 Administration > SNMP > Trap Hosts form



The **Administration > SNMP > Trap Hosts** form contains the following information:

- **IP Address:** This is the IP address of the trap host.
- **Port:** This is the logical port on the trap host that listens for SNMP traffic. The SNMP default port is 162.
- **Community (v2c):** This is the community string for the trap host.
- **Trap User (usm):** This is the user employed for trap authentication. The user must exist in the administration database and can belong to either the “oper” or “admin” groups. The “oper” group is recommended. The authentication and encryption passwords are the same as those currently in the database.
- **Delete button:** Deletes an SNMP trap host from the configuration. This button is only visible if trap hosts are present.
- **Modify button:** Modifies parameters for an existing trap host. This button is only visible if trap hosts are present. See the **Update** form on [page 286](#).
- **Add New Trap Host button:** Allows you to add and configure a new trap host. See the **Update** form on [page 286](#) for details.

Administration > SNMP > Trap Hosts > Update (Add or Modify)

Figure 8-47 shows the **Administration > SNMP > Trap Hosts > Update** form. Use this form to update the trap host information.

Figure 8-47 Administration > SNMP > Trap Hosts > Update form

The screenshot displays the Alteon Switched Firewall web interface. The top navigation bar includes 'Users', 'Access List', 'Telnet-SSH', 'Web', and 'SNMP'. The 'SNMP' menu is expanded to show 'General', 'System', 'Trap Hosts', 'USM Users', and 'Advanced'. The 'Trap Hosts' sub-menu is selected, leading to the 'Add Trap Host' form. The form contains the following fields:

- IP Address:** A text input field with '0.0.0.0' entered and a note '(format: 10.10.1.75)'.
- Port:** A text input field with '162' entered.
- Community String (v2c):** An empty text input field.
- Trap User (v3):** An empty text input field.

At the bottom of the form are 'Update' and 'Back' buttons. The footer of the page reads 'Copyright 2001-2003 Nortel Networks. All rights reserved.'

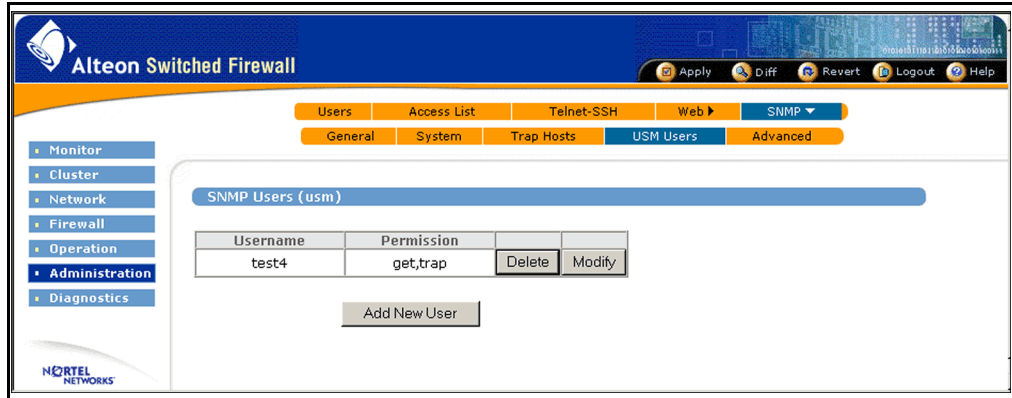
The **Administration > SNMP > Trap Hosts > Update** form contains the following information:

- **IP Address:** The IP address of trap host in dotted decimal notation.
- **Port:** The logical port to which the trap should be sent (the SNMP default port is 162).
- **Community String (v2c only):** The Community string for the trap host.
- **Trap User (v3 only):** The user employed for trap authentication. The user must exist in the administration database and can belong to either the “oper” or “admin” groups. The “oper” group is recommended. The authentication and encryption passwords are the same as those currently in the database.

Administration > SNMP > USM Users

Figure 8-48 shows the **Administration > SNMP > USM Users** form. This form is for administering USM users who are employed in SNMP v3 (usm) authentication/encryption. This user table is entirely separate from the global administration user database and is only used in SNMP v3 requests.

Figure 8-48 Administration > SNMP > USM Users form



The **Administration > SNMP > USM Users** form contains the following information:

- **Username:** Name of user for SNMP v3 (usm) authentication/encryption.
- **Permission:** Type of permission allowed for the user (read, trap, or both).
- **Delete button:** Delete a user from the system. This button is visible only when users are present.
- **Modify Button:** Modify a displayed user. This button is visible only when users are present. See the **Update** form on [page 288](#).
- **Add New User button:** Allows you to add a new USM user. See the **Update** form on [page 288](#) for details.

Administration > SNMP > USM Users > Update (Add or Modify)

Figure 8-49 shows the **Administration > SNMP > USM Users > Update** form. Use this form to update information for USM users.

Figure 8-49 Administration > SNMP > USM Users > Update form

The screenshot shows the 'Add SNMP User' form in the Alteon Switched Firewall web interface. The breadcrumb navigation is 'Administration > SNMP > USM Users > Update'. The form has a title bar 'Add SNMP User' and a left sidebar with navigation options: Monitor, Cluster, Network, Firewall, Operation, Administration (selected), and Diagnostics. The main content area contains the following fields and controls:

- Username:** A text input field containing 'test5'.
- Permission:** A field with two checkboxes: 'get' (checked) and 'trap' (checked).
- Authentication Password:** A password input field with masked characters.
- Authentication Password (again):** A second password input field for confirmation.
- Encryption Password:** A password input field for DES encryption.
- Encryption Password (again):** A second password input field for confirmation.

Below the fields, a blue note reads: 'Both passwords must be set when a user is added.' At the bottom of the form are two buttons: 'Update' and 'Back'.

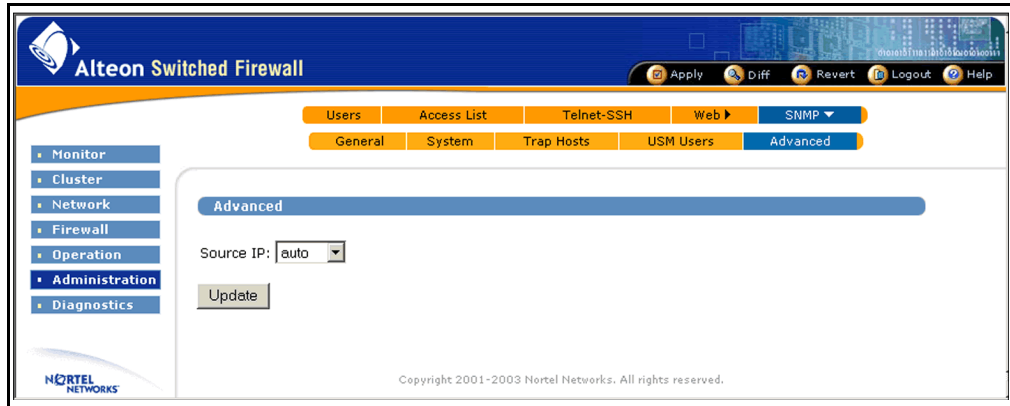
The **Administration > SNMP > USM Users > Update** form contains the following information:

- **Authentication Password:** Password used in MD5 authentication. You must set this password when the user is created.
- **Encryption Password:** Password used in DES encryption. You must set this password when the user is created (even if privacy is not desired).
- **Update** button: Submits the form changes to the pending configuration.
- **Back** button: Returns to the **Administration > SNMP > USM Users** form without saving changes to this form.

Administration > SNMP > Advanced

Figure 8-50 shows the **Administration > SNMP > Advanced** form. Use this form to configure the source IP address to be used with SNMP traps generated from the firewall iSD.

Figure 8-50 Administration > SNMP > Advanced form



The **Administration > SNMP > Advanced** form contains the following information:

- **Source IP:** This drop-down menu lets you choose among the following options:
 - **Auto:** The IP address of the outgoing interface is used. This is the default.
 - **Unique:** The IP address of the individual firewall iSD is used.
 - **MIP:** The IP address of the cluster MIP is used. This setting is useful with applications (such as some versions of HP OpenView) that expect devices to be limited to only one IP address.
- **Update** button: Submits the form changes to the pending configuration.

Diagnostics forms

The Diagnostics sub-menu contains one item: “[Diagnostics > System Commands](#)” on page 290.

Diagnostics > System Commands

Figure 8-51 shows the **Diagnostics > System Commands** form. Use this form to execute Check Point system commands that would normally be entered in a command window. For more information about each command, refer to your Check Point user documentation.

Figure 8-51 Diagnostics > System Commands form

The screenshot shows the Alteon Switched Firewall web interface. The left sidebar contains navigation links: Monitor, Cluster, Network, Firewall, Operation, Administration, and Diagnostics. The main content area is titled 'System Commands' and contains the following information:

Execute System Command

Host IP: 47.184.54.202

Command: Check Point licenses (cplic print -x -t)

Submit Query

Result for "cplic print -x -t"

Type	Host	Expiration	Signature	Features
central	eval	1Apr2003	d9buCNLe9ApJ9yv3pgAqv8GbpmqxQM4LaGhp	CPMP-EVAL-1-DES-NG CK-CP

The **Diagnostics > System Commands** form contains the following information:

- Host IP: Displays the IP address of the selected firewall iSD host.
- Command: Displays the current command and allows you to choose from a list of commands to be executed on the firewall iSD host. When you have made a selection, click the **Submit Query** button and the system will extract the present diagnostic status for that command.
- Result: Displays the result of the query for the selected command.

The following Check Point system commands are available:

- Check Point connection table size (fw tab -t connection)
- Check Point connection table size summary (fw tab -t connections -s)
- Check Point interface list (fw ctl iflist)

- Check Point licenses (cplic print -x-t)
- Check Point memory statistics (fw ctl ptstat)
- Check Point policies (fw stat)
- Check Point version (fw ver)
- Current interfaces (ifconfig)
- Current processes (ps -aefH)
- Iptables information (iptables -L)



CHAPTER 9

Applications

This chapter describes the following applications of the firewall iSD:

- A second firewall iSD can be added to a cluster to create a high-availability (also known as active-standby) firewall configuration. The firewall iSD uses Virtual Router Redundancy Protocol (VRRP) to dynamically assign routing responsibility to the backup firewall iSD if the first firewall iSD fails (see [“High Availability firewall configuration” on page 299](#)).

NOTE – VRRP on the iSDs is a custom implementation that deviates from RFC 2338 in some details. For information on VRRP for the firewall iSD, see [page 294](#).

- Two iSDs can be synchronized to provide stateful failover of sessions. With synchronization, open sessions on a failed iSD are transparently reassigned to the backup (see [“Synchronizing firewall iSDs” on page 309](#)).

Virtual Router Redundancy Protocol

VRRP, as defined by RFC 2338, eliminates single point of failure by dynamically assigning responsibility for a virtual router to one of the physical routers on a LAN. The advantage is that VRRP provides a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

The VRRP router controlling the IP addresses associated with the virtual router is called the active master, and it forwards packets intended for these IP addresses. If the active master becomes unavailable, VRRP provides dynamic failover by forwarding responsibility to a redundant VRRP router. This lets the end-hosts use the virtual router (and the associated IP addresses) as the default first hop router, regardless of which VRRP router is active.

VRRP on the firewall iSDs

This section describes VRRP parameters you must configure to implement VRRP on the firewall iSDs.

Firewall iSD cluster and VRRP

A maximum of two firewall iSDs can be in a cluster. A cluster is created when a second firewall iSD is added to the first using the `join` command. Access the `join` command from the Setup menu, which appears when you first turn on an iSD host that has not been configured (see [“Initializing the firewall iSD” on page 44](#)). The general order for configuring redundant firewall iSDs is presented in [“Installing the redundant firewall iSD” on page 301](#).

VRRP master and backup

Clustered iSD hosts act as virtual routers in a redundant relationship using VRRP. In an HA configuration, only one firewall iSD passes traffic, while the redundant firewall iSD is a dedicated backup.

The iSD host with the higher IP address is the default master. The iSD host with the lower IP address is the default backup. Initially, the default master is active, that is, it assumes the ARP response and packet forwarding responsibilities for the virtual routers. The default backup is inactive, but it is available to take over if it detects a failure on the default master.

In all cases, the assumption of the active role is managed by the VRRP election process (see [“VRRP election” on page 297](#)). Once past the initialization stage, the role of active master is independent of the default condition.

VRRP messaging

Two firewall iSD hosts in a VRRP configuration communicate through VRRP packets. The purpose of the VRRP packet is to communicate the state of the active iSD host. VRRP packets are encapsulated in IP packets that are sent to the multicast group address (224.0.0.18) assigned to VRRP.

VRRP router parameters

VRRP router parameters are defined at either CLI menus or BBI forms.

VRRP settings

VRRP protocol parameters are defined globally at the CLI VRRP Settings Menu (see “[VRRP Settings Menu](#)” on page 188) or the **Network > VRRP** form in the BBI.

- `/cfg/net/vrrp/ha` enables high availability. You can apply the condition only if there are two iSD hosts in the cluster.
- `/cfg/net/vrrp/adint` sets the interval in seconds between advertisement messages, which are multicast to 224.0.0.18 from the active master's sub-address (see “[VRRP interface](#)” on page 296). If the backup does not receive advertisement messages at the specified interval, the VRRP failover process begins (see “[VRRP failover](#)” on page 297).

NOTE – A rule to allow VRRP multicast packets to and from the virtual router sub-addresses on both iSD hosts must be configured at the Check Point SmartDashboard. If the policy is not properly implemented, both hosts will assume the role of active master (see “[Example SmartDashboard configuration for HA](#)” on page 312).

- It can be necessary to increase the `adint` value during high traffic periods that prevent the active host from issuing advertisement messages at the specified interval. Increasing the `adint` value lowers the chance for unnecessary disruption of packet forwarding, but increases the length of service disruption in the event that the active master fails.
- Once the backup detects a failure in the active master, the backup immediately flashes a Gratuitous ARP (GARP) message to the end hosts on the virtual router interface. The GARP (an unsolicited ARP response) forces end hosts to update their ARP caches with the new MAC address/IP address mapping. Then the backup waits a period of time defined by the `/cfg/net/vrrp/garp` (GARP delay) value before sending continuous GARP messages at intervals defined by the `/cfg/net/vrrp/gbcast` (Gratuitous Broadcast) value. Continuous GARP messages prevent end hosts from aging out their ARP entries for the virtual router.

- The flash GARP message shortens the “black hole” period, that is, the time it takes a device to discover a lost neighbor. (One of the goals of a properly implemented VRRP backup strategy is to keep black hole periods short for end hosts.)
- Increasing the `gbcast` value cuts down on the GARP traffic, but lengthens the interval between end host ARP cache updates.

VRRP interface

Virtual router interface parameters are defined for each virtual router at the VRRP Interface Menu (see “[VRRP Interface Menu](#)” on page 187) or the **Network > Interfaces > Update (Add or Modify)** form in the BBI. Before you configure using either of these menus, you must first configure the interface IP parameters at the Interface Menu (see “[Interface Menu](#)” on page 185). Each virtual router interface requires the following parameters:

- a common virtual router IP address
- a common virtual router ID (`vrid`)
- two sub-addresses (one representing each firewall iSD host)
- a common port on each firewall iSD host

The IP address you enter for `addr1` at the Interface Menu becomes the virtual router IP address. Other real interface parameters, including the port, must be filled in, as well.

The `vrid` and sub-addresses (`ip1` and `ip2`) are defined on the same interface as the virtual router interface. These items are configured at the VRRP Interface Menu (see “[VRRP Interface Menu](#)” on page 187). The virtual router IP address and the sub-addresses must be unique, but all three IP addresses must belong to the same subnet.

Active master determination

VRRP ensures that one virtual router, or the other, assumes the role of active master. VRRP election, the process that determines the active master, occurs during initialization (that is, when HA is enabled for the cluster), or during host startup (see “[VRRP election](#)” on page 297). VRRP failover occurs when the backup fails to receive advertisement packets at preset intervals from each interface on the active master (see “[VRRP failover](#)” on page 297). Both processes ensure that only one iSD host is active at a time, and that it is able to communicate on the LAN.

VRRP election

At startup, the virtual routers on both firewall iSDs exist in the backup state and wait for advertisement packets. When none are received (only active masters broadcast advertisement packets), each virtual router assumes the active master role and both virtual routers begin broadcasting advertisement packets. Once it detects advertisement packets from the other master, the virtual router with the lower IP address (default backup) reverts to backup leaving the virtual router with the higher IP address (default master) as the active master.

The active master continuously broadcasts advertisement packets at regular intervals defined by the `adint` value. If advertisement packets are not received within the advertisement interval, VRRP failover begins on the backup.

Reasons that advertisement packets do not reach the backup include:

- active link is down
- port is down
- high traffic spreads advertisement packets beyond the specified `adint` interval
- a device on the virtual router LAN blocks the advertisement packets or ARP traffic

NOTE – VRRP can mishandle failures because of externally blocked multicast traffic. This results in both firewall iSDs assuming the active role. Backups do not block traffic.

VRRP failover

If VRRP multicast advertisement packets to group address 224.0.0.18 are not received by any virtual router on the backup, all of the backup virtual routers will send four ARP requests (one per second) to the active master virtual router IP addresses. If ARP replies from the active master are not received, failover occurs (the backup virtual router assumes the role of active master).

If ARP replies from the active master are received, no failover occurs.

The lack of response from the active master can also indicate that traffic is too heavy for the master to send advertisement packets within the `adint` window. If you believe this is the case, increase the `adint` value (see the `/cfg/net/vrrp/adint` command on [page 188](#)).

NOTE – When a virtual router comes up from the fault state, it will test for an active master by sending ARP requests. If the virtual router receives an ARP response, it will assume the role of backup. The backup will continue sending ARP messages to the virtual router until it does not receive a response. It will then initiate the failover process.

NOTE – MIP ownership is always assigned to the VRRP master. After a failover takes place, the SSI restarts to allow the MIP ownership to migrate to the new VRRP master. System error messages will appear at the CLI and the BBI until MIP migration completes. Also, attempts to change the cluster configuration will be impeded.

MAC address mapping

In HA mode, the active master uses its vrid to set a unique virtual router MAC address according to this formula: 0x00005E0001<vrid>. This is the address that the active master returns in response to end host ARP requests and Proxy ARP requests. GARP messages also contain the virtual router MAC address of the active master. Meanwhile, the backup retains its physical MAC address.

When the active master becomes the backup, it overwrites its virtual router MAC address with its physical MAC address. At the same time, the newly active master overwrites its physical MAC address with its unique virtual router MAC address.

NOTE – In practice, GARP messaging is typically the mechanism that informs switches and routers of MAC address changes.

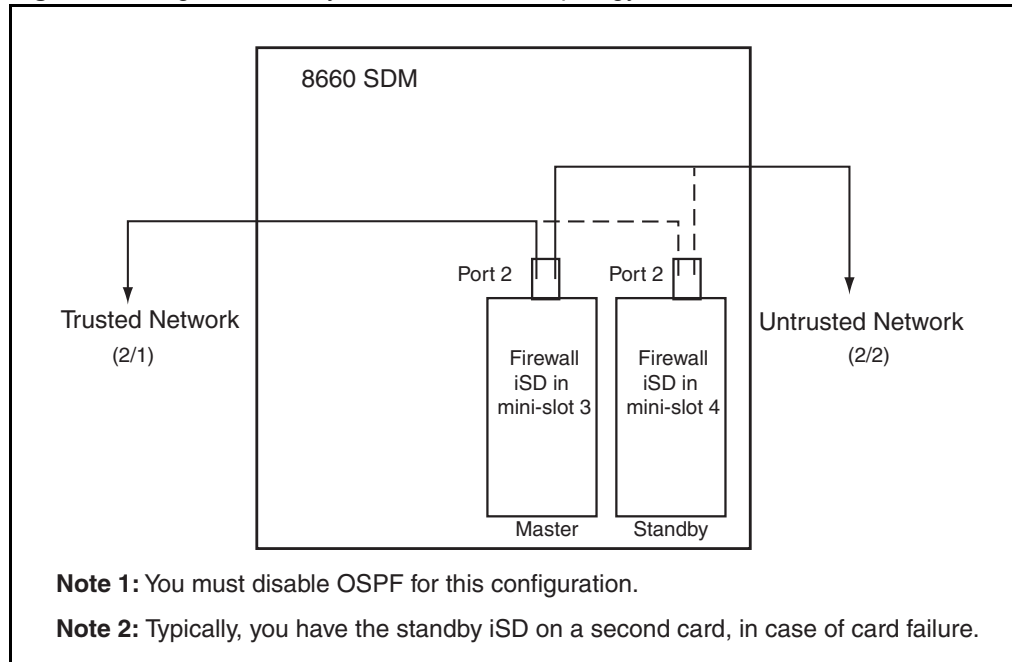
Stateful failover

Stateful failover is enabled globally at the Sync Configuration Menu (see “[Sync Configuration Menu](#)” on page 207) or the BBI **Firewall > Synchronization** form. When `/cfg/fw/sync` is enabled, the active master shares session state data with the backup. This allows sessions to continue on the backup when failover occurs. If `/cfg/fw/sync` is disabled, traffic is dropped at failover because the backup cannot find the existing session. This requires the client to reestablish the connection. Stateful failover requires a dedicated connection between firewall iSDs (see “[Synchronizing firewall iSDs](#)” on page 309).

High Availability firewall configuration

VRRP and the addition of a redundant firewall iSD to the cluster make it possible to configure an effective, HA network that reduces the chance that a single point of failure can bring down the system. The network topology for a typical HA network with firewall iSDs is shown in [Figure 9-1](#).

Figure 9-1 High-Availability firewall network topology



This example uses layer 2 switches to supply redundant feeds to the firewall iSD hosts (hubs may also be used for the same purpose). The default data path is through logical port 2 of the firewall iSD. The VRRP election process (see [“VRRP election”](#) on page 297) default-designates the host with the higher IP address (iSD in mini-slot 3, in this example) as the active master. If either link fails on the default path, the active master will stop sending VRRP advertisements and transition both virtual routers into a fault state. When the backup does not receive VRRP advertisements, it will initiate the VRRP failover process (see [“VRRP failover”](#) on page 297) and assume the role of active master.

The sync connection on port 2 supports stateful failover (see [“Synchronizing firewall iSDs”](#) on page 309 for configuration details), which is optional for HA networks.

Requirements

The installation of a redundant firewall iSD host is handled as an expansion that creates a firewall iSD cluster. The following conditions and equipment are required:

- A firewall iSD must be physically installed as described in *Installing the 8660 Service Delivery Module (SDM) for the 8600 Series Switch* (part number 217314-A).
- The firewall iSD must already be configured with basic parameters as described in [Chapter 2, “Initial setup,” on page 31](#).
- You must reinstall the software on the first firewall iSD host if you enabled the Check Point SmartCenter Server on it during initial setup (see [“Initializing the firewall iSD” on page 44](#)).
- The `/cfg/net/vrrp/ha` feature must be disabled on the first firewall iSD host before you add the second firewall iSD host. The ip1 address for each interface must also be configured on the first firewall iSD host before you add the second iSD host.
- You must be able to establish trust on both firewall iSDs (see [“Establishing trust on redundant iSDs” on page 308](#)).
- The redundant firewall iSD must be identical to the existing firewall iSD. You cannot mix different models or software versions in the same cluster.
- A layer 2 switch or hub is required to provide redundant network feeds to both iSD hosts. The switch or hub must have the ability to forward multicast packets.



CAUTION—Any firewall iSD being added must have the same version of Firewall OS as the other firewall iSD. See [Chapter 11, “Upgrading the software,”](#) for more information. Also, any firewall iSD being added must be set to the factory default mode. If moving a previously configured firewall iSD from another system, you must first delete the firewall iSD host from the old cluster to reset its configuration. For more information, see the `delete` command in the iSD Host menu on [page 153](#).

Installing the redundant firewall iSD

NOTE – This procedure applies to HA configuration.

1. **Ensure that the first firewall iSD is on and operational.**

NOTE – Ensure that `/cfg/net/vrrp/ha` is disabled at this point in the procedure.

2. **Install the redundant firewall iSD hardware, if necessary (see the *Installing the 8660 Service Delivery Module (SDM) for the 8600 Series Switch*).**
3. **Connect the power cable for the redundant firewall iSD, but do not turn it on yet.**
Attach power.
4. **Connect the redundant network feeds to the firewall iSDs.**

NOTE – Ensure that you connect each network to the same port/interface on both firewall iSDs.

Configuring the redundant firewall iSD

NOTE – This procedure applies to HA configuration.

1. **Log in as the administrator.**
2. **When the Setup Menu appears, select `join` and enter the basic configuration parameters, when prompted (see “[Using the join command](#)” on page 50).**
Enter a unique host IP address, but enter the same MIP you used for firewall iSD host 1.
3. **Reboot and log in to firewall iSD host 1 to complete the configuration (see “[Configuring VRRP on both firewall iSDs](#)” on page 302).**

NOTE – The Alteon Single System Image (SSI) maps the firewall iSD configuration across both firewall iSD hosts in the cluster. That is, whatever you had configured previously for firewall iSD host 1 is mapped to firewall iSD host 2. Any changes you add when logged into firewall iSD host 1 are mapped to firewall iSD host 2. This ensures that the configuration of both hosts is identical, a prerequisite for VRRP to work.

Note also that you must enter license information manually for each host, and that you must push policies to each host individually.

4. Enter the Check Point license:

```
>> # /cfg/pnp/add
Enter the IP Address: 192.168.1.5
Enter the Expiry date for the License :01Jun2004
Enter the Feature string :cpsuite-eval-3des-ng CK-GDWA5AB20H23
Enter the License string :aRkym9Dj6-zvcjsY4Ju-AUsq8FHvS-KrsakYosv
```

NOTE – You can also install licenses directly from the SmartCenter Server.

5. **Launch the Check Point SmartDashboard and configure HA** (see [“Configure HA at the Check Point SmartDashboard” on page 310](#)). This will allow you to manage the hosts as a cluster.
6. **(Optional) Configure synchronization** (see [Step 6 on page 314](#)).

Configuring VRRP on both firewall iSDs

The commands in this example use the parameters in [Figure 9-1 on page 299](#). Your configuration will differ, but it should observe the same configuration patterns as in the example.

NOTE – You must configure the vrid, ip1, and ip2 for each defined interface (except the Sync interface). Otherwise, HA will not work on any interface.

VRRP interface

NOTE – It is not necessary to configure `addr2` for HA mode.

1. **Log in to firewall iSD host 1 as the administrator and configure the virtual router interface:**

```
>> Main# /cfg/net/if 33/addr1 33.1.1.10
>> Main# /cfg/net/if 33/addr2 0.0.0.0
>> Main# /cfg/net/if 33/mask 255.255.255.0
>> Main# /cfg/net/if 33/port 2
>> Main# /cfg/net/if 33/ena
>> Main# /cfg/net/if 44/addr1 44.1.1.10
>> Main# /cfg/net/if 44/addr2 0.0.0.0
>> Main# /cfg/net/if 44/mask 255.255.255.0
>> Main# /cfg/net/if 44/port 2
>> Main# /cfg/net/if 44/ena
>> Main# /cfg/net/if 33/vlanid 33
>> Main# /cfg/net/if 44/vlanid 44
```

2. **Configure the VRRP sub-addresses.**

```
>> Main# /cfg/net/if 33/vrrp/ip1 33.1.1.11
>> Main# /cfg/net/if 33/vrrp/ip2 33.1.1.12
>> Main# /cfg/net/if 44/vrrp/ip1 44.1.1.11
>> Main# /cfg/net/if 44/vrrp/ip2 44.1.1.12
```

The VRRP sub-addresses must be on the same network as their virtual routers.

3. **Enter the vrid.**

```
>> Main# /cfg/net/if 33/vrrp/vrid 33
>> Main# /cfg/net/if 44/vrrp/vrid 44
```

Each virtual router interface gets a unique vrid, which is used to generate the virtual router MAC address (see [“MAC address mapping” on page 298](#)).

VRRP settings

VRRP settings are set globally for each firewall iSD.

1. Enable HA for the cluster:

```
>> Main# /cfg/net/vrrp/ha y
```

2. Set the adint, garp, gbcast, and phcintvl values.

```
>> Main# /cfg/net/vrrp/adint 10
>> Main# /cfg/net/vrrp/garp 1          default value
>> Main# /cfg/net/vrrp/gbcast 2       default value
>> Main# /cfg/net/vrrp/phcintvl 2    default value
```

3. Apply the changes.

```
>> Main# apply
```

Sync interface settings (optional)

The optional Sync interface requires a dedicated port on both firewall iSDs and a local connection. Its configuration differs from the other virtual router interfaces in that `/cfg/net/if #/addr1` and `/cfg/net/if #/addr2` are both set to 0.0.0.0. For additional information on the Sync interface, see [“Synchronizing firewall iSDs” on page 309](#).

1. Configure the virtual router interface and enable interface for the sync network.

```
>> Main# /cfg/net/if 192/addr1 0.0.0.0
>> Main# /cfg/net/if 192/addr2 0.0.0.0
>> Main# /cfg/net/if 192/mask 255.255.255.0
>> Main# /cfg/net/if 192/vlanid 5
>> Main# /cfg/net/if 192/port 2
>> Main# /cfg/net/if 192/ena y
```

NOTE – You must enter 0.0.0.0 for `addr1` and `addr2` for the feature to work properly.

NOTE – The Sync VLAN must have the lowest VLAN ID of any configured on the firewall iSD.

2. Configure the VRRP sub-addresses and vrid for the sync network.

```
>> Main# /cfg/net/if 192/vrrp/vrid 192
>> Main# /cfg/net/if 192/vrrp/ip1 192.168.1.1
>> Main# /cfg/net/if 192/vrrp/ip2 192.168.1.2
```


3. Enable synchronization and apply the changes.

```
>> Main# /cfg/fw/sync/ena           Enable synchronization
>> Main# apply
```

The following is the configuration dump for the active master and backup in [Figure 9-1 on page 299](#):

```
>> Main# /cfg/dump
/cfg
/cfg/sys
/cfg/sys/time
    tzone "America/Los_Angeles"
/cfg/sys/time/ntp
/cfg/sys/dns
/cfg/sys/cluster
    mip 10.10.1.33
/cfg/sys/cluster/host 1
    ip 10.10.1.193
/cfg/sys/cluster/host 2
    ip 10.10.1.194
/cfg/sys/accesslist
/cfg/sys/adm
    idle 10m
/cfg/sys/adm/telnet
    ena n
/cfg/sys/adm/ssh
    ena n
/cfg/sys/adm/web
/cfg/sys/adm/web/http
    port 80
    ena y
/cfg/sys/adm/web/ssl
    port 443
    ena n
    tls y
    sslv2 y
    sslv3 y
/cfg/sys/adm/web/ssl/certs
/cfg/sys/adm/web/ssl/certs/serv
/cfg/sys/adm/web/ssl/certs/ca
/cfg/sys/adm/snmp
    ena n
    model v2c
    level auth
        access d
    events n
    alarms n
        rcomm public
/cfg/sys/adm/snmp/users
/cfg/sys/adm/snmp/hosts
/cfg/sys/adm/snmp/system
/cfg/sys/adm/snmp/adv
    trapsrcip auto
/cfg/sys/log
    srcip auto
    debug n
```

```

/cfg/sys/log/syslog
/cfg/sys/log/ela
    ena n
    addr 0.0.0.0
    sev err
/cfg/sys/log/arch
    email none
    smtp 0.0.0.0
    int "1, 0"
    size 0
/cfg/sys/user
    expire 0
/cfg/net
/cfg/net/port 1
    name "Host Port"
    autoneg on
    speed 0
    mode full
/cfg/net/port 2
    name none
    autoneg on
    speed 0
    mode full
/cfg/net/port 3
    name none
    autoneg on
    speed 0
    mode full
/cfg/net/if 33
    addr1 33.1.1.10
    addr2 0.0.0.0
    mask 255.255.255.0
    vlanid 33
    port 2
    ena y
/cfg/net/if 33/vrrp
    vrid 33
    ip1 33.1.1.11
    ip2 33.1.1.12
/cfg/net/if 44
    addr1 44.1.1.10
    addr2 0.0.0.0
    mask 255.255.255.0
    vlanid 44
    port 2
    ena y
/cfg/net/if 44/vrrp
    vrid 44
    ip1 44.1.1.11
    ip2 44.1.1.12
/cfg/net/if 192
    addr1 0.0.0.0
    addr2 0.0.0.0
    mask 255.255.255.0
    vlanid 5
    port 2
    ena y
/cfg/net/if 192/vrrp
    vrid 192
    ip1 192.168.1.1
    
```

(*Sync interface*)

```

        ip2 192.168.1.2
/cfg/net/vrrp
    ha y
    aa n
    adint 10
    garp 1
    gbcast 2
/cfg/net/adv
/cfg/net/adv/route
    gateway 172.25.3.23
/cfg/net/adv/route/ospf
    rtrid 0.0.0.0
    spf "5, 10"
    ena n
/cfg/net/adv/route/ospf/if 33 (Identical /cfg/../../ospf configurations for if 33 and if 44)
    aindex 1
    prio 0
    cost none
    hello 10
    dead 40
    trans 1
    retra 5
    auth none
    md5key "1, "
    ena n
/cfg/net/adv/route/ospf/redirect
/cfg/net/adv/route/ospf/redirect/connected
    metric "10, t1"
    ena n
/cfg/net/adv/route/ospf/redirect/static
    metric "10, t1"
    ena n
/cfg/net/adv/route/ospf/redirect/defaultgw
    metric "10, t1"
    ena n
/cfg/net/adv/route/routes
/cfg/net/adv/parp
    enable y
/cfg/net/adv/parp/list
/cfg/pnp
/cfg/fw
    ena y
/cfg/fw/sync
    ena y
/cfg/fw/client
/cfg/misc
    warn y

```

Establishing trust on redundant iSDs

The ability to establish trust (SIC) on redundant firewall iSDs is required to push policies to the firewall iSDs from the Check Point SmartCenter Server. If your management station is on a different network from the firewall iSD host network, static routes must be added. In the example that follows, the management station is behind the firewall (a common strategy) on the same network as the virtual router interface (see [Figure 9-1 on page 299](#)).

1. **Open a DOS window on the management station and enter a static route between ip1 and the firewall iSD host #1 IP address. (For this example, the management station interface IP address is 10.10.1.200. Use the ip1 IP address as the gateway):**

```
C:\ route add 10.10.1.193 mask 255.255.255.255 33.1.1.12 -p
                ^destination      ^mask          ^gateway
```

2. **Enter a static route between ip2 and the iSD host #2 IP address (Use the ip2 IP address as the gateway):**

```
C:\ route add 10.10.1.194 mask 255.255.255.255 33.1.1.13 -p
```

3. **At the local console, add the management station IP address to the cluster access list:**

```
>> Main# /cfg/sys/accesslist/add
Enter network address: 10.10.1.200      Management station IP address
Enter netmask: 255.255.255.0
>> Main# apply                          Applies data to both iSD hosts
```

4. **From the management station DOS window, ping both firewall iSD hosts:**

```
C:\WINNT\system32>ping 10.10.1.193
Pinging 10.10.1.193 with 32 bytes of data:
Reply from 10.10.1.193: bytes=32 time<10ms TTL=25
C:\WINNT\system32>ping 10.10.1.194
Pinging 10.10.1.194 with 32 bytes of data:
Reply from 10.10.1.194: bytes=32 time<10ms TTL=25
```

5. **From the Check Point SmartDashboard, establish trust with both firewall iSDs (iSD host #1 and iSD host #2). See [“Establishing Secure Internal Communication” on page 79](#).**

Synchronizing firewall iSDs

Sessions running through firewall iSDs can be synchronized to provide stateful failover. With session state synchronization, if the active firewall iSD fails, the open sessions will be transparently reassigned to the backup firewall iSD.

You must configure synchronization using the CLI (see [“Configuring synchronization using the CLI” on page 309](#)) and the Check Point SmartDashboard (see [Step 6 on page 314](#)). The VRRP features and the virtual router must also be configured (see [“Configuring VRRP on both firewall iSDs” on page 302](#)).

Synchronization will impair system performance if traffic includes many short-lived sessions. Enable synchronization only for services that can benefit from it (such as Telnet) and not for services that cannot (such as http).

Configuring synchronization using the CLI

1. **Configure the Sync interfaces** (see example in [“Sync interface settings \(optional\)” on page 304](#)).
2. **Test the Sync network** (test initiated on example host #2).

```

>> Main# /maint/diag/fw/sync
Testing SFD : 10.10.1.193                               Example Host 1 IP
  SFD : UP. Test starting...
  10.10.1.194->10.10.1.193
  Communication OK.
Testing SFD : 10.10.1.194                               Example Host 2 IP
  SFD : UP. Test starting...
  Local Sync Address 10.10.1.194 OK.

```

3. **From the Check Point SmartDashboard, update the firewall interface information.**
See [Step 6 on page 314](#).
4. **From the Check Point SmartDashboard, re-install the security policies on both firewall iSDs.**

Configure HA at the Check Point SmartDashboard

Before you begin, ensure you have completed the following tasks:

- Ensure you can ping both firewall iSD hosts from the management station.
- Ensure you can establish trust with both firewall iSD hosts and push policies to the cluster.
- Deselect automatic ARP configuration for HA configurations before you push policies for the first time. Otherwise, the Proxy ARP module will not work properly.

To configure HA at the Check Point SmartDashboard:

1. **Start the Check Point SmartDashboard application on your SMART Client.**
2. **Create two new Check Point Gateway objects (Type: Gateway) in the General page of the Check Point Gateway window.**
3. **Establish trust with both firewall iSD hosts, if you have not done so already.**
4. **Click Get Interfaces on the Topology page to retrieve the interfaces for the new Check Point Gateways.**
5. **Create a new Gateway Cluster on the General page of the Gateway Cluster Properties window.**
6. **Add the Check Point Gateways (configured in Step 2) to the cluster on the Cluster Members page.**
7. **Configure state synchronization (see [Step 6 on page 314](#)) on the Synchronization page of the Gateway Cluster Properties window.**
8. **Add interface properties for each VRRP interface (addr1 and addr2) on the Topology page of the Gateway Cluster Properties window.**

NOTE – Addr2 applies only to Active-Active configurations, which are not currently supported on the 8660 SDM firewall modules.

9. **Go to Policy > Global Properties > NAT - Network Address Translation.**
10. **Deselect Automatic ARP Configuration.**
11. **Add a rule to allow advertisement messages (multicast packets) between redundant firewall iSDs and another rule to allow VRRP traffic.**
 - a. Create a node with IP address 224.0.0.18 (multi-cast address). See [Figure 9-2 on page 311](#).
 - b. Create two rules (see [Figure 9-3 on page 311](#)):
 - Rule 1 permits multicast packets

- Rule 2 permits inter-firewall traffic.

NOTE – If this rule is not properly implemented, both hosts will assume the role of active master (see “VRRP settings” on page 295).

Figure 9-2 Host Node - vrrp-multicast window

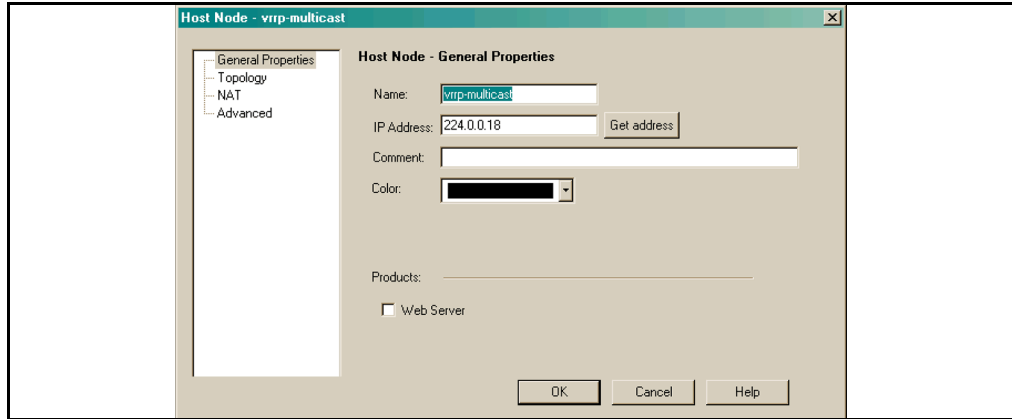
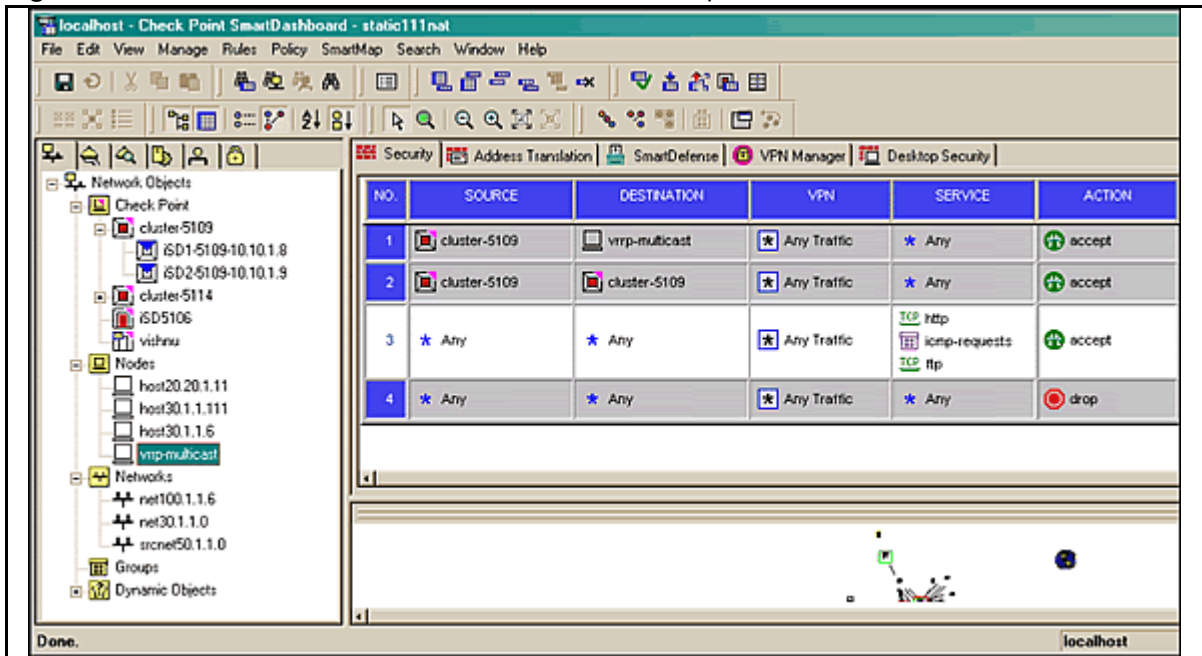


Figure 9-3 Rules 1 and 2 allow VRRP traffic and multicast packets



12. Turn on high availability as needed at the CLI (see “/cfg/net/vrrp” on page 188).
13. Push policies again.

Example SmartDashboard configuration for HA

The following procedure expands on the general steps presented in “Configure HA at the Check Point SmartDashboard” on page 310. Network data (in parenthesis) is consistent with the example cluster in Figure 9-1 on page 299.

NOTE – This procedure was created for NG with Application Intelligence.

1. Create a Gateway Check Point object:

- a. Open the **Network Objects** folder in the **Network Objects** pane (left pane).
- b. Right-click on the Check Point icon.
- c. Select **New Check Point > Gateway...**
- d. Select **Classic mode**.

The **Check Point Gateway** window opens.

- e. Select the **General Properties** option and enter the following data for first host:
 - Enter a name and host IP address (EC-1 and 10.10.1.193 for Host 1 and EC-2 and 10.10.1.194 for Host 2)

NOTE – Host is a reserved word and spaces are not allowed in object names.

- Comment, Color (optional)
- Version: (**NG with Application Intelligence**)
- Select **Firewall**
- Establish SIC (click the **Communication...** button and enter the **Activation Key** on the **Communication** window.

2. Retrieve the interfaces for the new Check Point Gateway:

- a. Select the **Topology** option.
- b. Click the **Get...** button
- c. Select **Interfaces**.

This retrieves the interface data that you configured on the host. The names (eth0, eth1, eth2) are set automatically by the firewall OS.

- d. Select an interface.
- e. Click the **Edit...** button.
- f. Select the **Topology** tab (if necessary, deselect **Cluster Interface** on the **General** tab to expose the **Topology** tab).
- g. Edit the topology.
If this interface leads to the internet, check **External**, **Anti-Spoofing**, and **Log**. If this interface leads to a local network, check **Internal**, **Anti-Spoofing**, and **Log**.
- h. Click **OK**.
- i. Repeat Step 2 for all retrieved interfaces.

3. Repeat Step 1 and Step 2 for the second host.

4. Create a new Gateway Cluster object:

- a. Right-click on the Check Point icon in the **Network Objects** pane.
- b. Select **New Check Point > Gateway Cluster...**
The **Gateway Cluster Properties** window opens.
- c. Select the **General Properties** option and enter the following data for the cluster:
 - Enter a name and MIP address (for example, enter “Example-Cluster” for the name and “10.10.1.33” for the MIP address).
 - Comment, Color (optional)
 - Version: (**NG with Application Intelligence**)
 - Select **Firewall**

NOTE – When you have finished adding the Gateway Cluster object, do *not* click **OK**, but go directly to Step 5 instead.

5. Add the Check Point Gateways to the Gateway Cluster object:

- a. Select the **Cluster Members** option.
- b. Click the **Add...** button.
- c. Select **Add Gateway to Cluster...**

The **Add Gateway to Cluster** window opens.

- d. Select the two Check Point Gateway objects and click **OK**.

NOTE – When you have finished adding the Gateway Cluster object, do *not* click **OK**, but go directly to Step 6 instead.

6. Configure State Synchronization:

- a. Select the **Synchronization** option.
- b. Select **Use State Synchronization**.
- c. Click the **Add** button.
- d. Enter the Synchronization data as follows:
 - Name (SyncNetwork)
 - Network Address: (192.168.1.0)
 - Network Mask: (255.255.255.0)

NOTE – The **Use State Synchronization** checkbox is selected by default. If you choose to not use this feature, deselect the box. If synchronization is not enabled, existing connections will be closed when failover occurs.

NOTE – When you have finished adding the Gateway Cluster object, do *not* click **OK**, but go directly to Step 7 instead.

7. Add interface properties for each VRRP interface:

NOTE – For HA, only addr1 is configured.

- a. Select the **Topology** option and add the interface properties for each interface:
 - Select the **Add** button.
The **Interface Properties** window opens.
 - Select the **General** Tab and enter a name, IP Address, and network mask for a VRRP interface you have configured on the firewall iSD.
 - Select the **Topology** tab
 - Edit the topology.

If this interface leads to the internet, select **External** and click **OK**. If this interface leads to local networks, check **Internal** and **Network defined by the interface IP and Net Mask**, and click **OK**.

Table 9-1 show the data for the HA example cluster in Figure 9-1 on page 299.

Table 9-1 Topology Data for Example Cluster (HA)

Name	IP Address	Network Mask	IP Addresses behind interface
Untrusted addr1	44.1.1.10	255.255.255.0	External
Trusted addr1	33.1.1.10	255.255.255.0	This Network

b. Click **OK**. This completes the configuration of the Gateway Cluster object.

8. Configure Automatic ARP:

a. Select **Policy > Global Properties** at the SmartDashboard menu.

The Global Properties window opens.

b. Select the **NAT - Network Address Translation** option.

c. Select the following:

— Allow bi-directional NAT

— Translate destination on client side for Automatic and Manual NAT

d. Ensure that **IP Pool NAT** is deselected.

9. Push policies to the cluster and reboot both hosts.



CHAPTER 10

Open Shortest Path First

The 8660 SDM supports the Open Shortest Path First (OSPF) routing protocol. This implementation conforms to the OSPF version 2 specifications detailed in Internet RFC 1583. The following sections discuss current OSPF support:

- “OSPF overview” on page 317.
- “Firewall OSPF implementation” on page 322.
- “OSPF configuration examples” on page 327.

OSPF overview

OSPF is designed for routing traffic within a single IP domain called an Autonomous System (AS). The AS can be divided into smaller logical units known as *areas*.

All routing devices maintain link information in their own Link State Database (LSDB). The LSDB for all routing devices within an area is identical, but is not exchanged between different areas. Only routing updates are exchanged between areas, significantly reducing the overhead for maintaining routing information on a large, dynamic network.

The following sections describe key OSPF concepts:

- “Types of OSPF areas” on page 318
- “Types of OSPF routing devices” on page 319
- “Neighbors and adjacencies” on page 319
- “Link-State Database” on page 320
- “Shortest Path First tree” on page 320
- “Authentication” on page 321
- “Internal and external routing” on page 321

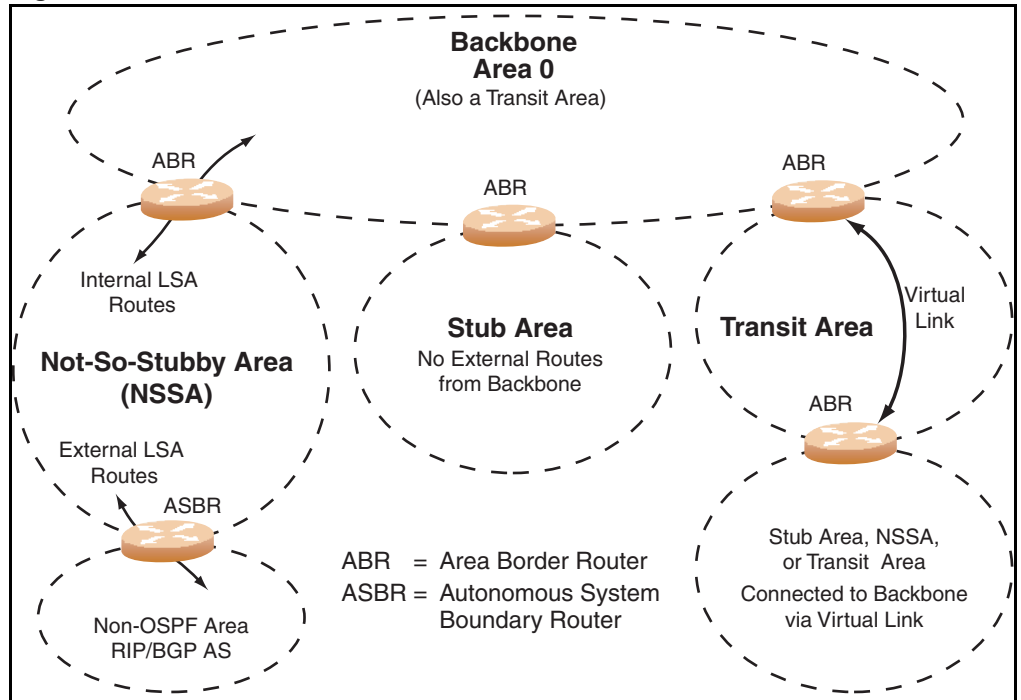
Types of OSPF areas

An AS is broken into logical units called “areas”. In any AS with multiple areas, one area must be designated as area 0, also known as the “backbone”. The backbone is the central OSPF area. All other areas in the AS must be connected to the backbone. Areas inject summary routing information into the backbone, which then distributes it to other areas as needed.

As shown in **Figure 10-1**, OSPF defines the following types of areas:

- **Stub Area**—an area that is connected to only one other area. External route information is not distributed into stub areas.
- **Not-So-Stubby-Area (NSSA)**—similar to a stub area with additional capabilities. Routes originating from within the NSSA can be propagated to adjacent transit and backbone areas. External routes from outside the AS can be advertised within the NSSA, but are not distributed into other areas.
- **Transit Area**—an area that allows area summary information to be exchanged between routing devices. The backbone (area 0), and any area that is not a stub area or an NSSA, are considered transit areas.

Figure 10-1 OSPF areas

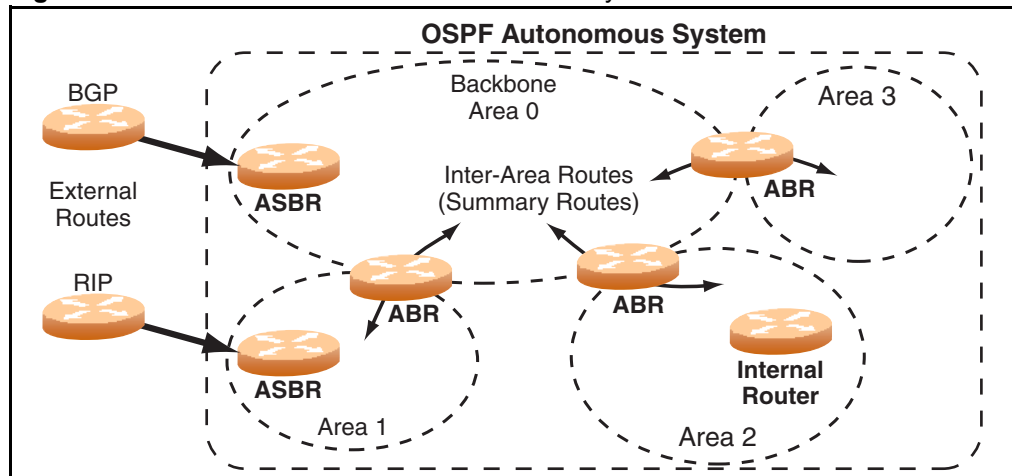


Types of OSPF routing devices

As shown in [Figure 10-2](#), OSPF uses the following types of routing devices:

- Internal Router (IR)—a router that has all of its interfaces within the same area. IRs maintain LSDBs identical to those of other routing devices within the local area.
- Area Border Router (ABR)—a router that has interfaces in multiple areas. ABRs maintain one LSDB for each connected area, and disseminate routing information between areas.
- Autonomous System Boundary Router (ASBR)—a router that acts as a gateway between the OSPF domain and non-OSPF domains, such as RIP, BGP, and static routes.

Figure 10-2 OSPF domain and an Autonomous System



Neighbors and adjacencies

In areas with two or more routing devices, “neighbors” and “adjacencies” are formed.

Neighbors are routing devices that maintain information about each other’s health. To establish neighbor relationships, routing devices periodically send “hello” packets on each of their interfaces. All routing devices that share a common network segment, that appear in the same area, and that have the same health (hello intervals and dead intervals) and authentication parameters respond to each other’s hello packets and become neighbors. Neighbors continue to send periodic hello packets to advertise their health to neighbors. In turn, they listen to hello packets to determine the health of their neighbors and to establish contact with new neighbors.

Adjacencies are neighbors that exchange OSPF database information. To limit the number of database exchanges, not all neighbors in an area (IP network) become adjacent to each other. Instead, the hello process is used for electing one of the neighbors as the area’s Designated Router (DR) and one as the area’s Backup Designated Router (BDR).

The DR is adjacent to all other neighbors and acts as the central contact for database exchanges. Each neighbor sends its database information to the DR, which relays the information to the other neighbors.

The hello process also elects a BDR because of the overhead required for establishing a new DR in the case of failure. The BDR is adjacent to all other neighbors (including the DR). Each neighbor sends its database information to the BDR just as with the DR, but the BDR merely stores this data, and does not distribute it. If the DR fails, the BDR will take over the task of distributing database information to the other neighbors.

Link-State Database

OSPF is a link-state routing protocol. A “link” represents an interface (or routable path) from the routing device. By establishing an adjacency with the DR, each routing device in an OSPF area maintains an identical LSDB describing the network topology for its area.

Each routing device transmits a Link-State Advertisement (LSA) on each of its interfaces. LSAs are entered into the LSDB of each routing device. OSPF uses “flooding” to distribute LSAs between routing devices.

When LSAs result in changes to the routing device's LSDB, the routing device forwards the changes to the adjacent neighbors (the DR and BDR) for distribution to other neighbors.

OSPF routing updates occur only when changes occur, rather than periodically. If an adjacency is interested in a new route that has been added (for example, if configured to receive static routes and the new route is indeed static), an update message containing the new route is sent to the adjacency. If a route is removed from the route table, and the route had already been sent to an adjacency, an update message containing the route to withdraw is sent.

Shortest Path First tree

The routing devices use a link-state algorithm (Dijkstra's algorithm) to calculate the shortest path to all known destinations, based on the cumulative cost required to reach the destination.

The cost of an individual interface in OSPF is an indication of the overhead required to send packets across it. The cost is inversely proportional to the bandwidth of the interface. A lower cost indicates a higher bandwidth.

Authentication

OSPF also allows packet authentication and uses IP multicast when sending and receiving packets. This ensures less processing on routing devices that are not listening to OSPF packets.

Internal and external routing

To ensure effective processing of network traffic, every routing device on your network needs to know how to send a packet (directly or indirectly) to any other location or destination in your network. This is referred to as “internal routing” and can be done with static routes or using active internal routing protocols, such as OSPF, RIP, or RIPv2.

It is also useful to tell routers outside your network (upstream providers or “peers”) about the routes to which you have access in your network. Sharing of routing information between autonomous systems is known as “external routing”.

Typically, an AS will have one or more border routers (peer routers that exchange routes with other OSPF networks), as well as an internal routing system enabling every router in that AS to reach every other router and destination within that AS.

When a routing device advertises routes to boundary routers on other autonomous systems, it is effectively committing to carry data to the IP space represented in the route being advertised. For example, if the routing device advertises 192.204.4.0/24, it is declaring that if another router sends data destined for any address in the 192.204.4.0/24 range, it will carry that data to its destination.

Firewall OSPF implementation

The following sections describe issues specific to OSPF implementation in the firewall iSD:

- “Configurable parameters” on page 322
- “Defining areas” on page 323
- “Interface cost” on page 325
- “Electing the DR and BDR” on page 325
- “Router ID” on page 326
- “Authentication” on page 326
- “OSPF features not supported in this release” on page 327

Configurable parameters

In the firewall iSD, OSPF parameters can be configured through the CLI or BBI.

The CLI supports the following parameters:

- interface output cost
- interface priority
- dead and hello intervals
- retransmission interval
- interface transmit delay

In addition, you can specify the Shortest Path First (SPF) interval, that is, the time interval between successive calculations of the shortest path tree using Dijkstra's algorithm.

Defining areas

If you are configuring multiple areas in your OSPF domain, one of the areas must be designated as area 0, known as the backbone. The backbone is the central OSPF area and is usually physically connected to all other areas. The areas inject routing information into the backbone, which, in turn, disseminates the information into other areas.

Since the backbone connects the areas in your network, it must be a contiguous area.

NOTE – Virtual links are not supported by the firewall iSD. Backbone partitioning, which requires virtual links to ensure that all parts of the AS are reachable, is also not supported by the firewall iSD.

Up to 17 OSPF areas (0-16) can be connected to a firewall iSD cluster. To configure an area, the OSPF number must first be defined, then attached to a network interface on the firewall iSD. The full process is explained in the following sections:

- “Assigning the area index” on page 323
- “Using the area ID to assign the OSPF area number” on page 324
- “Attaching an area to a network” on page 324

An OSPF area is defined by assigning two pieces of information—an area index and an area ID. The command to define an OSPF area is as follows:

```
>> # /cfg/net/adv/route/ospf/aindex <area index>/id <area ID number>
```

NOTE – The `aindex` option is an arbitrary index used only on the firewall iSD and does not represent the actual OSPF area number. The actual OSPF area number is defined in the `id` portion of the command. See “Assigning the area index” on page 323.

Assigning the area index

The `aindex <area index>` option is actually just an arbitrary index (1-16) used only by the firewall iSD. This index does not necessarily represent the OSPF area number.

For example, the following commands define OSPF area 1 because that information is held in the area ID portion of the command, even though the arbitrary area indexes do not agree with the area IDs:

```
>> # /cfg/net/adv/route/ospf/aindex 2/id 0.0.0.1(Use index 2 to set area 1)
```

NOTE – The backbone area 0 (aindex 1) is automatically configured as a transit area with `id 0.0.0.0`.

Using the area ID to assign the OSPF area number

The OSPF area number is defined in the `id <IP address>` option. The octet format is used to be compatible with two different systems of notation used by other OSPF network vendors. There are two valid ways to designate an area ID:

- Placing the area number in the last octet (0.0.0.n)

Most common OSPF vendors express the area ID number as a single number. For example, the Cisco IOS-based router command `network 1.1.1.0 0.0.0.255 area 1` defines the area number simply as `area 1`. On a firewall iSD, using the last octet in the area ID, `area 1` is equivalent to `id 0.0.0.1`.

- Multi-octet (IP address)

Some OSPF vendors express the area ID number in multi-octet format. For example, `area 2.2.2.2` represents OSPF area 2, and can be specified directly on a firewall iSD as `id 2.2.2.2`.

NOTE – Although both types of area ID formats are supported, ensure that the area IDs are in the same format throughout an area.

Attaching an area to a network

Once an OSPF area has been defined, it must be associated with a network. To attach the area to a network, you must assign the OSPF area index to an IP interface that participates in the area. The format for the command is as follows:

```
>> # /cfg/net/adv/route/ospf/if <interface number>/aindex <area index>
```

For example, the following commands could be used to configure IP interface 14 for a presence on the 10.10.10.1/24 network, to define OSPF area 1 using index 2 on the firewall iSD, and to attach the area to the network:

```
>> # /cfg/net/if 14                (Select menu for IP interface 14)
>> Interface 14# addr1 10.10.10.1  (Define IP address on the backbone)
>> Interface 14# ena                (Enable IP interface 14)
>> Interface 14# ../route/ospf/aindex 2 (Select menu for area index 2)
>> OSPF Area Index 2 # id 0.0.0.1   (Define area ID as OSPF area 1)
>> OSPF Area Index 2 # ena          (Enable area index 2)
>> OSPF Area Index 2 # ../if 14     (Select OSPF menu for interface 14)
>> OSPF Interface 14# aindex 2     (Attach area to network interface 14)
>> OSPF Interface 14# ena          (Enable interface 14 for area index 2)
```

Interface cost

The OSPF link-state algorithm (Dijkstra's algorithm) places each routing device at the root of a tree and determines the cumulative cost required to reach each destination. Usually, the cost is inversely proportional to the bandwidth of the interface. Low cost indicates high bandwidth. You can manually enter the cost for the output route with the following commands:

```
>> # /cfg/net/adv/route/ospf/if <interface number>
>> # cost <cost value (1-65535)>
```

Electing the DR and BDR

In any area with more than two routing devices, a DR is elected as the central contact for database exchanges among neighbors, and a BDR is elected in case the DR fails.

DR and BDR elections are made through the hello process. The election can be influenced by assigning a priority value to the OSPF interfaces. The commands are as follows:

```
>> # /cfg/net/adv/route/ospf/if <interface number>
>> # prio <priority value (0-255)>
```

A priority value of 255 is the highest, and 1 is the lowest. A priority value of 0 specifies that the interface cannot be used as a DR or BDR. If there are two routing devices with identical priority values, the routing device with the lowest router ID becomes the DR.

Router ID

Routing devices in OSPF areas are identified by a router ID. The router ID is expressed in IP address format. The IP address of the router ID is not required to be included in any IP interface range or in any OSPF area.

The router ID can be configured in one of the following two ways:

- Statically—Use the following command to manually configure the router ID:

```
>> # /cfg/net/adv/route/ospf/rtrid <IP address>
```

- Dynamically—OSPF protocol configures the lowest IP interface IP address as the router ID. This is the default. To use a dynamic router ID after having set it statically, set the router ID to 0.0.0.0 and reboot the firewall iSD.

Authentication

OSPF protocol exchanges are authenticated so that only trusted devices can participate. The firewall iSDs support simple authentication (type 1 plain text passwords) and MD5 authentication (encrypted data and passwords) among neighboring routing devices in an area.

Simple authentication

OSPF simple passwords are configured and enabled individually for each defined interface. The plain text passwords are up to eight characters long.

For interfaces, the following CLI commands are used:

```
>> # /cfg/net/adv/route/ospf/if <interface number> (Select OSPF interface)
>> OSPF Interface# auth password|none (Set simple authentication on/off)
>> OSPF Interface# key <password> (Set type 1 password)
```

MD5 authentication

OSPF MD5 passwords use strong cryptographic to protect data and passwords. To preserve security, MD5 passwords should be changed frequently.

MD5 passwords are configured and enabled individually for each defined interface. MD5 passwords are defined with a key ID (1-255) and a password with up to 16 characters.

For interfaces, the following CLI commands are used:

```
>> # /cfg/net/adv/route/ospf/inf <interface number>(Select OSPF interface)
>> OSPF Interface# auth md5|none (Set MD5 on/off)
>> OSPF Interface# md5key <key ID> <password>(Set MD5 ID & password)
```

OSPF features not supported in this release

The following OSPF features are not supported in this release:

- Filtering OSPF routes
- Load balancing equal cost routes

During traffic forwarding, if the first configured equal cost route is deleted, the next configured equal cost route is selected.
- Using OSPF to forward multicast routes
- Virtual links

OSPF configuration examples

A summary of the basic steps for configuring OSPF on a firewall iSD follows. See [“Example 1: simple OSPF domain” on page 328](#) for detailed instructions related to each of the following steps:

1. Configure IP interfaces.

One IP interface is required for each desired network (range of IP addresses) that is assigned to an OSPF area on the firewall iSD.

2. Enable OSPF on the firewall iSD.

3. Define the OSPF areas.

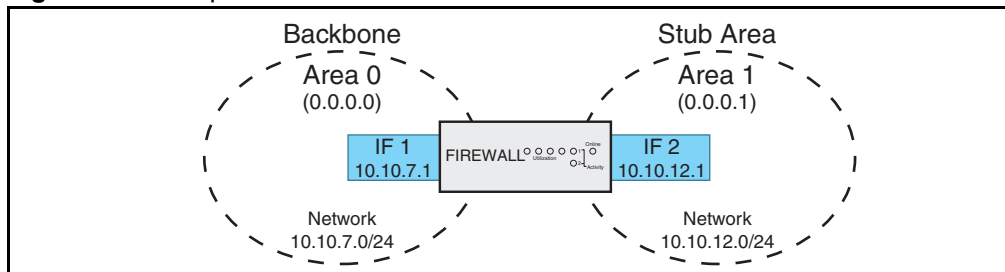
4. Configure OSPF interface parameters.

IP interfaces are used for attaching networks to the various areas.

Example 1: simple OSPF domain

In this example, two OSPF areas are defined—one area is the backbone and the other is a stub area (see Figure 10-3). A stub area does not allow advertisements of external routes, and so reduces the size of the database. Instead, a default summary route of IP address 0.0.0.0 is automatically inserted into the stub area. Any traffic for IP address destinations outside the stub area will be forwarded to the stub area's IP interface, and then into the backbone

Figure 10-3 Simple OSPF Domain



Configuring a single firewall iSD with OSPF

For the 8600 configuration, assume the following:

- VLAN 20 is untrusted and VLAN 30 is trusted.
- firewall iSD is in cluster 1
- cluster is already created
- NAAP already created

You will create two VLANS, then add the user ports to the VLAN.

Create VLAN 20

Use the following commands to create VLAN 20:

```
config vlan 20 create byport 1 firewall-vlan cluster 1
config vlan 20 ports add 2/2
```

Create VLAN 30

Use the following commands to create VLAN 30:

```
config vlan 30 create byport 1 firewall-vlan cluster 1
config vlan 30 ports add 2/1
```

NOTE – Firewall iSD logical port 2 (on the 8600, Slot 3, logical port 8) is automatically added to the VLAN because the firewall iSD was defined in cluster 1.

Passport-8610:5# show vlan info ports 20

```
=====
```

Vlan Port			
VLAN PORT	ACTIVE	STATIC	NOT_ALLOW
ID MEMBER	MEMBER	MEMBER	MEMBER

20	3/8		3/8

Firewall iSD configuration

Create vlan 20:

```
/cfg/net/if 20
addr1 20.20.20.1
mask 24
vlan 20
port 2
en
apply
```

Create vlan 30:

```
/cfg/net/if 30
addr1 30.30.30.1
mask 24
vlan 20
en
apply
```

Enable OSPF:

```
/cfg/net/adv/route/ospf en
```

Enable OSPF on each of the interfaces:

```

/cfg/net/adv/route/ospf/if 20
en

/cfg/net/adv/route/ospf/if 30
en

apply

```

Configuring OSPF support

To configure OSPF support as shown in [Figure 10-3](#), use the following steps:

1. Configure IP interfaces on each network that will be attached to OSPF areas.

In this example, two IP interfaces are needed: one for the backbone network on 10.10.7.0/24 and one for the stub area network on 10.10.12.0/24.

>> # /cfg/net/if 1	<i>(Select menu for IP interface 1)</i>
>> Interface 1 # addr1 10.10.7.1	<i>(Set IP address on backbone network)</i>
>> Interface 1 # mask 255.255.255.0	<i>(Set IP mask on backbone network)</i>
>> Interface 1 # broad 10.10.7.255	<i>(Set the broadcast address)</i>
>> Interface 1 # ena	<i>(Enable IP interface 1)</i>
>> Interface 1 # ../if 2	<i>(Select menu for IP interface 2)</i>
>> Interface 2 # addr1 10.10.12.1	<i>(Set IP address on stub area network)</i>
>> Interface 2 # mask 255.255.255.0	<i>(Set IP mask on stub area network)</i>
>> Interface 2 # broad 10.10.7.255	<i>(Set the broadcast address)</i>
>> Interface 2 # ena	<i>(Enable IP interface 2)</i>

2. Enable OSPF.

>> Interface 2 # /cfg/net/adv/route/ospf/ena	<i>(Enable OSPF on the Firewall)</i>
--	--------------------------------------

3. Define the stub area.

>> OSPF Area index 2 # ../aindex 2	<i>(Select menu for area index 2)</i>
>> OSPF Area index 2 # id 0.0.0.1	<i>(Set the area ID for OSPF area 1)</i>
>> OSPF Area index 2 # type stub	<i>(Define area as stub type)</i>
>> OSPF Area index 2 # ena	<i>(Enable the area)</i>

4. Attach the network interface to the backbone.

>> OSPF Area 2 # ../if 1	<i>(Select OSPF menu for IP interface 1)</i>
>> OSPF Interface 1 # ena	<i>(Enable the backbone interface)</i>

5. Attach the network interface to the stub area.

```
>> OSPF Interface 1 # ../if 2           (Select OSPF menu for IP interface 2)
>> OSPF Interface 2 # aindex 2         (Attach network to stub area index)
>> OSPF Interface 2 # ena             (Enable the stub area interface)
```

6. Apply the configuration changes.

```
>> OSPF Interface 2 # apply
```

Verifying OSPF support

Use the `/info/net` command to verify the OSPF configuration on your firewall iSD.



CHAPTER 11

Upgrading the software

Proper operation of the 8660 SDM depends on the software running on the following devices:

- Passport 8600 Series Switch
- firewall iSD
- Check Point management devices

It can become necessary to upgrade one or more of the software components. This chapter describes firewall iSD software upgrades. Refer to *Release Notes for the Passport 8600 Release 3.7.6* (part number 217316-A) for any known limitations. For information on upgrading software on the Passport 8600 Series Switch, refer to *Upgrading to Passport 8000 Switch Series Software Release 3.7.6* (part number 318843-A).

NOTE – Nortel Networks recommends that you use an FTP application when transferring files to and from the 8660 SDM. TFTP applications can experience slow transfer rates or incomplete file transfer. However, either FTP or TFTP applications can be used for saving configuration files. Note also, when downloading zipped files from a TFTP server, that an extra file extension of `.tar` can be added to the end of the software filename. To correct this, in the **Save as** dialog box, change **Save as type** from **WinZip File** to **All Files**.

NOTE – All software upgrades for the firewall iSDs or Check Point management devices must be obtained from Nortel Networks (for contact information, refer to “[How to Get Help](#)” on [page 20](#)). For information on locating software downloads on the Nortel Networks web site, refer to “[Locating your software](#)” on [page 18](#).”

NOTE – Installation of Check Point FireWall-1 packages through Red Hat Package Manager (RPM) is not supported.

Compatibility

When upgrading any software component, ensure that appropriate and compatible versions of software are installed. Be sure to check any accompanying release notes or readme files for software compatibility and special installation instructions.

The following versions of software are required for the 8660 SDM:

- **Firewall iSD software image, release 2.2.7.0_SDM or higher**

The firewall iSD software includes the firewall OS and built-in Check Point firewall software

- **Check Point management software FireWall-1 NG with Application Intelligence (R55) or higher**

The management software resides on the management workstation and client workstations in your network. It is used to install, maintain, and monitor security policies for all your network firewalls. The Check Point SmartCenter Server can be enabled on your firewall iSDs (refer to [Chapter 2, “Initial setup,” on page 31](#)) or installed on a separate workstation. Check Point SMART Clients can be installed on the same machine as the SmartCenter Server or installed on separate machines. The management software version (NG with Application Intelligence) must be compatible with the Check Point software that you have on your firewall iSD.

NOTE – The Passport 8600 Series Switch must be running software release 3.7.6.0, or higher, for proper operation of the 8660 SDM. To upgrade software on the Passport 8600 Series Switch, refer to *Upgrading to Passport 8000 Switch Series Software Release 3.7.6* (part number 318843-A).

Types of upgrade

The three major classes of software upgrades that are required for maintaining each 8660 SDM firewall iSD are as follows:

- software upgrades that affect the firewall iSD
- software upgrades that target only the Check Point firewall software on the firewall iSDs
- software upgrades that are installed on the Check Point management stations

Firewall iSD upgrades

The following upgrades affect the firewall iSD:

- **Major releases**

This type of upgrade contains important software corrections and feature enhancements for the firewall iSDs. It can affect the firewall OS or built-in Check Point firewall software. See [“Installing a minor/major release upgrade” on page 337](#).

The firewall iSD will automatically reboot after a major upgrade to initialize new features. All configuration data is retained when the ASF5100_2.2.7.0_SDM_R55.pkg file is loaded.

- **Minor releases**

This type of upgrade typically corrects minor software problems on the firewall iSDs. Minor upgrades may temporarily stop the firewall. Configuration data is retained when the ASF5100_2.2.7.0_SDM_R55.pkg file is loaded. See [“Installing a minor/major release upgrade” on page 337](#).

- **Replacing factory-installed software**

This type of upgrade requires that you re-install software. See [“Reinstalling Software” on page 345](#).

NOTE – There are two file types that can be used for upgrading software on the firewall iSD: .img and .pkg files. Both files contain the firewall OS software image, however the .pkg file installs the image in parallel with the existing software version (that is, it installs only new and modified files and does not override the configuration file). The .img file overwrites any existing firewall OS software, as well as any existing configuration file.

Built-in firewall software upgrades

The following upgrades affect the built-in Check Point firewall software:

■ Check Point Feature Pack

This type of upgrade typically contains important firewall software corrections and feature enhancements. This may be necessary to ensure compatibility with the Check Point software installed on the supporting management stations.

The firewall iSD can automatically reboot after installation of a feature pack. All configuration data is retained.

■ Check Point Hotfix

This type of upgrade typically corrects minor software problems in the Check Point firewall software that is built into the firewall iSDs. Hotfixes can usually be installed without rebooting the firewall, retaining normal operational traffic flow. All configuration data is retained.

Check Point management station upgrades

- Management station Check Point Feature Pack
- Management Station Hotfix

Overview of upgrade tasks

Upgrading the software on your firewall iSDs consists of the following tasks:

- Load the new software upgrade package or install image onto an FTP server on your network (see [“Installing a minor/major release upgrade” on page 337](#)).
- Select the firewall iSD on which you will update software (see [“Switching management and console ports among iSDs” on page 56](#)).
- Download the new software from the FTP server to your firewall iSD.
- Activate the new software image on your firewall iSD.

Procedures for activating the software are dependent on the number of firewall iSDs in a cluster. You must always create a cluster during initial configuration of the firewall iSD. A cluster contains either one firewall iSD, or two firewall iSDs. See [“Activating the software upgrade package” on page 339](#) for procedures to activate each type of cluster (single member [iSD] and two member [iSD]).

NOTE – Make certain that your FTP server is on a secure, trusted network before you use FTP for 8660 SDM tasks. One way to ensure FTP security is to implement the FTP server on the SmartCenter Server workstation.

Installing a minor/major release upgrade

To install a minor or major release upgrade on your firewall iSD, you require the following:

- CLI access through a local console terminal or to the firewall iSD host IP address through a remote Telnet or SSH connection (connected through firewall iSD logical port 1 to the Passport 8600 Series Switch).
- The software upgrade package loaded on an FTP server on your network. The FTP server must allow anonymous login.
- A policy installed on the firewall iSD from the Check Point SmartDashboard that allows FTP download onto the firewall iSD from a FTP server.
- The host name or IP address of the FTP server. If you choose to specify the host name, note that you must first have configured the DNS parameters. For more information, see the [“DNS Servers Menu” on page 151](#).
- The name of the software upgrade package (upgrade packages are identified by the .pkg extension).

Access can be gained through the local serial port, or through a remote Telnet or SSH connection. Note that Telnet and SSH connections are disabled by default and must be manually configured after you set up the firewall iSD. For more information on enabling Telnet and SSH connections, see [Chapter 5, “The Command Line Interface,” on page 123](#).

Once you have logged in to the firewall iSD CLI, use the following procedure.

1. **At the Main menu prompt, enter the following command:**

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

2. **Select TFTP or FTP.**

```
Select TFTP or FTP (tftp/ftp) [tftp]: ftp
```

3. When prompted, enter the host name or IP address of the FTP server.

```
Enter hostname or IP address of server: 172.17.124.46
```

4. Enter the name of the new software file on the FTP server.

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

5. Wait for the software to complete loading.

If no problems are encountered, the size of the downloaded file will be reported once the download is complete, followed by an **ok** message and the CLI menu prompt.

```
Received 13056048 bytes in 27.2 seconds
Unpacking...
ok
>> Software Management#
```

Once the upgrade is loaded, the software must be activated. See [“Activating the software upgrade package”](#) on page 339.

Activating the software upgrade package

A firewall iSD can hold up to two versions of the same major software release simultaneously (for example, version 2.2.7.0 and version 2.2.7.1). To view the current software status, use the `/boot/software/cur` command. When a new version of the software is downloaded to the firewall iSD, the software package is decompressed automatically and marked as `unpacked`. After you activate the unpacked software version (which causes the firewall iSD to reboot), the software version is marked as `permanent`. The software version previously marked as `permanent` will then be marked as `old`.

Single member (iSD) cluster upgrade

When you have downloaded the software upgrade package, you inspect its status and activate it using the following commands.

1. Inspect the status of the software:

```
>> Main# /boot/software/cur
Version                Name                Status
-----                ----                -
2.2.7.1                tdo                 unpacked
2.2.7.0                tdo                 permanent
```

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

- **unpacked** means that the software upgrade package has been downloaded and automatically decompressed.
- **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`.
- **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.

2. Activate the new (unpacked) software package:

```
>> Software Management# activate 2.2.7.1
Confirm action 'activate'? [y/n]: y
Activate ok, relogin
Restarting system.

login:
```

After you run the `activate` command, the system logs you out (the CLI menus can be upgraded during this process). Wait until the login prompt appears again (this can take up to two minutes while the system reboots).

3. Log in and check the software status again:

```
>> Main# /boot/software/cur
Version          Name          Status
-----          ----          -
2.2.7.1         tdo           permanent
2.2.7.0         tdo           old
```

In this example, version 2.2.7.1 is now operational and will survive a reboot of the system, while the software version previously indicated as `permanent` now is marked as `old`.

NOTE – After an upgrade, you must push the policies to the cluster.

Two member (iSD) cluster upgrade

Before you begin the upgrade:

- Obtain the version of .pkg file that you want to install.
- Copy the .pkg file to an FTP server.
- Verify that you have a rule on the Check Point management system that allows you to ping the FTP server and connect to it.
- Verify that you can successfully ping the FTP server.

You are now ready to download and activate the new software.

1. Determine which firewall iSD holds the MIP (the host with the * in the MIP column) and log in to it as admin:

```
>> Main# /info/summary
IP addr      type      MIP Local  cpu(%)  mem(%)  op
192.168.1.2  master   *      *       26      42      up
192.168.1.3  master
```

2. Inspect the status of the software:

```
>> Main# /boot/software/cur
Version      Name      Status
-----
2.2.7.0      tdo      permanent
```

The status should be permanent for the currently running software.

3. Download the new .pkg file from the FTP server:

```
>> Main# /boot/software/download
Select TFTP or FTP (tftp/ftp) [tftp]: ftp
Enter hostname or IP address of server: 172.17.124.46
Enter filename on server: ASF5100_2.2.7.0_SDM_R55.pkg
Received 53212760 bytes in 4.0 seconds
Unpacking...
ok
```

4. Inspect the status of the software again:

```
>> Main# /boot/software/cur
Version      Name      Status
-----
2.2.7.1      tdo      unpacked
2.2.7.0      tdo      permanent
```

The status should be unpacked for the software you just downloaded.

5. Disable the firewall iSD:

```
>> Main# /cfg/fw/dis/apply
```

It will take 2 to 3 minutes for the firewall iSD to re-initialize.

6. Verify that the firewall iSD is not running:

```

>> Main# /info/clu
IP Address :192.168.1.2 [MIP] [Up]
Health Report as of Wed Feb 11 10:53:09 2004

    Runtime Information...
        Hard disk usage[Read/Write partition]: 54%
        Memory usage 11%
        CPU Load: 1%

    Application status.
        Webserver
        Running for 24Hrs 19Mins 31Secs

        SNMP
        Not running..

        Check Point Firewall-1
        Not running..                The firewall is not running

        Inet server
        Running for 24Hrs 20Mins 6Secs
IP Address :192.168.1.3 [Up]
Health Report as of Wed Feb 11 10:53:09 2004

    Runtime Information...
        Hard disk usage[Read/Write partition]: 54%
        Memory usage 11%
        CPU Load: 1%

    Application status.
        Webserver
        Running for 24Hrs 19Mins 31Secs

        SNMP
        Not running..

        Check Point Firewall-1
        Not running..                The firewall is not running

        Inet server
        Running for 24Hrs 20Mins 6Secs
    
```

7. Disable HA:

```
>> Main# /cfg/net/vrrp/ha n
>> Main# apply
```

8. Disable synchronization:

```
>> Main# /cfg/fw/sync/dis
>> Main# apply
```

9. Verify that both firewall iSDs are “up” (see op column):

```
>> Main# /info/summary
IP addr          type    MIP Local  cpu(%) mem(%) op
192.168.1.2     master *      *      26    42    up
192.168.1.3     master          26    42    up
```

10. Activate the new (unpacked) version of software (do not disturb the system until it reboots):

```
>> Software Management# activate 2.2.7.1
Confirm action 'activate'? [y/n]: y
Activate ok, relogin

Restarting system.

login:
```

NOTE – You can receive health report error messages whenever two firewall iSDs in a cluster lose the connection with each other. The error messages stop when the two iSDs re-establish connection (that is, when the system stabilizes after implementation of commands).

Both the firewall iSDs will reboot. After two to three minutes, the status of the new software version will change from unpacked to permanent and the older version will change from permanent to old:

```
>> Software Management# cur
Version          Name          Status
-----
2.2.7.1         tdo           permanent
2.2.7.0         tdo           old
```

11. Enable the firewall iSD and HA:

```
>> Main# /cfg/fw/ena
>> Main# /cfg/net/vrrp/ha y
>> Main# apply
```

It will take 3 to 6 minutes for the firewall iSD to become active.

12. Verify that the firewall iSD is running (refer to [Step 6 on page 342](#)).

Both firewall iSDs show “Running for x Hrs y Mins z Secs” if they are running.

13. Push policies to the firewall iSDs.**14. Verify VRRP status (for HA mode):**

```
>> Main# /info/net/vrrp/status
Host 192.168.1.2
      VRRP Backup
Host 192.168.1.3
      VRRP Master
```

15. (Optional) Enable sync and verify operation:

```
>> Main# /cfg/fw/sync enable
Current value: n
Enabling sync may reboot all SFDs when you apply. Are you sure (y|n)? y
>> Main# apply
>> Main# /info/summary
```

16. Launch SmartView Tracker on the Check Point SMART Client and verify that all modules have a green tick. If not, reboot the firewall iSDs.

When reboot completes, login as root and verify that sync is working properly by entering `cphaprob stat` at the root prompt.

Both firewall iSDs should be active.

17. Verify that data traffic is forwarding properly by watching the Check Point logs using SmartView Tracker on the Check Point SMART Client.

Reinstalling Software

Reinstalling the software is seldom required except after a serious malfunction.

To reinstall software on the firewall iSD, you must connect directly to the 8660 SDM serial port and log in as the `boot` user. When the reinstallation is performed, the new firewall iSD is reset to its factory default configuration. All previous configuration data and software is erased, including old software image versions or upgrade packages.

NOTE – Because a reinstallation erases all configuration data (including network settings), Nortel Networks recommends that you first save all configuration data to a file on an FTP/TFTP 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](#)” on page 144.

Re-install software on the firewall iSD using an `.img` file version through FTP.

Nortel Networks recommends that you re-install the firewall iSD software using the front-facing 8600 SDM management port (logical port 3 of the firewall iSDs). If this fails to work for any reason, use logical port 1 of the firewall iSD you want to re-image. If you must use logical port 1, follow these steps:

- 1. Use the existing management VLAN, or create the management VLAN on logical port 1.**
- 2. Configure one of the Passport 8600 Ethernet ports to be a member of the management VLAN.**
- 3. Transfer the software using FTP.**

Ensure you enter the host IP address of logical port 1 for the target address (to which the software is transferred).

Reinstalling software using FTP

To reinstall software using FTP, you need the following:

- Access to the target firewall iSD through a direct connection to its serial port. Remote Telnet or SSH connections cannot be used for reinstalling software.
- The `.img` file must be loaded on an FTP server on your network.

- The host name or IP address of the FTP server. If you choose to specify the host name, you must first configure the DNS parameters. For more information, see the “DNS Servers Menu” on page 151.
- The name of the .img file.

Reinstallation is performed using the following procedure.

1. **Log in as the `boot` user. The password is `ForgetMe`.**
2. **After a successful login, follow the onscreen prompts and provide the required information.**

For example:

```
login: boot
Password: ForgetMe
*** Reinstall Upgrade Procedure ***
If you proceed beyond this point, all traffic processing will be shut
down, and the active network configuration will be reset, requiring
a reboot to restore any current setup. However, no permanent changes
will be made until the boot image has been downloaded.
Continue (y/n)? [y]: y
Select a network port (1-3, or i for info) [1]: 3
Enter VLAN tag id (or zero for no VLAN tag) [0]:
Enter IP address for this iSD [10.10.1.1]: 192.168.1.2
Enter network mask [255.255.255.0]: (Press <Enter> if correct)
Enter gateway IP address [192.168.128.1]: (Press <Enter> if correct)
Select TFTP (t) or FTP (f) [t]: f
Enter FTP server address: <IP address>
Enter file name of boot image: ASF5100_2.2.7.0_SDM_R55.img
Downloading boot image...
ASF5100_2.2.7.0_SDM_R55.img:                62.65 MB  600.33 kB/s
Installing new boot image...
Done
Restarting...
Restarting system.
login: root
Password:
```

If the firewall iSD has not been previously configured for network access, you must provide information about network settings such as IP address, network mask, and gateway IP address. After the new boot image has been installed, the firewall iSD will reboot. You can log in again when the login prompt appears.

3. **Restore the configuration from the FTP/TFTP server using the `/cfg/gtcfg` command.**

4. **Reboot the firewall iSD to apply the restored configuration file.**
5. **Re-establish SIC and push policies from the Check Point SMART Client.**



CHAPTER 12

Event Logging API

The firewall iSD Event Logging API (ELA) is an OPSEC application that allows system log messages to be sent to a Check Point management station for display through the Check Point SmartView Tracker. Log messages are sent to the Check Point SmartCenter Server through a secure, encrypted channel.

For information on configuring and administering OPSEC applications in Check Point, refer to your complete Check Point FireWall-1 NG documentation.

ELA configuration requires steps at both the Check Point SmartCenter Server and at the firewall iSDs. For each firewall iSD, you must create a new OPSEC application at the Check Point SmartCenter Server, and initialize SIC. For each firewall iSD, the certificate associated with the SIC must be pulled to the firewall iSD before the ELA will operate.

This chapter details the steps required to use ELA.

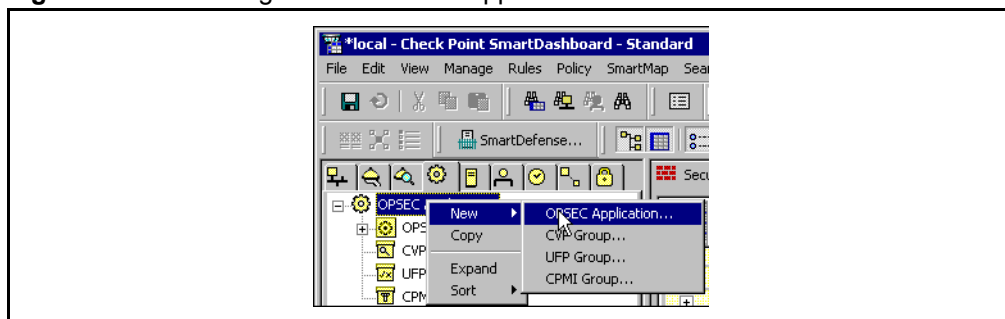
Configure the Check Point SmartCenter Server

Open the Check Point SmartDashboard to create an ELA OPSEC application for the firewall iSD.

1. Create a new OPSEC application.

In the tabbed menu on the left, click on the **OPSEC Applications** tab and choose **New > OPSEC Application**. See [Figure 12-1](#).

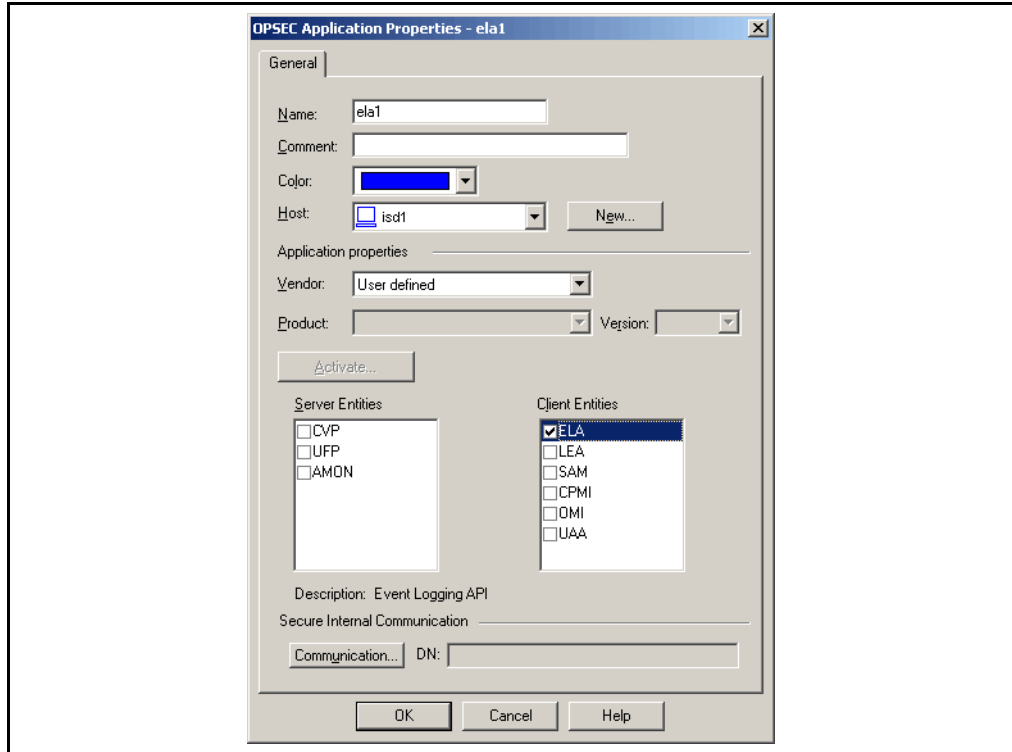
Figure 12-1 Selecting New > OPSEC Application



2. Initialize the OPSEC application by filling in the fields as follows (see [Figure 12-2 on page 351](#)):

- Enter an appropriate identifier in the **Name** field. You will need to use this name when pulling the certificate to the firewall iSD.
- Enter the firewall iSD number in the **Host** field.
- Enter *User defined* in the **Vendor** field.
- Select **ELA** in the **Client Entries** box.

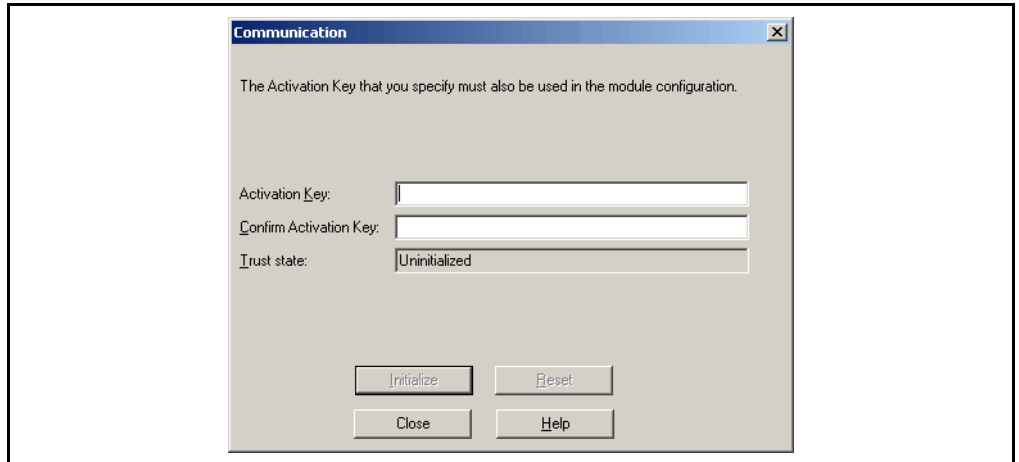
Figure 12-2 OPSEC Application Properties



3. Click the **Communication** button to initialize SIC.

The **Communication** dialog box opens. See [Figure 12-3](#).

Figure 12-3 Communication dialog box



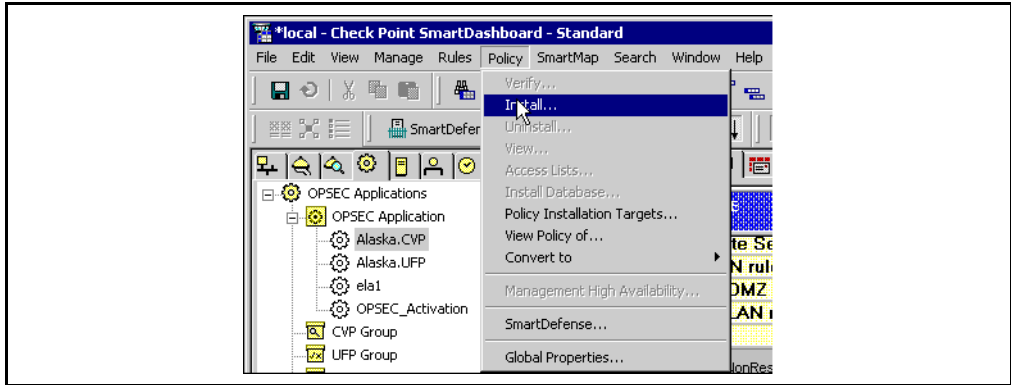
4. Enter an **Activation Key**. You will need to use this **Activation Key** later when pulling the certificate to the firewall iSD.
5. Click **Initialize**.

NOTE – When initialized, the trust state will be displayed as `Initialized` but `trust not established`. This is normal and will not change even after the SIC certificate is pulled from the Check Point SmartCenter Server.

6. Install the policy to the firewall iSD.

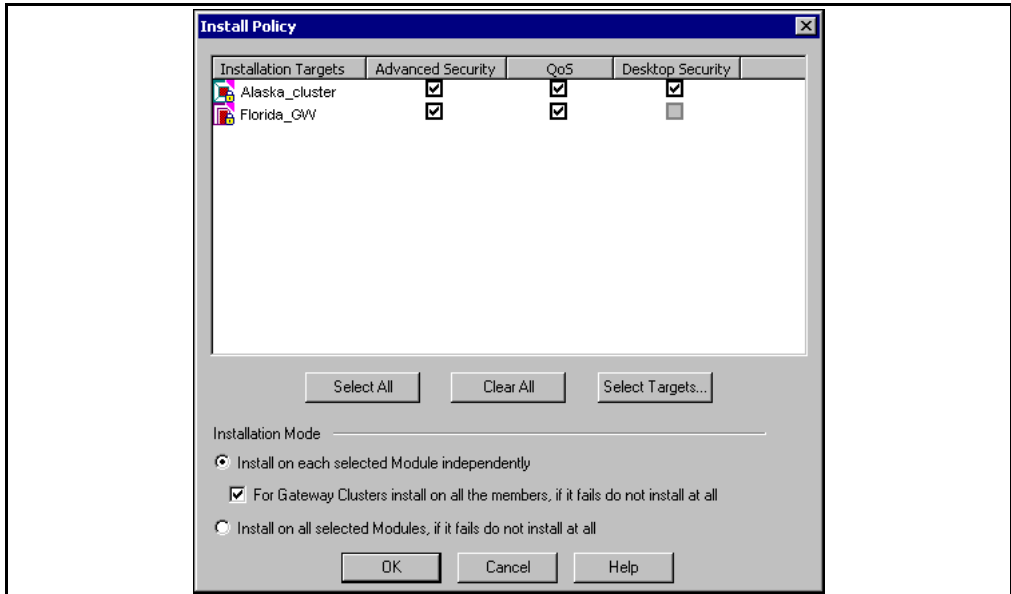
From the SmartDashboard menu bar, select **Policy > Install**. See [Figure 12-4](#).

Figure 12-4 Selecting Policy > Install



The **Install Policy** dialog box opens. See [Figure 12-5](#).

Figure 12-5 Install Policy dialog box



7. Select the object.

8. Click OK to initiate installation of the rulebase.

NOTE – If the Check Point anti-spoofing feature is not enabled, a warning message will appear. See your Check Point documentation to determine whether antispoofing is necessary for your firewall.

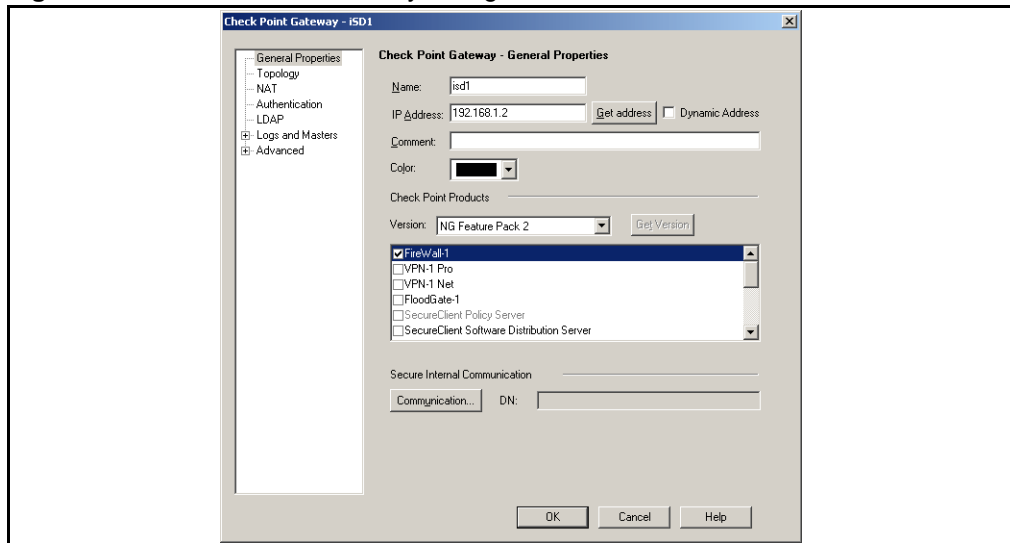
9. **Close the Install Policy window when the process is complete.**

Configuring ELA on the firewall iSD

You can configure ELA on the firewall iSD through the CLI or the BBI. The following steps use the BBI method. For configuring the ELA using the CLI, see “[ELA Logging Menu](#)” on [page 175](#).

Before beginning the following procedure, determine the management station Distinguished Name (DN). You will need this information to fill out the **Cluster > Logs > ELA** form. To determine the management station DN, access the properties of the SmartCenter Server (see [Figure 12-6](#)) by double-clicking on its displayed icon in the Check Point SmartDashboard. The DN is found in the **Secure Internal Communication** area.

Figure 12-6 Check Point Gateway dialog box



To configure ELA on the firewall iSD:

1. **Log in to the BBI using the host IP address.**

2. Select the **Cluster > Logs > ELA** form. See [Figure 12-7](#).

Figure 12-7 Cluster > Logs > ELA form

3. Define the General Settings as follows:

- Set **Status** to enabled.
- Set **Management Station IP** to the IP address of the Check Point management station. Use dotted decimal notation.
- Set **Minimum Severity**, if necessary. All messages at the specified level of severity or higher will be logged to ELA.
- Set the **Management Station DN**.

4. Save and apply the settings.

Click the **Update** button to submit your changes. Click the global **Apply** button to activate your changes.

5. Pull the SIC certificate from the SmartCenter Server.

NOTE – For ELA to function, a separate certificate for SIC communication needs to be installed on each firewall iSD.

In the **Pull SIC Certificate** section of the **Cluster > Logs > ELA** form, set the following parameters:

- a. Set **ISD IP** to the IP address of the firewall iSD being updated.

- b. Set the **OPSEC Application Name** to the name specified when creating an OPSEC application in the Check Point SmartDashboard (see [Figure 12-2 on page 351](#)). Each host maps to a unique OPSEC application.
 - c. Set the password to match that specified when configuring SIC for the OPSEC application.
6. Click the **Submit** button to finish.

The Check Point SmartView Tracker

To view the logs, open the Check Point SmartView Tracker. See [Figure 12-8](#).

Figure 12-8 Viewing logs

No.	Date	Time	Product	Interface	Origin
1	16May2000	18:35:10	VPN-1 & FireWall-1		10.27.10.2
2	6Mar2001	17:08:19	VPN-1 & FireWall-1	daemon	
3	6Mar2001	17:08:20	VPN-1 & FireWall-1	daemon	10.20.8.46
4	6Mar2001	17:08:26	VPN-1 & FireWall-1	hme0	10.20.8.46
5	6Mar2001	17:12:03	VPN-1 & FireWall-1	hme0	10.20.8.46
6	6Mar2001	17:13:33	VPN-1 & FireWall-1	daemon	10.20.8.46
7	16May2000	18:35:11	VPN-1 & FireWall-1	daemon	10.27.10.2
8	16May2000	18:35:12	VPN-1 & FireWall-1	daemon	10.27.10.2
9	16May2000	18:35:13	VPN-1 & FireWall-1	E190x3	10.27.10.2
10	16May2000	18:35:14	VPN-1 & FireWall-1	E190x1	10.27.10.2
11	16May2000	18:35:10	Multi-product	E190x1	10.27.10.2
12	16May2000	18:35:18	VPN-1 & FireWall-1	daemon	10.27.10.2
13	16May2000	18:35:28	VPN-1 & FireWall-1	E190x1	10.27.10.2

The firewall iSD and registry must be running for logging to occur. This happens late in the boot process. Messages are cached locally until they can be sent to the ELA logging server. Therefore, it can take a few minutes before messages appear after a reboot.



APPENDIX A

Common tasks

This chapter describes procedures for the following firewall iSD management tasks:

- “Tuning Check Point NG performance” on page 360
- “Reading system memory information” on page 362
- “Cluster backup and clone procedures” on page 363
- “Generating a public or private DSA key pair” on page 366

Tuning Check Point NG performance

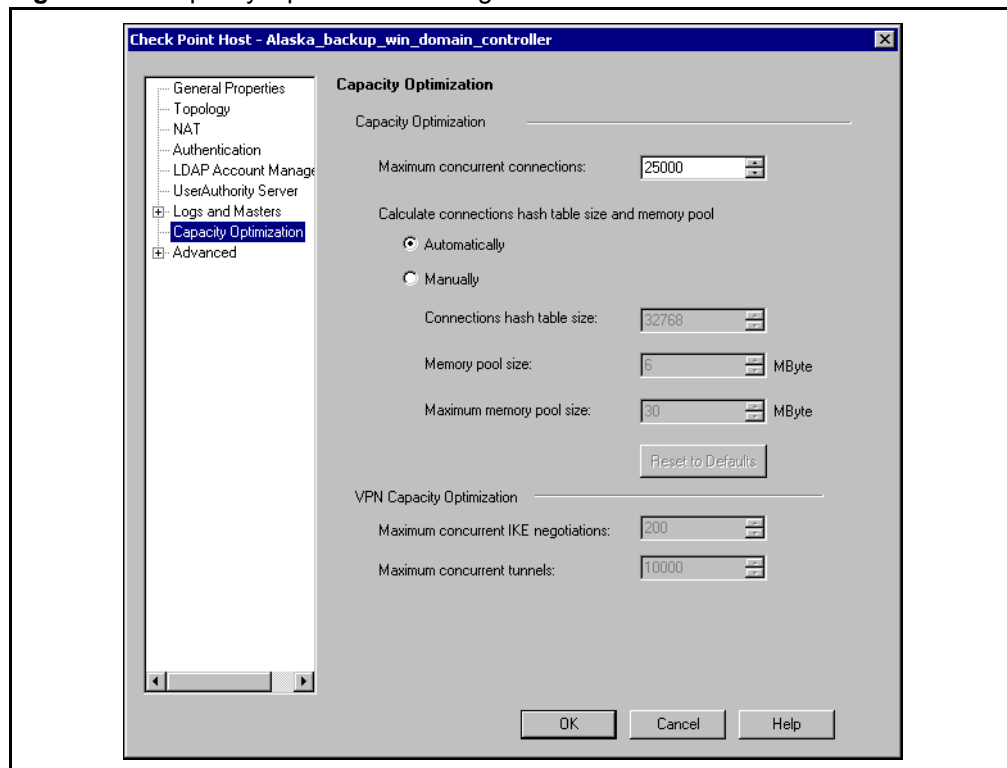
Connection parameters

To tune connection parameters:

1. **Right-click on the firewall iSD object in the Check Point SmartDashboard and select Edit.**
2. **Open the Logs and Masters > Capacity Optimization tab to edit the maximum concurrent sessions.**

The Capacity Optimization dialog box opens. See [Figure A-1](#).

Figure A-1 Capacity Optimization dialog box



3. **Raise the Maximum concurrent connections level so that it is consistent with the specifications for the model you are using (see [Table 1-3 on page 25](#)). The default is 25 000.**

4. Select the **Automatically** option button to calculate the connections hash table size and memory pool.

The automatically configured hash size of the connections is 4 194 304 because it matches the increased number of connections on the firewall iSD. The default is 32 768.

NAT parameters

If the Network Address Translation (NAT) policy is being used by a large number of concurrent sessions, then the following two parameters can be modified:

- `nat_hash_size`: The current limit is 16 384. It should be increased to 131 072.
- `nat_limit`: The current limit is 25 000. It should be increased to 180 000.

NOTE – Modification is optional since setting the connections table value also sets the NAT connections table value for FP3, R54, R55 and above.

You can tune the performance of the Check Point NG by entering the following commands at the firewall iSD CLI and at the Check Point management station command line.

1. Log in to the local terminal as admin to disable the firewall iSD:

```
>> /cfg/fw/dis
```

Allow several minutes for FireWall-1 services to stop before entering `/cfg/fw/ena`.

NOTE – The firewall iSD will automatically restart FireWall-1 services unless you use the `/cfg/fw/dis` command to disable the unit. For that reason, it is recommended that you do not use the `cpstop/cpstart` commands at the management station to disable/enable the firewall iSD.

2. Log out of the local terminal and log in as `root`.

3. Edit the file: `$FWDIR/conf/objects_5_0.C`

(see “Tuning Check Point NG performance” on page 360 for parameters to tune).

NOTE – It is recommended that you use `guidbedit` from within the Check Point management station to edit `objects_5_0.C`. You can download the `guidbedit` utility from <http://www.checkpoint.com/techsupport/downloadsng/utilities.html#dbtool>.

4. Log out of the local terminal and log in as `admin`.
5. Re-enable the firewall iSD:

```
>> /cfg/fw/ena
```

6. Start the SMART Client.
7. Reinstall the policies and download them to the firewall iSD using the SMART Client.

Reading system memory information

Table A-1 lists commands for accessing memory information.

Table A-1 Commands to access memory information

Memory type	Command
General Linux memory information	<code>free</code> or <code>vmstat <seconds></code> or <code>cat /proc/meminfo</code> or <code>top</code>
Kernel modules information	<code>lsmod</code>
NG memory information	<code>fw ctl pstat</code>

Cluster backup and clone procedures

In this scenario, two firewall iSDs were configured for HA. The Check Point rules are framed, gateway cluster has been formed, and the policies are installed on both the firewall iSD hosts. After the VRRP/HA setup is completed, both firewall iSD hosts must be backed up individually.

Backing up

1. **Login as `root` and enter the following command to test whether the sync is working correctly:**

```
# fw ctl pstat
```

The total packets sent and total packets received (under Sync) should show valid values (that is, non-zero values). If the sync is working only for one side of the interface, then do the following:

- a. Reset SIC on both firewall iSDs.
 - b. Reinstall the policies on both units.
 - c. Reboot both units.
 - d. Redo [Step 1](#).
2. **Copy the current configuration to a remote ftp/tftp server.**
 3. **Exit.**
 4. **Login as `admin`, and enter the following commands:**

```
>> Main# /cfg/sys/backup/bckremote
Select TFTP (t) or FTP (f) [t] : t
Enter the tftp/ftp Server IP Address :10.10.10.2
Configuration filename : test
Uploading configuration file of 7055360 bytes...
Configuration file test:7055360 bytes saved to TFTP server
```

If the operation fails, verify the following conditions:

- When using TFTP, the filename you enter must already exist in the TFTP server.

- When using FTP, **anonymous ftp** must be enabled in the FTP server. Additionally, the anonymous ftp login should have **file list** and **file put** permission.
- When using FTP, ensure the **put** operation stores the file in the user-specified folder. (In some FTP server configurations, all files transferred under anonymous login are stored in an **incoming** folder. Do not use this configuration.)
- Ensure Check Point does not drop packets sent to the TFTP/FTP server. Check whether FTP or TFTP access to the TFTP/FTP server is working from the `root` login.

Cloning

Before you begin, verify that both firewall iSDs are running the same software version. Log in to each firewall iSD and verify that the permanent software version on both units is the same (see [Figure A-2](#)).

Figure A-2 Verifying the software version on a firewall iSD

```
>> Boot# cur

Boot:
  Software Management:
    Version           Name           Status
    -----           ----           -
    2.2.7.0_SDM       tdo            permanent
    2.2.5.0           tdo            old
```

If the software versions are not the same, upgrade one or both to the desired software version (see [“Installing a minor/major release upgrade”](#) on page 337 for upgrade instructions). Once they are the same you can proceed with cloning as follows:

1. **Load the backup file onto the second firewall iSD.**
2. **Log in as `root` on the second firewall iSD.**

3. Enter the following commands (substitute your IP address and port number as needed):

```
[root@a172-25-3-11 root]# clone

*** Clone Procedure ***
If you proceed beyond this point, all traffic processing will be shut
down, and the active network configuration will be reset, requiring
a reboot to restore any current setup.
Continue (y/n)? [y]: y
Select a network port (1-3, or i for info) [4]: 1
Enter VLAN tag id (or zero for no VLAN tag) [0]:
Enter IP address for this iSD [172.16.2.155]:
Enter network mask [255.255.255.0]:
Enter gateway IP address [none]:
Select TFTP (t) or FTP (f) [t]:
Enter TFTP server address: 172.16.2.183
Enter configuration file name in TFTP server: test
Downloading configuration ...
Validating downloaded configuration
Configuring System...
System will be configured on reboot
Restarting system
```

Once cloning is complete, Check Point takes up to 10 minutes to re-sync its configuration information. Once the re-sync is complete, the second firewall iSD will work as expected.

Generating a public or private DSA key pair

The following procedures and command strings demonstrate:

- generation of the DSA key pair
- creating an SSH account on a firewall iSD
- opening an SSH session on the firewall iSD

In this scenario, there is one firewall iSD and one Linux host from which to launch an SSH connection.

1. Generate the public/private DSA key pair.

NOTE – Use the passphrase from [Step 5 on page 368](#).

- a. On the Linux host enter the DSA key generate commands:

```
[test@Phantom test]$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/test/.ssh/id_dsa): tkey
tkey already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in tkey.
Your public key has been saved in tkey.pub.
The key fingerprint is:
2d:77:72:7d:35:58:2c:4b:a4:f8:56:50:73:42:92:ae test@Phantom
```

- b. Print the public and private keys to the screen:

```
[test@Phantom test]$ cat tkey.pub
ssh-dss
AAAAB3NzaC1kc3MAAACBAKEdba7LVbSwXDoYDmQaPifvruRFxa465FffwsGmF/LQ98tP
YqwJvwLgtCyQVUL9GyUvAlECvPTlBCsAATnITo0KYL03axqqRr9PmdgaxrCcAkyQ1LoO
HcDzuhUXB0wYXc9ymDTP+4HFSFEuJWNkz7taAmftapuxrmOrah6fejQJAAAAFQDwRbUK
QkRQpwdRyW7AhhbZEsUdsQAAAIQA1pw56WRG7c6oH9MV3ppjUIQdLXylMY1+aVEqcAki
VqxKwEbpjsSfn4v465ZLHOIXv9aku7FpyXoOwkESNDIvIdyecu2BchK6fc1CWPCLM/cq
GxmSm3gWYvFKCdoFcroNeTgVb1B2VvMn4QuDLj7jbeNoHL708Nida3eb/xxAEAAAAIEA
k1hg9Y2Q8u9sEgWNN870LsrXkcySc8YJfPSCsd0ePewU5j41VojQda8a6C2xKypbQth
zshaXdPO2WiNzJWAzGdWcm73yIrgGSpFNkpCB48GKkMdRyJ/Ntv3QwX/bUcMilJZEHWt
EdRyjP84WbIZAK4kpbw3mz6ptYhEvLcPvyA= test@Phantom
```

The public key includes every character after the command line (ssh-dss-test@Phantom).

2. Create an SSH account on the firewall iSD.

- a. Log in to the firewall iSD.
- b. Enter the user (account) name information:

```
>> Main# /cfg/sys/user/adv/user
Enter user name: test
Creating SSH User test

-----

[SSH User test Menu]
    name      - Set Full name of User
    pubkey    - Set RSA/DSA Public Key for User
    ena       - Enable User Account
    dis       - Disable User Account
    del       - Remove SSH User

>> SSH User test# name
Current value: none
Enter a descriptive name for user: Phantom

>> SSH User test# pubkey
Current value: none
Enter RSA/DSA public key for user: ssh-dss
AAAAB3NzaC1kc3MAAACBAKEdba7LVbswXDoYDmQaPifvruRFxa465FffwsGmF/LQ98t
PYqwJvwLgtCyQVUL9GyUvA1ECvPT1BCsAATnITo0KYL03axqqRr9PmdgaxrCcAkyQlL
oOHcDzuhUXB0wYXc9ymDTP+4HFSFEuJWNkz7taAmftapuxrmOrah6fejQJAAAAFQDwR
bUKQkRQpwdRyW7AhhbZEsUdsQAAAIAQlpw56WRG7c6oH9MV3ppjUIQdLXylMY1+aVEq
cAkiVqXkWEbpjsSfn4v465ZLHOIXv9aku7FpyXoOwkESNDivIdyecu2BchK6fclCWPC
LM/cqGxmSm3gWyvfKCdofcroNeTgVblB2VvMn4QuDLj7jbeNOHL708Nida3eb/xxAEA
AAAEAk1hg9Y2Q8u9sEgWNN870LsrXkcySc8YJfPSCsd0ePewU5j41VojQda8a6C2x
KypbQthzshaXdPO2WiNzJWazGdWcM73yIrcGSpFNkpcB48GKkMdRYj/Ntv3QwX/bUcM
ilJZEHWTEdRyjP84WbIZAK4kpbw3mz6ptYhEvLcPvyA= test@Phantom

>> SSH User test# ena

>> SSH User test# apply
**NOTE**
Telnet, SSH and Web (HTTP) are enabled.

Changes applied successfully.

>> SSH User test#
```

3. Enter the Linux host network and network mask into the firewall iSD access list:

```
>> Main# /cfg/sys/accesslist/add
Enter network address: 33.1.1.0
Enter netmask: 255.255.255.0

>> Access List# apply
**NOTE**
Telnet and Web (HTTP) are enabled.

Changes applied successfully.
```

4. Enable SSH on the firewall iSD host and apply the change:

```
>> Main# /cfg/sys/adm/ssh/ena/apply
**NOTE**
Telnet, SSH and Web (HTTP) are enabled.
```

5. Connect to the firewall iSD shell through SSH:

```
[test@Phantom test]$ ssh -l test 33.1.1.18 -2
test@33.1.1.18's password: <passphrase>
```

For a password, enter the passphrase you entered when you generated the SSH keys in [Step 1 on page 366](#).



APPENDIX B

Troubleshooting

Failed to establish trust between SmartCenter Server and firewall iSD

In this scenario, the user is unable to establish trust between the SmartCenter Server and the firewall iSD.

NOTE – This scenario assumes you are logged into a SmartCenter Server that is installed on a separate workstation.

Failure to establish trust can also mean that you cannot download policies to the firewall iSD (see [“Cannot download policy on firewall iSD” on page 371](#)).

Actions

1. Verify that the management station is connected to the correct port by entering the following command on the firewall iSD:

```
/info/net/if
```

2. Reset the SIC (using the one-time password) using the following command:

```
/cfg/fw/sic
```

NOTE – The one-time password is used to establish the first-time communication. After that, the password is negotiated by the devices and changed. The new password is used for the rest of the session.

3. Unload the firewall policies:

```
/maint/diag/fw/unldplcy
```



CAUTION—Unloading the firewall policies allows all traffic to pass through the firewall iSD. Remember to push your firewall policies from the Check Point SmartDashboard after you have re-established trust.

4. Enter the following command to test if the firewall iSD is enabled in the configuration:

```
/cfg/fw/cur  
(or)  
/info/host
```

5. If the firewall iSD is not enabled, enter the following command:

```
/cfg/fw/ena
```

NOTE – It takes up to three minutes for FireWall-1 services to start after enabling the firewall iSD.

(The steps that follow require that you be logged into the firewall iSD as the `root` user.)

6. Ping the firewall iSD from the management station using the IP address. To check if routing is working correctly between the firewall iSD and the management station, use the `fwstop` command to turn off the firewall iSD before pinging.

```
fwstop  
ping <Firewall host IP>
```

7. Enter the following command to see if the firewall iSD MAC address is learned:

```
arp -a
```

This command should display the firewall iSD's IP address and MAC address. If not, check the gateway information on the management server.

8. Enter the following command to see if ICMP reaches the firewall iSD from your source IP address:

```
tcpdump -n icmp
```

Cannot download policy on firewall iSD

In this scenario, after downloading the policy on the firewall iSD, you cannot check the communication or download the policy again.

NOTE – Users often forget to update the SmartDashboard after `add/delete` interfaces from the firewall iSD console. As a result, anti-spoofing blocks the traffic because incorrect interfaces were used.

Action

Delete the existing policies by entering the following command and retrieving the interfaces from the SMART Client again:

```
/maint/diag/fw/unldplcy
```



CAUTION—Unloading the firewall policies allows all traffic to pass through the firewall iSD. Remember to push your firewall policies from the Check Point SmartDashboard after you have re-established trust.

Poor performance with other devices

In this scenario, you see poor performance when using the 8660 SDM with another network device such as a router.

Action

From the 8660 SDM console, manually configure the link parameters for the port or ports suspected of poor performance. Turn off autonegotiation. Set port speed (10,100, 1000) and duplex mode (full, half) to be compatible with the adjacent device. Verify that compatible parameters are set on the adjacent device.

Cannot log into the management station from the SMART Client

In this scenario, the SMART Client cannot login into the management station.

Actions

1. If the SMART Client and SmartCenter Server are not in the same network, add a rule to allow Check Point Management Interface (CPMI) to go through these two networks.
2. Enter the command `cpconfig` on the management station to see if client IP address is on the SMART Client list.

If you are running your management station from the firewall iSD, log in as `root` before entering this command.

Check Point sends connection failed messages to the firewall iSD

In this scenario, you receive `fwconn_record_conn: Id_set_wto(connections) failed` messages during the session. This occurs when the Check Point session limit is reached. The default is 25 000 connections.

Action

Increase the session limit on the management station. Refer to [“Tuning Check Point NG performance” on page 360](#).

VRRP configuration tips

VRRP configuration tasks must be performed in a particular order:

1. Do not enable synchronization or VRRP on either firewall iSD host until you have added the second firewall iSD host to the cluster (see [“/cfg/net/if <interface number>/vrrp” on page 187](#) and [/cfg/net/vrrp/ha on page 188](#)).
2. Make sure both virtual router interfaces can communicate with each other.

3. **Configure the virtual router interface on both firewall iSD hosts using CLI** (see [“/cfg/net/if <interface number>” on page 185](#)) or BBI (see [“Network > Interfaces” on page 250](#)).
4. **Ping the IP address of the virtual router for firewall iSD 1 from firewall iSD 2 (or the opposite).**
5. **If unsuccessful, troubleshoot cabling and make sure port LEDs for your model are properly lit** (see *Installing the 8660 Service Delivery Module (SDM) for the Passport 8600 Series Switch* [part number 217314-A] for information on port LED indicators).
6. **Establish trust with both units.**
 - Make sure you can ping both firewall iSD host IP addresses from the management station (if the management station and firewall iSD host IP address are not on the same network, add static routes as needed on the management station).
 - Reset the cluster SIC using Check Point SMART Client (see [“Establishing Secure Internal Communication” on page 79](#)).
 - Reset the cluster SIC using CLI (see [/cfg/fw/sic page 205](#)).
7. **Once SIC completes (this can take several minutes), push policies from the Check Point SmartDashboard to the cluster.**
8. **Configure VRRP for both firewall iSD hosts.**
 - Configure vrid (see [/cfg/net/if <interface number>/vrrp/vrid on page 187](#)).
 - Configure ip1 (see [/cfg/net/if <interface number>/vrrp/ip2 on page 187](#)).
 - Configure ip2 (see [/cfg/net/if <interface number>/vrrp/ip2 on page 187](#)).
 - Enable synchronization (optional) (see [“/cfg/fw/sync” on page 207](#)).
 - Enable VRRP (see [“/cfg/net/vrrp” on page 188](#)) and set the rest of the VRRP parameters.
 - Apply changes.

VRRP: active master backup fails

In this scenario, the active master fails, but failover does not take place. A likely cause is loss of trust between the firewall iSD and the SmartCenter Server.

Actions

1. Log in as root and check the firewall iSD status:

```
root# fw stat
```

2. If the SmartCenter Server and the firewall iSD are not communicating, the firewall iSD will return a status message indicating that the policy and host identities are unknown:

```
HOST          POLICY        DATE
--           ---          --- [>eth0] [<eth0] [>eth1] [<eth1] [>eth2]
[<eth2] [>eth3] [<eth3]
```

You can repair this condition by reestablishing trust with the firewall iSD.

3. Open the SMART Client application and verify the SIC status between the management station and the firewall iSD. If the devices are not communicating:
 - a. Reset SIC at the SMART Client (see [“Establishing Secure Internal Communication”](#) on page 79) and at the CLI (see [“/cfg/fw/sync”](#) on page 207).
 - b. Push policies from the SmartCenter Server to the firewall iSD.
 - c. After SIC completes (this can take several minutes), log in to the firewall iSD as root and check the firewall iSD status:

```
root# fw stat
HOST          POLICY        DATE
localhost VRRP          14Mar2003 14:08:05 : [>eth0] [<eth0] [>eth1]
[<eth1] [>eth2] [<eth2] [>eth3] [<eth3]
```

This status message indicates that trust has been established. When trust is established on a system running VRRP, failover should take place in less than 40 seconds.

NOTE – The policy must allow VRRP advertisement (multicast) packets for VRRP failover to work properly.

VRRP: Both masters are active

In this scenario, both the master and the backup have assumed the active role. This may be because the firewall iSD policy on the cluster does not permit VRRP multicast packets, which are required for the VRRP election process to work (see [“VRRP election” on page 297](#)).

Actions

1. **Log in as `root` and check the output of the backup interface:**

```
root# tcpdump -i eth1 Prints out packet headers on interface
```

Watch for VRRP advertisement packets (multicast packets) that indicate VRRP active master activity on the interface.

2. **Check the firewall iSD status if you do not see VRRP advertisement packets:**

```
root# fw stat
HOST      POLICY      DATE
localhost InitialPolicy 20Mar2003 10:30:10 : [>eth0] [<eth0] [>eth1]
[<eth1] [>eth2] [<eth2] [>eth3] [<eth3] Policy = InitialPolicy
```

If the Policy is **DefaultFilter** or **InitialPolicy**, push policies to the firewall iSD that allow VRRP advertisement packets.

NOTE – The dual active master phenomenon will also result from momentary interruption of continuity (for example, pulling a cable and restoring it) between a firewall iSD host and a device running STP. Given these conditions, STP will halt traffic flow for up to 30 seconds. This will prevent the VRRP advertisement packets sent by the active master from reaching the backup that is being restored from the VRRP fault state. Not seeing the advertisement packets, the backup will assume the active role along with the other firewall iSD host. The condition will self-correct through the VRRP election process when STP allows traffic to flow again. See [“VRRP election” on page 297](#) and [“VRRP failover” on page 297](#).

Poor performance under heavy traffic

In this scenario, there is poor performance under heavy traffic.

Action

Ensure the management station is configured as explained in [“Tuning Check Point NG performance”](#) on page 360.



APPENDIX C

Software licenses

The 8660 SDM includes software that is covered by the licenses described in this section.

Apache Software Licence

The 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 above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above 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, please 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 “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 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 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 software consists of voluntary contributions made by many individuals on behalf of the Apache Software Foundation. For more information on the Apache Software Foundation, please 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.

mod_ssl License

LICENSE

The mod_ssl package falls under the Open-Source Software label because it's distributed under a BSD-style license. The detailed license information follows.

Copyright (c) 1998-2001 Ralf S. Engelschall. 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 above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above 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 Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).”
4. The names “mod_ssl” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact rse@engelschall.com.
5. Products derived from this software may not be called “mod_ssl” nor may “mod_ssl” appear in their names without prior written permission of Ralf S. Engelschall.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>).”

THIS SOFTWARE IS PROVIDED BY RALF S. ENGELSCHALL “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 RALF S. ENGELSCHALL OR HIS 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.

OpenSSL and SSLeay Licenses

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2001 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 above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above 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, please 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 (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 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's 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, etc., 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 above 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. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

PHP License

The PHP License, version 2.02

Copyright (c) 1999, 2000 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "PHP" must not be used to endorse or promote products derived from this software without prior permission from the PHP Group. This does not apply to add-on libraries or tools that work in conjunction with PHP. In such a case the PHP name may be used to indicate that the product supports PHP.
4. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number.

Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.

5. Redistributions of any form whatsoever must retain the following acknowledgment:
 "This product includes PHP, freely available from <http://www.php.net/>".
6. The software incorporates the Zend Engine, a product of Zend Technologies, Ltd. ("Zend"). The Zend Engine is licensed to the PHP Association (pursuant to a grant from Zend that can be found at <http://www.php.net/license/ZendGrant/>) for distribution to you under this license agreement, only as a part of PHP. In the event that you separate the Zend Engine (or any portion thereof) from the rest of the software, or modify the Zend Engine, or any portion thereof, your use of the separated or modified Zend Engine software shall not be governed by this license, and instead shall be governed by the license set forth at <http://www.zend.com/license/ZendLicense/>.

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "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 PHP DEVELOPMENT TEAM 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 software consists of voluntary contributions made by many individuals on behalf of the PHP Group.

The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project, please see [<http://www.php.net>](http://www.php.net).

SMTPclient License

LICENSE

SMTPclient—simple SMTP client

Copyright (C) 1997 Ralf S. Engelschall, All Rights Reserved.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License in the file COPYING along with this program; if not, write to:

Free Software Foundation, Inc.,
675 Mass Ave, Cambridge,
MA 02139, USA.

Notice, that “free software” addresses the fact that this program is **distributed** under the term of the GNU General Public License and because of this, it can be redistributed and modified under the conditions of this license, but the software remains **copyrighted** by the author. Don't intermix this with the general meaning of Public Domain software or such a derivated distribution label.

The author reserves the right to distribute following releases of this program under different conditions or license agreements.

Ralf S. Engelschall
rse@engelschall.com
www.engelschall.com

GNU General Public License

GNU GENERAL PUBLIC LICENSE Version 2, June 1991

Copyright (C) 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.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, 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 above, 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, that in whole or in part 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 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 above 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 above 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 above 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 accord with Subsection b above.)

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, since 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 would 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 would 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 whose distribution conditions are different, write to the author to ask 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

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

```
<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>
```

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.



Index

Symbols

/ 131

? (help) 131

[] 17

A

abbreviating commands (CLI) 134

applications

high availability firewall configuration 299–307

vrrp overview 294–298

autonomous systems (AS) 321

B

basic setup

allowing client access 62

Check Point Management tools 62

Check Point Management tools installation 64

firewall object definition w/SmartDashboard 76

firewall policy test rule 79

licenses 54

new installation 45, 50

re-installing existing license 91

SmartDashboard/firewall secure comms 79

task overview 31

Windows NT hosts file 63

basic setup using CLI 36

BBI 322

basics 223

getting started 218–221

BBI forms

administration forms 272–289

cluster forms 238–244

diagnostics forms 290–291

firewall forms 263–267

global command forms 224–232

monitor forms 234–237

network forms 246–261

operations forms 268–270

Boot user

software reinstall 345

Browser-Based Interface 322

C

Check Point

tuning NG performance 360

cli access

local serial port 123

remote access list 124

secure shell 127

telnet 125

cli basics

idle time-out 131

multiple administration sessions 131

operation 129

shortcuts 134

tab completion 134

Cluster Menu 152

Command Line Interface 322

command syntax and usage

access list menu 155

administrative applications menu 156

boot menu 210

- CA certificate management menu 165
- configuration menu 37, 38, 39, 144
- date and time menu 148, 149
- DNS servers menu 151
- ELA logging menu 176
- firewall configuration menu 206
- firewall license menu 205
- firewall maintenance menu 213
- groups menu 182
- host information menu 152
- http configuration menu 160
- information menu 139
- interface menu 186
- log archiving menu 177
- main menu 136
- miscellaneous settings menu 209
- network configuration menu 183
- NTP servers menu 150
- platform logging menu 173
- port menu 184
- routes menu 202, 203
- SMART clients menu 208
- SNMP administration menu 166
- SNMP users menu 168
- software management menu 211
- SSH administration menu 158
- SSL configuration menu 161
- system logging menu 174
- system menu 147
- Telnet administration menu 157
- trap hosts menu 170, 171
- user admin menu 180, 181
- user menu 178
- web administration menu 159

Command-Line Interface (CLI) 123

commands

- abbreviations 134
- shortcuts 134
- stacking 134
- tab completion 134

D

disconnect idle timeout 131

DNS servers

- add to configuration 151
- list configured 151
- remove configured 151

E

Event Logging API (ELA)

- Check Point SmartCenter Server config 350–354
- Check Point SmartView Tracker 357
- description 349
- firewall configuration 355–357

external routing 321

F

factory default configuration

- after reinstalling software 345

feature summary 21

- BBI 217
- hardware 22
- logging and monitoring 25
- performance 25
- software 21
- system management 25

firewall basics

- management interfaces 27
- network elements 26
- networks 26

firewall policy test rule 79, 86

G

global commands

- nslookup 132

H

help 131

I

idle timeout

- overview 131

internal routing 321

L

license configuration using CLI 54
 license installation on local workstation 92
 lines (display option) 132
 local console 27
 logging features 25

M

major/minor release upgrades 337
 management interfaces
 local console 27
 remote console 27
 SmartCenter Server 27
 management tools overview
 BBI 119
 Check Point interface 119
 cli 119
 memory status 362
 monitoring features 25

N

NAT parameter modifications 361
 network elements 26
 network topology
 example 33
 networks
 semi-trusted 26
 trusted 26
 untrusted 26
 NTP servers
 add to configuration 150, 169, 170
 list configured 150, 168, 170
 remove configured 150, 169, 170
 NTP servers menu 150

O

online help 131
 OSPF
 configuration examples 327
 defining an OSPF domain 328

P

passwords 120
 performance figures 25
 ping 132
 publications
 hard copy 19
 pwd 132

Q

quiet (screen display option) 132

R

reinstalling software 345
 remote access list definition 124
 remote console 27
 routers
 border 321
 peer 321
 routes, advertising 321
 routing
 internal and external 321

S

secure shell (SSH) 127
 shortcuts (CLI) 134
 SmartCenter Server
 installation 64
 SmartCenter Server management station 27
 SmartDashboard
 launch 76
 secure comms w/firewall 79

SNMP

menu options 166, 168, 170

software

reinstall 345

SSH sessions 129

stacking commands (CLI) 134

Support contacts 20

system management features 25

system memory status 362

T

tab completion (CLI) 134

technical publications 19

telnet sessions 127

timeouts

idle connection 131

traceroute 132

troubleshooting

policy download failure 371

poor performance 371, 376

SMART client login failure 372

trust 369, 372

types of upgrades 335

U

upgrade

compatibility issues 334

upgrade tasks

major/minor releases 337

overview 336

reinstalling software 345

upgrade types 335

built-in Check Point software 336

Check Point management station software 336

firewall SSI software 335

user

Boot user for reinstall 345

usernames 120

V

verbose 132

VRRP troubleshooting

active master backup fails 374

both masters are active 375

VRRP Configuration Tips 372