BayRS Version 14.00

Part No. 308613-14.00 Rev 00
September 1999

4401 Great America Parkway
Santa Clara, CA 95054

Configuring BaySecure FireWall-1

NORTEL NETWORKS™

Copyright © 1999 Nortel Networks

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

NORTEL NETWORKS is a trademark of Nortel Networks.

Bay Networks and BN are registered trademarks and ARN, ASN, BayRS, BaySecure, and BCC are trademarks of Nortel Networks.

Windows NT is a registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks NA Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks NA Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks NA Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as “Software” in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH NORTEL NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Nortel Networks NA Inc. (“Nortel Networks”) grants the end user of the Software (“Licensee”) a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Nortel Networks Agent software or other Nortel Networks software products. Nortel Networks Agent software or other Nortel Networks software products are licensed for use under the terms of the applicable Nortel Networks NA Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Nortel Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Nortel Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Nortel Networks’ and its licensors’ confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Nortel Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee’s facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Nortel Networks warrants each item of Software, as delivered by Nortel Networks and properly installed and operated on Nortel Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Nortel Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Nortel Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Nortel Networks will replace defective media at no charge if it is returned to Nortel Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee’s intended results and for the installation, use, and results obtained from the Software. Nortel Networks does not warrant a) that the functions contained in the software will meet the Licensee’s requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Nortel Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Nortel Networks or in accordance with its instructions; (ii) used in conjunction with another vendor’s product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL NORTEL NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF NORTEL NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO NORTEL NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Nortel Networks of any such intended examination of the Software and may procure support and assistance from Nortel Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Nortel Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Nortel Networks copyright; those restrictions relating to use and disclosure of Nortel Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Nortel Networks the Software, user manuals, and all copies. Nortel Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Nortel Networks, 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN NORTEL NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST NORTEL NETWORKS UNLESS NORTEL NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Chapter 1
Overview of the BaySecure FireWall-1 Software

Chapter 2
Installing the FireWall-1 Management Software

Chapter 3
Configuring a Firewall on a Router

Chapter 4
Customizing a Firewall on a Router

Appendix A
Monitoring the Firewall Using BCC show Commands

Appendix B
Upgrading to BayRS Version 14.00

Index

Figures

Preface

This guide describes BaySecure™ FireWall-1 and what you do to start and customize BaySecure FireWall-1 services on a Nortel Networks router.

You can use the Bay Command Console (BCC™) to configure BaySecure FireWall-1 services on a router.

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Nortel Networks BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)

Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command.

Example: If the command syntax is:
ping <*ip_address*>, you enter:
ping 192.32.10.12

bold text

Indicates command names and options and text that you need to enter.

Example: Enter **show ip** {**alerts** | **routes**}.

Example: Use the **dinfo** command.

italic text

Indicates file and directory names, new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore.

Example: If the command syntax is:
show at <*valid_route*>
valid_route is one variable and you substitute one value for it.

`screen text`

Indicates system output, for example, prompts and system messages.

Example: `Set Trap Monitor Filters`

separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

This guide uses the following acronyms:

GUI	graphical user interface
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	local area network
MIB	management information base
TCP/IP	Transmission Control Protocol/Internet Protocol

Hard-Copy Technical Manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase selected documentation sets, CDs, and technical publications through the collateral catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

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 one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	**Telephone Number**
Billerica, MA	800-2LANWAN (800-252-6926)
Santa Clara, CA	800-2LANWAN (800-252-6926)
Valbonne, France	33-4-92-96-69-68
Sydney, Australia	61-2-9927-8800
Tokyo, Japan	81-3-5402-7041

Chapter 1
Overview of the BaySecure FireWall-1 Software

The BaySecure FireWall-1 software builds firewall security features into Nortel Networks router software. It does this by integrating the stateful inspection module from Version 2.1 of the Check Point Software Technologies FireWall-1 software into the Nortel Networks router operating system (BayRS) of Nortel Networks BN®, ASN™, and ARN™ routers.

BaySecure FireWall-1 is a firewall only, and does not include the entire suite of Check Point features. BaySecure FireWall-1 supports the inspection module and logging capabilities of the Check Point FireWall-1 product.

Managing Firewall Operation

A *firewall* is the hardware and/or software that limits the exposure of a computer or network to an attack from an external source.

To control the operation of a firewall on the router, you use the Check Point FireWall-1 management software.

You install this management software on a computer running Windows NT® or UNIX to create a *firewall management station*. From the management station, you can use the FireWall-1 management software to define a security policy and download it to the router. The *security policy* specifies how the firewall operates. For instructions on how to install the FireWall-1 management software, see Chapter 2, “Installing the FireWall-1 Management Software.” To learn how to configure a security policy, see your Check Point documentation.

How the Firewall Software Works

The management station downloads the policy information to the stateful inspection module in the Nortel Networks router software. The *stateful inspection module* inspects all data packets traveling between the data link and network layers, and communicates the results to the management station. (Note that the management station does not inspect the packets.) If the data packets meet the security requirements specified in the security policy, the router forwards the data. If the data packets violate the security policy, the router drops the data packets and logs the information to the management station.

Using Backup Management Stations

You can use the Bay Command Console (BCC) to configure up to two backup management stations. Doing so provides the redundancy required to use FireWall-1 in large enterprise networks. If your router loses communication with its firewall management station, a backup firewall management station automatically establishes communication with the router. As a result, firewall security remains intact and firewall statistics logging continues.

BaySecure FireWall-1 does not require a backup management station to remain dormant until called into service when the firewall management station fails. A backup management station can simultaneously be a working firewall management station for another firewall.

Selecting a Backup Management Station

A router connects to a backup firewall management station upon termination of the TCP connection (with TCP_ABORT) between the current firewall management station and the router.

➡ **Note:** When an event, such as a LAN failure, prevents communication between the router and the firewall management station, the firewall management station closes the TCP connection from its end when data does not flow from the idle TCP connection. However, the router does not close the TCP connection from its end for a period of time determined by the TCP keepalive timer. The TCP keepalive timer in the firewall application on the router periodically checks the TCP connection before the router terminates the idle TCP connection. For information on setting the TCP keepalive timer, see "Setting the Keepalive Timer" on page 4-4.

If the connection between a firewall management station and the router fails, the router begins a round-robin selection process. During this process, the router continuously tries to connect to another management station at 40-second intervals. The order of the round-robin selection is primary, first backup, and then second backup management station.

For example, if the connection between the router and the primary management station fails, the router tries to connect to the first backup management station. If the connection to the first backup management station fails, the router tries to connect to the second backup management station before trying to connect to the primary management station again.

For information about specifying backup management stations, see "Identifying the First Backup Firewall Management Station" on page 3-5, and "Identifying the Second Backup Firewall Management Station" on page 3-5.

Where to Go Next

To get a firewall up and running on your Nortel Networks router, see the following table:

For information about how to	Go to page
Obtain licenses from Check Point	2-1
Install the Check Point Management software	2-5
Create a firewall	3-1
Enable the firewall on the router	3-7
Establish a relationship between the management station and the router	3-3
Enable the router on specific interfaces	3-7
Activate the firewall	3-10
Configure a firewall security policy	3-10, and see your Check Point FireWall-1 documentation
Install the security policy on the router	3-11, and see your Check Point FireWall-1 documentation
Upgrade to BayRS Version 13.20 from an earlier version	B-1

Chapter 2
Installing the FireWall-1 Management Software

To install the FireWall-1 software, see the following topics:

Obtaining Software Licenses

Before you can install the FireWall-1 software and create a firewall on the router, you must first obtain a permanent software license from Check Point Software Technologies for:

- The firewall management station

  You need a software license for the firewall management station (the PC or UNIX workstation that you use to manage the firewall software on the Nortel Networks router). You also need a software license for each backup management station that you configure.

- The router

  You need a BaySecure FireWall-1 agent license for each Nortel Networks router protected by the firewall software. You install the agent license on the management station and not on the router itself.

➡ **Note:** If you want to use a backup management station with the router, you must obtain a second agent license for the router.

Obtaining a FireWall-1 License for the Management Station

To obtain a FireWall-1 license for the firewall management station, follow these instructions:

➡ **Note:** You need one license for each FireWall-1 management station. To obtain a license for each additional management station, you must repeat the steps outlined in this section.

1. **Locate your certificate key.**

   A certificate key (serial number) is located on a sticker on the inside of the CD folder containing the Check Point FireWall-1 management software media. If you lose the certificate key bearing the FireWall-1 serial number, contact Nortel Networks.

2. **Contact Check Point Software Technologies.**

   To obtain a permanent license, you must contact Check Point with your certificate key information. You can reach Check Point in any of these ways:

   - On the World Wide Web at *http://license.CheckPoint.com*
     Most customers prefer to contact Check Point using this method.
   - By sending e-mail to license@checkpoint.com
   - By phoning Check Point:

     800-429-4391 (North America)

     +972-3-613-1833 (outside North America)

   When requesting a license, you must also provide the IP address or UNIX host ID of the management station on which you plan to install the license.

Sample Response from Check Point

```
Your license request with the following details has been accepted.
Below you will find the corresponding license string.

We recommend printing this page and saving it in your files for future
reference.

Request Details
---------------
Certificate Key:    5xxx 5xxx fxxx
Customer Name:      Nortel Networks
Product:            CPFW-ESC-U
Version: 4.0
Host ID:            123.123.123.123

License(s) Issued
-----------------
Host ID:            123.123.123.123
Features:           control
License String:     7xxxxxxx-8xxxxxxx-fxxxxxxx

License(s) Installation
-----------------------
run 'fw putlic 123.123.123.123 7xxxxxxx-8xxxxxxx-fxxxxxxx control '

Contact Information
-------------------
This Check Point product has been purchased through: Nortel Networks
```

Note: If you need to change the IP address of a FireWall-1 management station, contact Check Point at 800-429-4391 (North America) or +972-3-613-1833 (locations outside of North America).

For information about how to install the license, see “Installing and Running the FireWall-1 Management Software” on page 2-5 and the Check Point FireWall-1 documentation.

Obtaining a FireWall-1 License for the Router

To obtain a FireWall-1 license for a router you plan to protect with a firewall, follow these instructions:

➡ **Note:** You need one license for each router that you plan to protect with a firewall. You need an additional license for each router if you want to use the backup management station. To obtain additional licenses, you must repeat the steps outlined in this section.

1. **Locate your certificate key.**

   A certificate key (serial number) is located on a sticker on the inside of the CD folder containing the Check Point FireWall-1 software media. If you lose the certificate key bearing the FireWall-1 serial number, contact Nortel Networks.

2. **Contact Check Point Software Technologies.**

   To obtain a permanent license, you must contact Check Point. To process your request, Check Point requires your certificate key and the IP address of the management station.

   You can reach Check Point in any of these ways:

   - On the World Wide Web at *http://license.CheckPoint.com*
     Most customers prefer to contact Check Point using this method.
   - By sending e-mail to license@checkpoint.com
   - By phoning Check Point:

     800-429-4391 (North America)

     +972-3-613-1833 (outside North America)

   To synchronize the FireWall-1 password on the router and the management station, use the **fw putkey** command. See “Synchronizing the Management Station and the Router Passwords” on page 2-19.

Sample Response from Check Point

```
The following license was generated:
We recommend printing this page and saving it in your files for future
reference.

Request Details
---------------
Certificate Key:    7xxx dxxx 1xxx
Customer Name:      Nortel Networks
Product:            BABN-IM-U
Version:            4.0
Host ID:            012.012.012.012

License Issued
--------------
Host ID:            012.012.012.012
Features:           embedul
License String:     7fff6161-408d3b21-a161c10f

License Installation
--------------------
run 'fw putlic 012.012.012.012 7fff6161-408d3b21-a161c10f embedul '
```

Installing and Running the FireWall-1 Management Software

Once you obtain a FireWall-1 license from Check Point, you can install the Check Point FireWall-1 management software on a computer running either Windows NT or UNIX.

Topic	**Page**
Installing on a Computer Running Windows NT	2-5
Installing on a UNIX Platform	2-12

Installing on a Computer Running Windows NT

Use the following sections as a guide to installing the FireWall-1 management software on a computer running Windows NT. For more details, refer to your Check Point FireWall-1 documentation.

Sample Installation

The following sample installation takes the Check Point FireWall-1 software from a CD and installs it onto a PC running Windows NT. Use this sample installation to familiarize yourself with a basic FireWall-1 installation.

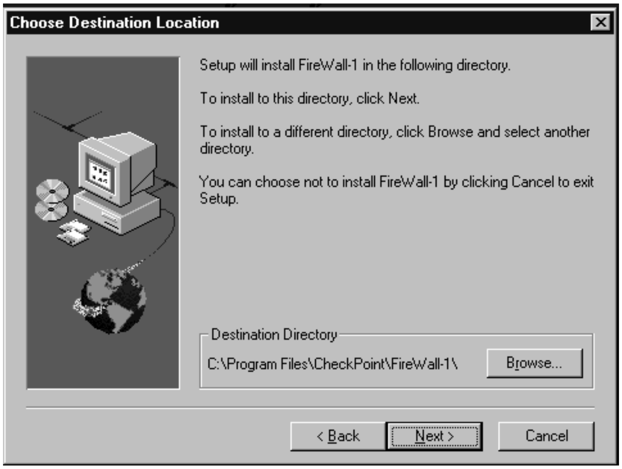
Note: This sample installation shows only those screens necessary for a basic installation. Your installation may be different.

Installing the Management Software

1. **Insert the CD into the CD-ROM drive and run the Setup program, *setup.exe*. To specify the name and location of the program to run, enter (where D is the name of your CD-ROM drive):**

   D:\windows\fw1\setup.exe

   The Choose Destination Location window (Figure 2-1) opens.



Choose Destination Location

Setup will install FireWall-1 in the following directory.

To install to this directory, click Next.

To install to a different directory, click Browse and select another directory.

You can choose not to install FireWall-1 by clicking Cancel to exit Setup.

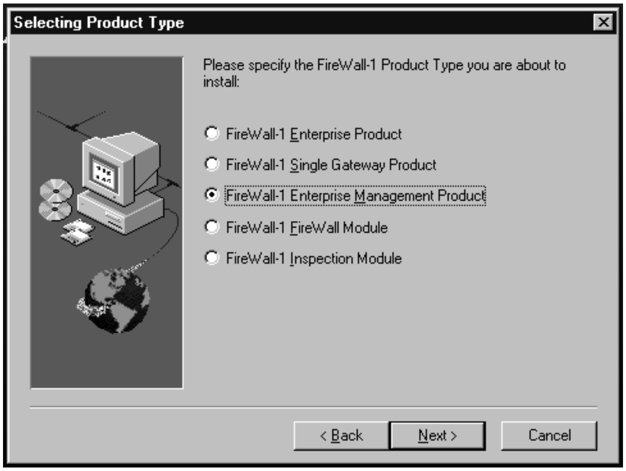
Destination Directory

C:\Program Files\CheckPoint\FireWall-1\

Figure 2-1. Choose Destination Location Window

2. **Choose a destination directory. You can either accept the default directory (Program Files) or make another selection.**
3. **Click on Next.**

The Selecting Product Type window (Figure 2-2) opens.



Selecting Product Type

Please specify the FireWall-1 Product Type you are about to install:

○ FireWall-1 Enterprise Product

○ FireWall-1 Single Gateway Product

● FireWall-1 Enterprise Management Product

○ FireWall-1 FireWall Module

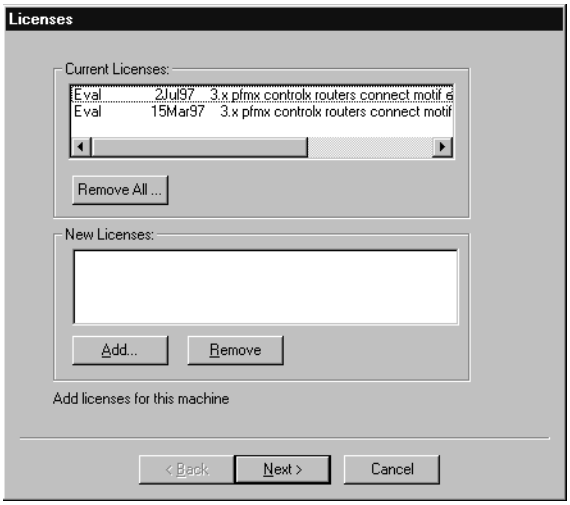
○ FireWall-1 Inspection Module

Figure 2-2. Selecting Product Type Window

4. **Choose FireWall-1 Enterprise Management Product as the FireWall-1 component you want to install.**

5. **Click on Next.**

   The Licenses window (Figure 2-3) opens.



Licenses

Current Licenses:

```
Eval      2Jul97   3.x pfmx controlx routers connect motif e
Eval      15Mar97   3.x pfmx controlx routers connect motif
```

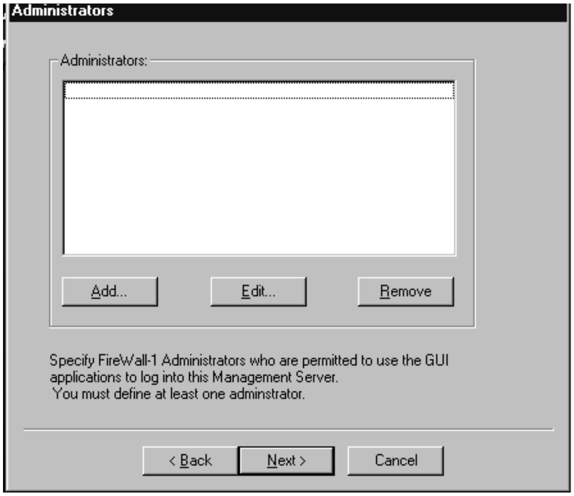
New Licenses:

Add licenses for this machine

Figure 2-3. Licenses Window

6. **Enter the license information you obtained from Check Point.**
7. **Click on Next.**

   The Administrators window (Figure 2-4) opens.



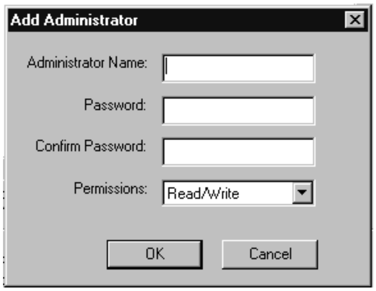
Specify FireWall-1 Administrators who are permitted to use the GUI applications to log into this Management Server.
You must define at least one adminstrator.

Figure 2-4. Administrators Window

You must specify at least one administrator.

8. **Click on Add.**

   The Add Administrator window (Figure 2-5) opens.



Administrator Name:
Password:
Confirm Password:
Permissions: Read/Write

Figure 2-5. Add Administrator Window

9. **Enter the administrator's user name and password (limited to eight characters), and a password confirmation, then click on OK. You return to the Administrators window.**

10. **Click on Next.**

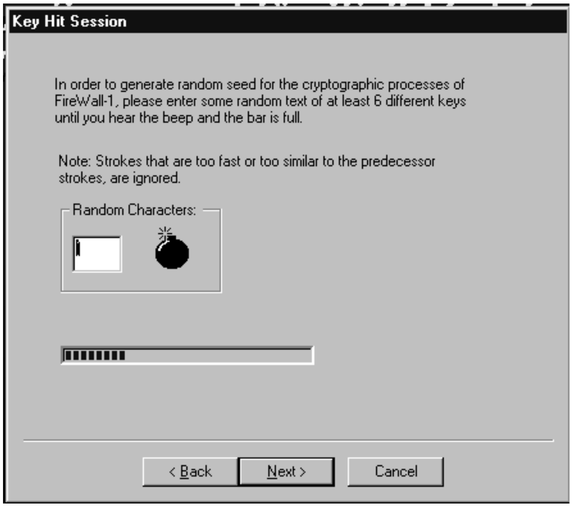
    The GUI Clients window opens. Do not enter any GUI clients at this time.

11. **Click on Next.**

    The Remote Modules window appears. Do not enter any remote modules at this time.

12. **Click on Next.**

    The Key Hit Session window (Figure 2-6) opens.



Key Hit Session

In order to generate random seed for the cryptographic processes of FireWall-1, please enter some random text of at least 6 different keys until you hear the beep and the bar is full.

Note: Strokes that are too fast or too similar to the predecessor strokes, are ignored.

Figure 2-6. Key Hit Session Window

13. **Follow the directions in the window and enter random characters, with a delay of a few seconds between them, until the indicator bar is full.**

    Be sure not to type the same character twice in a row, to vary the delay between the characters.

14. **Click on Next.**

    The CA Key window opens.

15. **Click on Generate to generate a new key.**

    The host uses the RSA key to generate a digital signal for authenticating its communications in its capacity as a Certificate Authority.

    Generating the key may take several minutes.

16. **Click on Finish.**

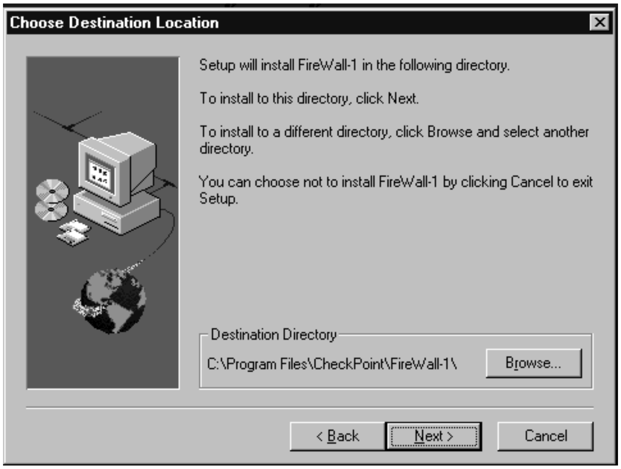
Installing the GUI Client

1. **Insert the CD into the CD-ROM drive and run the *setup.exe* file. To specify the name and location of the program to run, enter (where D is the name of your CD-ROM drive):**

   D:\windows\gui_client\disk1\setup.exe

   The Choose Destination Location window (Figure 2-7) opens.

2. **Choose a destination directory.**



Choose Destination Location

Setup will install FireWall-1 in the following directory.

To install to this directory, click Next.

To install to a different directory, click Browse and select another directory.

You can choose not to install FireWall-1 by clicking Cancel to exit Setup.

Destination Directory

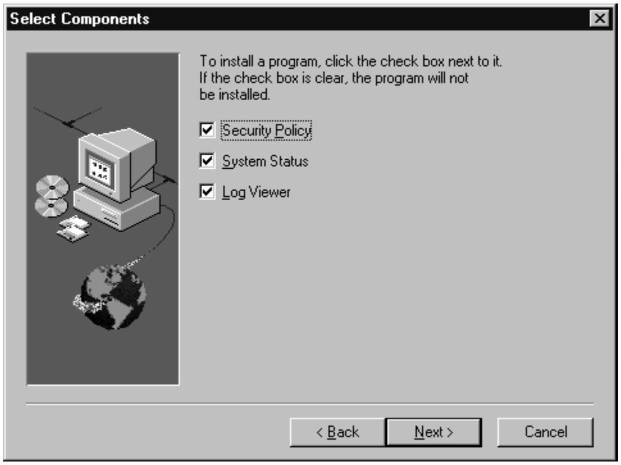
C:\Program Files\CheckPoint\FireWall-1\

Figure 2-7. Choose Destination Location Window

You can either accept the default directory (Program Files) or make another selection.

3. **Click on Next.**

   The Select Components window (Figure 2-8) opens.



Select Components

To install a program, click the check box next to it. If the check box is clear, the program will not be installed.

☑ Security Policy

☑ System Status

☑ Log Viewer

Figure 2-8. Select Components Window

4. **Install the Security Policy, System Status, and Log Viewer components by clicking on each item.**

Customizing the FireWall-1 Installation

You can customize your FireWall-1 installation by running the *FireWall-1 Configuration* file.

To execute the file, enter:

D:\Start\Programs\FireWall-1\FireWall-1 Configuration

Using the *FireWall-1 Configuration* file, you can add:

- A license
- Administrators
- GUI clients
- Remote modules
- CA keys

For more information, refer to your Check Point documentation.

Installing on a UNIX Platform

Use the following sections as a guide to installing the FireWall-1 software on a computer running UNIX. For more details, refer to your Check Point FireWall-1 documentation.

Before You Install

Before you attempt to install the Check Point FireWall-1 software, be sure that you have completed these tasks:

- Obtain a FireWall-1 license for each firewall management station and router that you plan to protect with a firewall.
- Set up the directories that will contain the FireWall-1 information. To do so, add **setenv FWDIR/etc/fw** to your *.cshrc* file, or add **FWDIR=/etc/fw** to your *.cshrc* file and, if using the korn shell, add **export FWDIR** to your *.profile* file; if using the c shell, add **setenv FWDIR** to your *.profile* file.
- Add */etc/fw/bin* to your path.
- Add */etc/fw/man* to your MANPATH environment.

Mounting the CD and Extracting the Tar File

Check Point distributes its FireWall-1 software on CD-ROM. You must supply the UNIX commands to mount the CD drive and extract the tar files.

The commands to mount a CD drive and extract the tar files vary depending on the device name of the CD drive, the operating system used, and other environmental factors. Use the instructions that follow only as guidelines for mounting the CD drive and extracting the tar files. The commands you need may differ.

For SunOS

```
lab#   mount -r -t hsfs /dev/sr0 /cdrom
lab#   cd /tmp
lab#   tar xvf /cdrom/sunos4/fw1/fw.sunos4.tar
```

For Solaris

```
lab#   mount -F hsfs -r /dev/sr0 /cdrom
lab#   cd /tmp
lab#   tar xvf /cdrom/solaris2/fw1/fw.solaris2.tar
```

For HP-UX

```
lab#   mount -r /dev/dsk/c1t2d0 (or your specific CD-ROM address)  /cdrom
lab#   cd /tmp
lab#   tar xvf  “/cdrom/HPUX/FW1/FW.HPUX.TAR;1”
```

Installing the Check Point FireWall-1 Software

Once you have extracted the Check Point FireWall-1 files, you can install the management software. To install the software, change directories so that you’re in the directory where you put the extracted files and then issue the **fwinstall** command.

For example, if you extracted the files into your */tmp* directory, install the software by entering the following commands:

```
lab#   cd /tmp
lab#   ./fwinstall
```

Installation Options

Note that during the installation, the script asks you to select the FireWall-1 option you want to install. To be compatible with BaySecure FireWall-1, enter selection 3, FireWall-1 Enterprise Management Console Product. A sample follows:

```
Which of the following FireWall-1 options do you wish to install?

(1) FireWall-1 Enterprise Product
(2) FireWall-1 Single Gateway Product
(3) FireWall-1 Enterprise Management Console Product
(4) FireWall-1 FireWall Module
(5) FireWall-1 Inspection Module

Enter your selection (1-7/a): 3
```

Sample Installation

The following sample installation takes the Check Point FireWall-1 software from a CD and installs it onto a SparcStation running SunOS. Use this sample installation to familiarize yourself with the FireWall-1 installation script.

Note: In the following sample installation, all user input is in **bold**.

```
**************** FireWall-1 v4.0 Installation ****************

Reading fwinstall configuration.  This might take a while.
Please wait.

Configuration loaded.  Running FireWall-1 Setup.

Checking available options. Please wait.....................

Which of the following FireWall-1 options do you wish to install/
configure ?
------------------------------------------------------------------
-----
(1) FireWall-1 Enterprise Product
(2) FireWall-1 Single Gateway Product
(3) FireWall-1 Enterprise Management Console Product
(4) FireWall-1 FireWall Module
(5) FireWall-1 Inspection Module

Enter your selection (1-5/a): 3

Installing/Configuring FireWall-1 Enterprise Management Console
Product.

Please wait...

Selecting where to install FireWall-1
---------------------------------------
FireWall-1 requires approximately 9017 KB of free disk space.
Additional space is recommended for logging information.

Enter destination directory [/etc/fw]): <Return>

Checking disk space availability...

Installing FW under /etc/fw (50836 KB free)
Are you sure (y/n) [y] ? y

Software distribution extraction
--------------------------------
Extracting software distribution. Please wait ...
Software Distribution Extracted to /etc/fw
Installing license
------------------
Reading pre-installed license file fw.LICENSE... done.
```

```
The following evaluation License key is provided with this
FireWall-1 distribution
Eval             15Mar97    3.x pfmx controlx routers connect motif

Do you want to use this evaluation FW-1 license (y/n) [y]? n

Do you wish to start FireWall-1 automatically from /etc/rc.local
(y/n) [y] ? n


Welcome to FireWall-1 Configuration Program
===========================================
This program will guide you through several steps where you
will define your FireWall-1 configuration. In any later time,
you can reconfigure these parameters by running fwconfig


Configuring Licenses...
=======================
The following licenses are installed on this host:
Eval             15Mar97    3.x pfmx controlx routers connect motif

Do you want to add licenses (y/n) [n] ? n

Configuring Administrators...
=============================
No FireWall-1 Administrators are currently defined for this
Management Station.

Do you want to add users (y/n) [y] ? n


Configuring GUI clients...
==========================
GUI clients are trusted hosts from which FireWall-1 Administrators
are
allowed to log on to this Management Station using Windows/X-Motif
GUI.

Do you want to add GUI clients (y/n) [y] ? n

Configuring Remote Modules...
=============================
Remote Modules are FireWall or Inspection Modules that are going
to be controlled by this Management Station.

Do you want to add Remote Modules (y/n) [y] ? n
```

```
Configuring Groups...
=====================
FireWall-1 access and execution permissions
-------------------------------------------
Usually, FireWall-1 is given group permission for access and
execution.
You may now name such a group or instruct the installation
procedure
to give no group permissions to FireWall-1. In the latter case,
only the
Super-User will be able to access and execute FireWall-1.

Please specify group name [<RET> for no group permissions]:

No group permissions will be granted. Is this ok (y/n) [y] ? y

Configuring Random Pool...
==========================
You are now asked to perform a short random keystroke session.
The random data collected in this session will be used for
generating Certificate Authority RSA keys.

Please enter random text containing at least six different
characters. You will see the '*' symbol after keystrokes that
are too fast or too similar to preceding keystrokes. These
keystrokes will be ignored.

Please keep typing until you hear the beep and the bar is full.

    [                    ] *

Thank you.

Configuring CA Keys...
======================
fw: no license for 'ca'
The installation procedure is now creating an FWZ Certificate
Authority Key
for this host. This can take several minutes. Please wait...
fw: no license for 'ca'

Configuration ended successfully

**************** FireWall-1 is now installed. ****************

Do you wish to start FW-1 now (y/n) [y] ? n
******************************************************************
Configuration ended successfully
```

```
**************** FireWall-1 is now installed. ****************

Do you wish to start FW-1 now (y/n) [y] ? n

******************************************************************
                DO NOT FORGET TO:
1. add the line:    setenv FWDIR /etc/fw   to .cshrc
                or  FWDIR=/etc/fw; export FWDIR to .profile
2. add  /etc/fw/bin  to path
3. add  /etc/fw/man  to MANPATH environment
******************************************************************

You may configure FireWall-1 anytime, by running fwconfig.

**************** Installation completed successfully **************
```

Customizing the FireWall-1 Installation

You can use the **fwconfig** command to customize your FireWall-1 installation. Using **fwconfig**, you can add or remove:

- A license
- Administrators
- Groups
- GUI clients
- Remote modules
- CA keys

Note: To add an administrator, you must first add a group in which the user is a member. If you do not add a group, and if you are logged in as root, then you can run the FireWall-1 GUI using only the **fwui** command.

For more detail, refer to your Check Point FireWall-1 documentation.

Installing a License on the Management Station

To install a FireWall-1 license, enter the license installation command listed in the response message that Check Point displayed when you requested the license. (See the sample Check Point responses on page 2-3 and page 2-5.)

To install the management station's FireWall-1 license, enter the following command from the management station:

fw putlic [*hostid* **|** *ip_address*] <*lic_string*> **control**

To install the FireWall-1 license for a router you plan to protect with a firewall, enter the following command from the management station:

fw putlic [*hostid* | *ip_address*] <*lic_string*> **embedul**

hostid is the UNIX host ID of the management station, and *ip_address* is the IP address of the management station. You enter either the host ID or the IP address, whichever you provided when you requested the license.

lic_string is a string of alphanumeric characters that Check Point provides with your FireWall-1 license.

Starting and Stopping the FireWall-1 Daemons

To *start* the FireWall-1 daemon, enter the following command at the system prompt:

```
lab# fwstart
```

To *stop* the FireWall-1 daemon, enter the following command at the system prompt:

```
lab# fwstop
```

Synchronizing the Management Station and the Router Passwords

Once you have installed licenses on the firewall management station and the router, you must synchronize your password on the two systems. To synchronize the router and the management station passwords, enter the following commands:

- On the firewall management station:

  fw putkey -p *<password> <ip_address_fwall_router>*

- On the router:

  fwputkey <*password> <ip_address_mgmt_station>*

  password is a string of alphanumeric characters that specifies your password.

  ip_address_fwall_router is the IP address of your firewall router.

  ip_address_mgmt_station is the IP address of your FireWall-1 management station.

➡ **Note:** If the management station is managing more than one router, each router should use the same password.

Starting FireWall-1

To start FireWall-1, enter the following command at the system prompt:

```
lab# fwui&
```

Optionally, you can use the FireWall-1 XMotif graphical user interface. For instructions on how to install and start the XMotif GUI, see your Check Point documentation.

Transferring Security Policy and Configuration Files

Firewall backup management stations must have the same security policies and configuration files that the primary firewall management station uses. Nortel Networks has provided script files to make it easy to synchronize firewall management stations. The script files enable you to use a single command, **fwfilex**, to package files associated with a management station's security environment. You then manually transfer the files to other firewall management stations.

Note: The redundant management scripts do not support cross-platform redundancy. You can use these scripts only when transferring from one Windows NT platform to another, or from one UNIX platform to another. If you want to use one platform for your primary backup station and another for your secondary backup station, you must rebuild and install the security policy from scratch on the secondary station.

Getting the Files

You can get the files necessary to synchronize backup stations from two different sources, the BayRS software CD or the World Wide Web, as described in the following sections.

From the BayRS Software CD

The directory *fwbkpscr* contains the subdirectories *unix* and *win*:

- If you are using UNIX systems for your backup management stations, copy the file in the *unix* directory (*fwfilex.*) into the FireWall-1 bin directory (typically */etc/fw/bin*) on your primary backup station.
- If you are using Windows NT systems for your backup management stations, copy the files in the *win* directory (*zip.exe*, *unzip.exe*, and *fwfilex.cmd*) into the FireWall-1 bin directory (typically *\WINNT\FW1\bin*) on your primary backup station.

Note: After you copy the file (*fwfilex.*) to the */etc/fw/bin* directory on the UNIX system serving as the primary backup station, you must rename the file to *fwfilex* so that it no longer has a period (.) at the end.

From the World Wide Web

You can also download the files from the World Wide Web. Complete the following steps:

1. **Use your browser to go to the customer service Web page at this URL:**

   http://support.baynetworks.com/software

2. **Scroll down to Nortel Networks Routers.**
3. **Select Router_Software_v_13.x.**
4. **Click on Go.**
5. **Scroll down to the Firewall Scripts banner and click on the tar file for UNIX platforms or the zip file for Windows NT.**

Note: The redundant management scripts do not support cross-platform redundancy. You can use these scripts only when transferring from one Windows NT platform to another, or from one UNIX platform to another. If you want to use one platform for your primary backup station and another platform for your secondary backup station, you must rebuild and install the security policy from scratch on the secondary station.

Preparing and Transferring Firewall Files Between Windows Platforms

When you complete the following steps, the Windows NT platforms are synchronized and ready to be used in a redundant firewall management configuration:

1. **Ensure that the files *zip.exe*, *unzip.exe*, and *fwfilex.cmd* reside in the FireWall-1 bin directory (typically *\WINNT\FW1\bin*) on the primary backup station. (You can get these files from the BayRS CD or download them from the customer support web page. For instructions, see "Getting the Files" on page 2-20.)**
2. **To package the firewall environment (that is, firewall security policies, logs, objects, and so on) into a single file, navigate to the FireWall-1 bin directory and enter:**

   ```
   c:\WINNT\FW\BIN> fwfilex -i <filename>
   ```

   filename is the name of the zip file that you can transfer to the secondary backup server.

3. **Using FTP, copy, or another transfer utility, manually transfer the file <*filename*>*.zip* to the FireWall-1 bin directory on the secondary Windows NT backup station.**

4. **To unpackage the firewall environment, on the destination machine, enter:**

   ```
   c:\WINNT\FW\BIN> fwfilex -o <filename>.zip
   ```

Preparing and Transferring Firewall Files Between UNIX Platforms

When you complete the following steps, the UNIX platforms are synchronized and ready to be used in a redundant firewall management configuration:

1. **Ensure that the file *fwfilex* resides in the FireWall-1 bin directory (typically */etc/fw/bin*) on the primary backup station. (You get this file from the BayRS CD or download it from the customer support web page. For instructions, see "Getting the Files" on page 2-20.)**

2. **Make sure you have access to the standard UNIX program *tar.***

3. **To package the firewall environment (that is, firewall security policies, logs, objects, and so on) into a single file, navigate to the FireWall-1 bin directory and enter:**

   ```
   station1/etc/fw/bin# fwfilex -i <filename>
   ```

   filename is the name of the file that you can transfer to the secondary backup station.

4. **Using FTP, copy, or another transfer utility, manually transfer the file <*filename*> to the FireWall-1 bin directory on the secondary UNIX backup station.**

5. **To unpackage the firewall environment on the destination machine, enter:**

   ```
   station2/etc/fw/bin# fwfilex -o <filename>
   ```

Chapter 3
Configuring a Firewall on a Router

To configure a firewall on the router, see the following topics:

Effective with the release of BayRS 13.20, the Bay Command Console (BCC) is the only means of managing the BaySecure FireWall-1. See *Using the Bay Command Console (BCC)* for instructions on how to use the BCC.

Creating a Firewall on a Router

Before you can create a firewall on a router, you must first configure and enable IP on the router and enable TCP on all slots on the router. For instructions, see *Quick-Starting Routers*.

This section explains how to create a firewall on a Nortel Networks router using the BCC.

You can also use the Technician Interface, which lets you modify parameters by issuing **set** and **commit** commands that specify the MIB object ID. This process is equivalent to modifying parameters using the BCC. For more information about using the Technician Interface to access the MIB, see *Using Technician Interface Software*.

⛔ **Caution:** The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

Beginning at the top-level BCC box prompt, enter:

ip

The IP global prompt appears.

To create a base firewall configuration on the router, enter:

firewall primary-log-host <*IP_address*> **local-host** <*IP_address*>

The primary log host address is the IP address of the primary firewall management station. The local host address is the IP address of the router to be protected by the firewall.

By default, the firewall is enabled on the router; however, the firewall cannot function unless you have followed the proper licensing sequence. (For information on the firewall licensing procedure, see Chapter 2.) To disable or reenable the firewall on the router, see "Disabling and Reenabling a Firewall on a Router" on page 3-3.

For example, the following command sequence invokes the IP global prompt and creates a base firewall configuration:

```
box# ip
ip# firewall primary-log-host 1.1.1.1 local-host 2.2.2.2
firewall#
```

Disabling and Reenabling a Firewall on a Router

By default, a firewall is enabled when you first create it on the router.

To disable a firewall, navigate to the firewall prompt (for example, **box; ip; firewall**) and enter:

state disabled

For example, the following command disables the firewall on the router:

```
firewall# state disabled
firewall#
```

To reenable a firewall, navigate to the firewall prompt and enter:

state enabled

For example, the following command enables the firewall on the router:

```
firewall# state enabled
firewall#
```

Setting Up Communications Between the Firewall Management Station and the Router

The firewall cannot protect your router until you set up communications between the firewall management station and the router. You must also establish the relationship between each backup firewall management station and the firewall management station it supports.

To establish these relationships, you must use the same IP address you used to obtain FireWall-1 licenses for the router and each firewall management station.

Establishing a Static Route

You may need to establish a static route between the router and the management station before you configure the firewall parameters. By default, FireWall-1 filters in-bound routing protocol packets from RIP or OSPF. Therefore, if your router and firewall management station are on different subnets, you will need to establish a static route on the router, pointing to the management station's subnet; otherwise, your management station will be unable to communicate with the router. For information about creating a static route, see *Configuring IP, ARP, RARP, RIP, and OSPF Services.*

Establishing the Firewall Management Station

The firewall management station is the PC or UNIX workstation where you installed the FireWall-1 software. You use the firewall management station to enforce the firewall security policy that you created for the router. If the rules specify that logging is to occur, the management station also logs all attempted violations of the security policy. (To define a security policy, see "Defining a Firewall Security Policy" on page 3-10. You will also need to consult your Check Point FireWall-1 documentation.)

Use the BCC to identify the management station to the router. Navigate to the firewall prompt (for example, **box; ip; firewall**) and enter:

primary-log-host <*ip_address*>

ip_address is the address of the primary firewall management station. (To view the current primary firewall management station, you can issue the **primary-log-host** command without the IP address.)

For example, the following command specifies as the primary firewall management station the PC or UNIX workstation with the IP address of 2.2.2.2:

```
firewall# primary-log-host 2.2.2.2
firewall#:
```

Identifying the First Backup Firewall Management Station

If your router loses communication with its firewall management station, the router automatically establishes communication with the first backup firewall management station so that firewall security remains intact. The backup firewall management station must be a PC or UNIX workstation on which you installed the following:

- Check Point FireWall-1 management software
- Router licenses for each router you want to protect with the firewall

Use the BCC to specify the first backup firewall management station. Navigate to the firewall prompt (for example, **box; ip; firewall**) and enter:

backup1-log-host <*ip_address*>

ip_address is the address of the first backup firewall management station in the event that the router loses communication with the primary management station. (To view the current first backup firewall management station, you can issue the **backup1-log-host** command without the IP address.)

For example, the following command specifies as the first backup firewall management station the PC or UNIX workstation with the IP address of 3.3.2.2:

```
firewall# backup1-log-host 3.3.2.2
firewall#:
```

Identifying the Second Backup Firewall Management Station

If your router loses communication with its firewall management station and the first backup firewall management station, the router automatically establishes communication with the second backup firewall management station so that firewall security remains intact. The backup firewall management station must be a PC or UNIX workstation on which you installed the following:

- Check Point FireWall-1 management software
- Router licenses for each router you want to protect with the firewall

Use the BCC to specify the second backup firewall management station. Navigate to the firewall prompt (for example, **box; ip; firewall**) and enter:

backup2-log-host <*ip_address*>

ip_address is the address of the second backup firewall management station in the event that the router loses communication with its firewall management station and the first backup firewall management station. (To view the current second backup firewall management station, you can issue the **backup2-log-host** command without the IP address.)

For example, the following command specifies as the second backup firewall management station the PC or UNIX workstation with the IP address of 4.4.2.2:

```
firewall# backup2-log-host 4.4.2.2
firewall#:
```

Identifying the Router

Use the BCC to specify the router protected by the firewall. Navigate to the firewall prompt (for example, **box; ip; firewall**) and enter:

local-host <*ip_address*>

The local host address is the IP address of the router to be protected by the firewall. (To view the current router protected by the firewall, you can issue the **local-host** command with the IP address.)

For example, the following command specifies firewall protection for the router with IP address 5.5.5.5:

```
firewall# local-host 5.5.5.5
firewall#
```

By default, the firewall is automatically enabled on the router. To disable or reenable the firewall, see "Disabling and Reenabling a Firewall on a Router" on page 3-3.

Enabling the Firewall on Router Interfaces

After you have created a firewall on the router, use the BCC to enable it on one or more interfaces. For each interface on which you want to enable the firewall, do the following:

1. Navigate to the IP interface-specific prompt.
2. Add a firewall to the interface.
3. Optionally, specify a firewall name.
4. Optionally, set the policy index.

Note: Once the firewall is protecting your router, and you put firewall protection on a new interface, the new interface will use the default security policy supplied by Check Point, which prevents the new interface from communicating with the router.

You can download your customized security policy to the new interface using the Check Point FireWall-1 command line interface (CLI). You can also use the Check Point FireWall-1 graphical user interface (GUI) to download the security policy. The GUI, however, downloads the same security policy to all interfaces. For further information and instructions, see your Check Point documentation.

Navigating to the Prompt for the IP Interface

To navigate to the IP interface on which you want to enable the firewall, first navigate to the prompt for the slot/connector on which you have configured the IP interface (for example, **box; eth 2/1**). Then enter:

ip address *<ip_address>* **mask** *<address_mask>*

ip_address is the IP address you have assigned to the interface.

address_mask is the mask associated with the IP address.

The prompt for the IP interface appears.

For example, the following command invokes the prompt for IP interface 2.2.2.2/255.0.0.0 (which has been configured on Ethernet slot 2, connector 2):

```
ethernet/2/2# ip address 2.2.2.2 mask 255.0.0.0
ip/2.2.2.2/255.0.0.0#
```

Adding a Firewall to an Interface

When you add a firewall to an IP interface, the firewall is automatically enabled on that interface. To add a firewall to an IP interface, enter:

firewall

The firewall prompt appears. For example, the following command adds a firewall to the IP interface 2.2.2.2/255.0.0.0:

```
ip/2.2.2.2/255.0.0.0# firewall
firewall/2.2.2.2#
```

Note: After you enable a firewall on an interface and reboot the router, you can communicate with the router if you are connected to the console port through a terminal server. However, if you use a Telnet connection to the router (to issue Technician Interface commands), you cannot communicate with the router until you change the FireWall-1 default security policy. For more information, see “Defining a Firewall Security Policy ” on page 3-10.

Caution: If your firewall management station and router are on different subnets, you will not be able to communicate with the router from the management station unless you establish a static route from the management station to the router before you activate the firewall. For information about creating a static route, see *Configuring IP, ARP, RARP, RIP, and OSPF Services*.

Specifying a Firewall Name

Optionally, you can specify a firewall name to associate with the interface. To do so, enter:

firewall-name *<name>*

name is any string of alphanumeric characters that you want to use to identify the interface by name.

For example, the following command assigns the name “offsite” to the firewall on IP interface 2.2.2.2/255.0.0.0:

```
firewall/2.2.2.2# firewall-name offsite
firewall/2.2.2.2#
```

Setting the Policy Index

The policy index allows multiple circuits to share the same instance of Firewall-1. You can have up to 32 instances of Firewall-1, with many circuits making up each Firewall-1 instance. All circuits in a grouping must share the same security policy.

By default, the policy index for a circuit is equal to the circuit number. If you are using Firewall-1 on less than 33 circuits, you do not need to use policy indexes.

If you are using Firewall-1 on more than 32 circuits, group circuits that share the same security policy. Then, set the policy index on each circuit in a group to the same value. For example, suppose you want to use Firewall-1 on 40 circuits. The first five circuits share one security policy; the next 35 share a different security policy. Using the BCC, assign policy index 1 to the first five circuits and policy index 2 to the next 35 circuits. You then have a total of 40 firewall circuits on the router, with two policy index values and two security policies.

➡ **Note:** If you do not use policy index values and you configure more than 32 circuits on the router, all IP forwarding is disabled on circuits after the 32nd. If you use policy index values, but configure more than 32 policy index groupings, all circuits assigned policy indexes after the 32nd will have all IP forwarding disabled. The router logs warning messages that can help you determine if you have any circuits on which all IP forwarding is disabled.

The CheckPoint log viewer treats circuits that share a policy index as one circuit.

To set the policy index value, navigate to the firewall prompt and enter:

policy-index <*value*>

value is the index value from 1 through 1023.

For example, the following command sets the policy index to 1:

```
firewall/2.2.2.2## policy-index 1
firewall/2.2.2.2#
```

Activating the Firewall

Before the FireWall-1 security policy can take effect on the router, you must first activate the firewall by booting the router using the Technician Interface on the management station. Booting a router warm-starts every processor module in the router. Pressing the Reset button on the front panel of the router performs the same procedure.

For information about using the Technician Interface **boot** command, see *Using Technician Interface Software*.

➡ **Note:** When you activate the firewall, the default security policy prevents all interfaces supported by the firewall from communicating with the router. If the firewalled router and management station are on different subnets, you must establish a static route to enable communication between the router and the management station before you activate the firewall. For information about configuring a static route, see *Configuring IP, ARP, RARP, RIP, and OSPF Services.*

Defining a Firewall Security Policy

A *security policy* is a collection of rules that define the way the firewall operates. The default FireWall-1 security policy drops all attempts at communication with the router. This security policy goes into effect when you first activate the firewall on the router.

You must establish a security policy that explicitly defines acceptable communication to the router, based on the source address, destination address, and type of service. For details about how to configure a security policy, see your Check Point FireWall-1 documentation.

Installing the Security Policy on the Router and Its Interfaces

Once you have defined a security policy, you must install it on the router. Installing a security policy means downloading it to the firewalled objects that will enforce it.

When you download the security policy, the FireWall-1 software:

- Verifies that the rule base is logical and consistent
- Generates an inspection script from the rule base
- Compiles the inspection script to generate inspection code for the router
- Downloads the inspection code to the router

➡ **Note:** Once the firewall is protecting your router, if you put firewall protection on a new interface, the new interface will use the default security policy supplied by Check Point, which prevents the new interface from communicating with the router.

You can download your customized security policy to the new interface using either the Check Point FireWall-1 command line interface or the Check Point FireWall-1 graphical user interface (GUI). The GUI, however, downloads the same security policy to all interfaces.

For instructions on how to install the security policy, see your Check Point FireWall-1 documentation.

Troubleshooting Checklist

If you experience problems with the FireWall-1 software, verify that you have performed these steps:

- Enabled IP on the router
- Enabled TCP on all slots on the router
- Created a firewall using the BCC
- Created a static route if the router and firewall management stations are on different subnets
- Synchronized the router and management station passwords by executing the **fwputkey** command on both the router and the firewall management station
- Defined a security policy and added a network object for the router using the FireWall-1 graphical user interface
- Saved the configuration and booted the router
- Installed the security policy on the router

If you have performed these steps and are still having system problems, contact your Nortel Networks Technical Solutions Center.

Chapter 4
Customizing a Firewall on a Router

To customize a firewall on the router, see the following topics:

Effective with the release of BayRS 13.20, the Bay Command Console (BCC) is the sole means of managing the BaySecure FireWall-1. See *Using the Bay Command Console (BCC)* for instructions on how to use the BCC.

Specifying FireWall-1 Memory

You can specify the maximum and minimum amount of memory that FireWall-1 uses. By default, the minimum amount of memory is 50,000 bytes. The maximum amount of memory is 100,000 bytes.

Caution: We recommend that you accept the default memory allocation settings. If you change them, you may see unexpected and undesired results.

To set the maximum amount of FireWall-1 memory, navigate to the firewall prompt (for example, **box; ip; firewall**) and enter:

max-hmemory *<memory>*

memory is any integer value representing the number of bytes you want to allocate.

For example, the following command sets the maximum memory allocated to 200,000 bytes:

```
firewall# max-hmemory 200000
```

To set the minimum amount of FireWall-1 memory, navigate to the firewall prompt (for example, **box; ip; firewall**) and enter:

min-hmemory *<memory>*

memory is any integer value representing the number of bytes you want to allocate.

For example, the following command sets the minimum memory allocated to 100,000 bytes:

```
firewall# min-hmemory 100000
```

Setting the Firewall Filter Timer

The firewall filter timer is the number of seconds between attempts to download the firewall security policy from the backup management station if the download is not successful from the primary firewall management station. The default interval is 40 seconds. You can use the BCC to specify a new value for the filter timer.

Navigate to the firewall prompt (for example, **box; ip; firewall**) and enter:

filter-timer <*interval*>

interval is the number of seconds, from 20 to 180.

For example, the following command sets the filter timer to 90 seconds:

```
firewall# filter-timer 90
firewall#
```

Setting the Log Timer

The log timer is the number of seconds between attempts to write to the log on the backup management station if logging is not successful on the primary firewall management station. The default interval is 40 seconds. You can use the BCC to specify a new value for the log timer.

Navigate to the firewall prompt (for example, **box; ip; firewall**) and enter:

log-timer <*interval*>

interval is the number of seconds, from 20 to 180.

For example, the following command sets the log timer to 90 seconds:

```
firewall# log-timer 90
firewall#
```

Specifying a Timeout Period for an Inactive TCP Connection

If a TCP connection is inactive for a certain period of time, the router sends a TCP keepalive message, and expects an acknowledgment (ACK) from the management station. If the router does not receive the ACK from the management station, it retransmits the keepalive message. If after retransmitting the keepalive message the router does not receive an ACK from the management station, the TCP connection is disabled.

You can control the timeout period for an inactive TCP connection using the following:

- Keepalive timer **-** specifies the number of seconds that a TCP connection can remain inactive before the router sends a TCP keepalive message to the management station.
- Keepalive retransmit timer **-** specifies the interval, in seconds, at which a router retransmits unacknowledged keepalive messages to the management station.
- Keepalive timer retries **-** specifies the number of times to retransmit an unacknowledged keepalive message. If after the number of retries the router does not receive an ACK from the management station, the TCP connection is disabled.

The following sections describe the BCC commands you can use to control the timeout period.

Setting the Keepalive Timer

The keepalive timer specifies the number of seconds that a TCP connection can remain inactive before the router sends a TCP keepalive message to the management station. The default keepalive timer value is 180 seconds. You can use the BCC to specify a new value.

Navigate to the firewall prompt (for example, **box; ip; firewall**) and enter:

idle-time-keepalive <*interval*>

interval is the number of seconds, from 0 to 3600. A value of 0 disables the keepalive feature.

For example, the following command disables the keepalive feature:

```
firewall# idle-time-keepalive 0
firewall#
```

Setting the Keepalive Retransmit Timer

The keepalive retransmit timer specifies the interval, in seconds, at which a router retransmits unacknowledged keepalive messages to the management station. The default keepalive timer value is 5 seconds. You can use the BCC to specify a new value.

Navigate to the firewall prompt (for example, **box; ip; firewall**) and enter:

retry-timeout-keepalive <*interval*>

interval is the number of seconds, from 0 to 600. A value of 0 prevents the router from transmitting keepalive messages. The TCP connection is disabled once the keepalive retransmit timer expires.

For example, the following command sets the keepalive retransmit timer to 25 seconds:

```
firewall# retry-timeout-keepalive 25
firewall#
```

Setting the Keepalive Timer Retries

You can specify the number of times to retransmit an unacknowledged keepalive message. If after the number of retries the router does not receive an ACK from the management station, the TCP connection is disabled. The default number of retries is 10. You can use the BCC to specify a new value.

Navigate to the firewall prompt (for example, **box; ip; firewall**) and enter:

retries-keepalive <*value*>

value is the number of retries, from 0 to 100. A value of 0 causes the router to retransmit only one keepalive message.

For example, the following command sets the keepalive retransmit timer to 5 seconds:

```
firewall# retries-keepalive 5
firewall#
```

Deleting a Firewall

You can use the BCC to delete the global firewall (removing the firewall from all interfaces on the router) or to delete a firewall from specific interfaces.

Caution: Deleting the global firewall deletes the MIB. This action disables the FireWall-1 functionality on the router.

To delete the global firewall, thereby removing the firewall from all interfaces on the router, navigate to the firewall prompt (for example, **box; ip; firewall**) and enter:

delete

For example, the following command deletes the firewall on the router:

```
firewall# delete
ip#
```

To delete a firewall from a specific interface, navigate to the firewall prompt for the interface from which you want to remove the firewall (for example, **box; eth 2/1; ip address 2.2.2.2 mask 255.255.255.0; firewall**) and enter:

```
firewall/2.2.2.2# delete
ip/2.2.2.2/255.255.255.0#
```

Appendix A
Monitoring the Firewall Using BCC show Commands

This appendix describes how to use the BCC **show** command to obtain BaySecure FireWall-1 statistical data from the management information base (MIB). The type and amount of data displayed depend on the specific settings you want to view. This appendix includes descriptions of the following **show** commands:

Command	**Page**
show firewall interfaces	A-2
show firewall summary	A-3

Online Help for show Commands

To display a list of command options, enter **show firewall ?** at any BCC prompt. To learn more about any **show firewall** command option and its syntax, use the question mark (**?**) command as follows:

Example

```
bcc> show firewall?
interfaces    summary
bcc> show interfaces ?
show firewall interfaces
     No further options available
bcc>
```

show firewall interfaces

The **show firewall interfaces** command displays information about the interfaces on which firewall is configured.

The output includes the following information:

IP Address	Internet address of the interface on which a firewall is configured.
Cct Name	Name of the circuit associated with the IP interface.
Policy Index	Value that lets circuits share the same virtual machine. For circuits to share a virtual machine, the circuits must have the same policy index.
Firewall Name	Name identifying the interface.
State	State of the interface: up, down, init (initializing), or not pres (not present).

show firewall summary

The **show firewall summary** command displays the current firewall configuration.

The output includes the following information:

State	State of the firewall on the router: enabled or disabled.
Version	Firewall protocol version number.
Firewall Operational State	State of the interface: up, down, init (initializing), or not pres (not present).
Local Host	IP address of the router protected by the firewall.
Primary Log Host	IP address of the primary firewall management station.
Log Host 1backup	IP address of the first backup firewall management station.
Log Host 2backup	IP address of the second backup management station.
Fast Path	Reserved for future enhancements.
Default Policy	Default policy on the router: block all or pass all.
Filter Timer	Interval, in seconds, between attempts to download the filter from the backup management station if the download is not successful from the primary firewall management station.
Log Timer	Interval, in seconds, between attempts to write to the log on the backup management station if logging is not successful on the primary firewall management station.
Idle Timer Keepalive	Number of seconds that a TCP connection can remain inactive before the local TCP host sends a TCP keepalive message to the peer.
Retry Timeout Keepalive	Interval, in seconds, at which a local TCP host retransmits unacknowleged keepalive messages to the peer.
Retries Keepalive	Number of unacknowledged keepalive messages that the local TCP host retransmits before the TCP session is terminated.

Appendix B
Upgrading to BayRS Version 14.00

This appendix describes the procedure you must follow if you are upgrading to BayRS Version 14.00 from an earlier version of BaySecure FireWall-1.

To upgrade to FireWall-1 in BayRS Version 14.00, complete the following steps:

1. **Familiarize yourself with the Bay Command Console (BCC).**

   Starting with BayRS Version 13.20, FireWall-1 no longer supports Site Manager as a configuration tool. You must use the BCC to manage and configure FireWall-1. Chapters 3 and 4 of this manual explain how to use the BCC to configure and customize FireWall-1. For basic information about using the BCC, see *Using the Bay Command Console (BCC)*.

2. **Make sure you will not lose access to your router.**

   When you upgrade to BayRS Version 14.00, after you boot your router, the Version 14.00 software invokes the default FireWall-1 security policy. This default security policy blocks all attempts at communication with the router.

   If you are managing a router at a remote location, you will no longer be able to gain access to the router through the WAN connection. Before you upgrade, make sure that you can gain access to the router by dialing in through the console port, or that there is somebody at the remote location who can configure the router.

3. **Reboot the router with BayRS Version 14.00, using an existing configuration file.**

4. **Use the BCC to reenable FireWall-1 on each IP interface.**

   You must reenable FireWall-1 on each IP interface that you want to protect with a firewall.

To reenable firewall on each IP interface, use the BCC to navigate to the prompt for the slot/connector on which you have configured the IP interface (for example, **box; eth 2/2**). Then enter:

ip address *<ip_address>* **mask** *<address_mask>*

ip_address is the IP address you have assigned to the interface.

address_mask is the mask associated with the IP address.

The prompt for the IP interface appears.

For example, the following command invokes the prompt for IP interface 2.2.2.2/255.0.0.0 (which has been configured on Ethernet slot 2, connector 2):

```
ethernet/2/2# ip address 2.2.2.2 mask 255.0.0.0
ip/2.2.2.2/255.0.0.0#
```

At the prompt for the IP interface, enter the following command to reenable firewall:

firewall

The firewall prompt appears. For example, the following command reenables firewall on the IP interface 2.2.2.2/255.0.0.0:

```
ip/2.2.2.2/255.0.0.0# firewall
firewall/2.2.2.2#
```

5. **To use FireWall-1 on more than 32 circuits, set the policy index number for each IP interface.**

   The policy index allows multiple IP interfaces to share the same instance of FireWall-1. You can have up to 32 instances of FireWall-1 on the router, with many IP interfaces making up each FireWall-1 instance. All interfaces that make up an instance grouping must share the same security policy.

   By default, the policy index for each interface is the same as the circuit number. If you are using FireWall-1 on 32 or fewer circuits, you do not need to configure the policy index number.

If you are using FireWall-1 on more than 32 circuits, you must group circuits with the same security policy and assign those circuits the same policy index number. For example, you might have a group of five IP interfaces to which you assign policy index 1. Those five IP interfaces count as one instance of firewall on the router; they all share the same security policy. You could assign policy index number 2 to another group of 35 interfaces that share a different security policy. You would then have a total of two firewall instances on the router, with two policy index values and two security policies.

If you are running FireWall-1 on more than 32 circuits and you therefore need to set the policy index value, use the BCC to navigate to the firewall prompt, as described in step 4. Then enter:

policy-index *<value>*

value is the index value, from 1 through 1023.

For example, the following command sets the policy index to 1:

```
firewall/2.2.2.2# policy-index 1
firewall/2.2.2.2#
```

6. **Save the configuration file and reboot the router.**
7. **Reinstall the security policy.**

Since you previously defined a security policy (using the earlier version of BaySecure FireWall-1), you do not need to define it again. However, you must reinstall it on the router. For complete instructions on how to install the security policy, see your Check Point FireWall-1 documentation.

If you want to install different security policies for different policy indexes, use the Check Point FireWall-1 command line interface to enter the following command:

fw load ../conf/*<config_file>* **pol***<policy_index_number>@<router_name>*

For example, the following command installs the security policy in the configuration file *drop_ftp* on policy index number 1 on router *asn1:*

fw load ../conf/drop_ftp pol1@asn1

Preventing Spoofing with FireWall-1

You can configure FireWall-1 to eliminate the possibility of *spoofing*, that is, someone violating the firewall by sending a packet with a source address from within the network. To configure FireWall-1 to eliminate spoofing, complete the following steps:

1. **Make sure that each firewalled interface has a unique policy index number. For best results, make sure that each circuit has a unique policy index number.**

   For example, suppose your router has three Ethernet interfaces to LANs protected by the firewall and one frame relay synchronous firewalled connection that includes multiple PVCs. Each Ethernet interface must have a unique policy index number. You may assign the same policy index number to each of the frame relay PVCs if necessary, although configuring the interfaces in this way allows each frame relay interface to spoof the other frame relay interfaces.

2. **Enter the BCC show command, show firewall interfaces, to note the policy index number for each router circuit.**
3. **In the Check Point user interface, click on Manage Network Objects.**
4. **Highlight the defined router object (you may need to create a router) and click on Edit.**
5. **Click on the Interfaces tab.**
6. **Click on SNMP Get. (Ignore the outdated pop-up message.)**
7. **Highlight a circuit and click on Edit.**
8. **In the Name field, type pol.**
9. **In the Num field, type the policy index number of the circuit (which you noted from the BCC show command in step 2).**
10. **Repeat steps 7 through 9 for each firewalled circuit.**

For more information about preventing spoofing, refer to your Check Point documentation.

Index