Check Point FireWall-1 Guide

NG FP3

For additional technical information about Check Point products, consult Check Point’s SecureKnowledge at

http://support.checkpoint.com/kb/

Part No.: 700527
September 2002
LICENSE:

Copyright 1997 by Carnegie Mellon University. All Rights Reserved.

Carnegie Mellon University. The following statements refer to those portions of the software copyrighted by
Portions of the software copyright
University of Michigan. The following statements refer to those portions of the software copyrighted by
Verisign is a trademark of Verisign Inc.

The products described in this document are protected by U.S. Patent No. 5,606,668, 5,699,431 and 5,835,726 and may be protected by other U.S. Patents, foreign patents, and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the 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 and FAR 52.227-19.

TRADEMARKS:

Check Point, the Check Point logo, ClusterXL, ConnectControl, FireWall-1, FireWall-1, FireWall-1 Gateway, FireWall-1 SecureServer, FireWall-1 SmallOffice, FireWall-1 VSA, Firewall-1, FLOODGATE-1, INSPECT, INSPECT XL, IQ Engine, Open Security Extension, OPSEC, Provider-1, SecureKnowledge, SecurePlatform, SecureXL, SiteManager-1, SmartCenter, SmartService, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SVN, UAM, User-to-Address Mapping, UserView, VPN-1, VPN-1 Accelerator Card, VPN-1 appliance, VPN-1 Certificate Manager, VPN-1 Gateway, VPN-1 Net, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecureClient, VPN-1 SecureRemote, VPN-1 SecureServer VPN-1 SmallOffice and VPN1 VSA are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

The products described in this document are protected by U.S. Patent No. 5,606,668, 5,699,431 and 5,835,726 and may be protected by other U.S. Patents, foreign patents, and pending applications.

THIRD PARTIES:

Entrust is a registered trademark of Entrust Technologies, Inc. in the United States and other countries. Entrust’s logos and Entrust product and service names are also trademarks of Entrust Technologies, Inc. Entrust Technologies Limited is a wholly owned subsidiary of Entrust Technologies, Inc. FireWall-1 and SecuRemote incorporate certificate management technology from Entrust.

Verisign is a trademark of Verisign Inc.

The following statements refer to those portions of the software copyrighted by University of Michigan.

Portions of the software copyright © 1992-1996 Regents of the University of Michigan. All rights reserved. Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty. Copyright © Sax Software (terminal emulation only).

The following statements refer to those portions of the software copyrighted by Carnegie Mellon University.

Copyright 1997 by Carnegie Mellon University. All Rights Reserved. Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The following statements refer to those portions of the software copyrighted by The OpenSSL Project.

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 *
POTENTIAL POSSIBILITY OF SUCH DAMAGE. * The following statements refer to those portions of the software copyrighted by Eric Young.

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 CONTRIBU

TORS 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.

Copyright © 1998 The OpenSSL Project.

Check Point Software Technologies Ltd.

International Headquarters:
3A Jabotinsky Street
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256
e-mail: info@CheckPoint.com

Please direct all comments regarding this publication to techwriters@checkpoint.com.

U.S. Headquarters:
Three Lagoon Drive, Suite 400
Redwood City, CA 94065
Tel: 800-429-4391; (650) 628-2000
Fax: (650) 654-4233
http://www.checkpoint.com
# Table Of Contents

## Preface
- Who Should Use this User Guide 9
- Summary of Contents 9
- Check Point Documentation 10
- What Typographic Changes Mean 12
- Shell Prompts in Command Examples 13
- Network Topology Examples 13

## Chapter 1  SmartDefense
- Overview 15
- Configuring SmartDefense 16
- Anti Spoofing Configuration 17
- Denial of Service 18
  - Teardrop 20
  - Ping of Death 21
  - LAND 22
- IP and ICMP 22
  - Fragment Sanity Check 24
  - Packet Sanity 25
  - Max Ping Size 26
- TCP 26
  - SYN Attack 27
  - Small PMTU 30
  - Sequence Verifier 32
- DNS 33
- FTP 34
  - FTP Bounce Attack 35
  - FTP Security Server 36
- HTTP 42
  - General HTTP Worm Catcher 43
  - HTTP Security Server 44
- SMTP Security Server 48
  - SMTP Content 49
  - Mail and Recipient Content 50
- Successive Events 52
  - Address Spoofing 53
  - Port Scanning 55
  - Local Interface Spoofing 56
  - Successive Alerts 57
  - Successive Multiple Connections 58
- SYN Attacks and SYNDefender 58
  - Guidelines for Deploying SYNDefender 64
Chapter 2  Network Address Translation (NAT)

Introduction  67
- The Need for Address Translation  67
- Example  69
Configuring Network Address Translation  70
- Address Translation Modes  70
  - Hide Mode  71
  - Statically Translating Addresses  75
Address Translation and Routing  78
- Configuring Routing on the Gateway  78
IANA Recommendations  86
- Supported Services  86
  - Restrictions  86
  - FTP port command  87
Generating Address Translation Rules Automatically  87
- Overview  87
Network Address Translation Rule Base  89
- Overview  89
  - Structure of a NAT Rule  89
  - NAT Rule Base Example  91
Defining Address Translation Rules  93
- Using the NAT Rule Base Editor  93
Address Translation Examples  102
- Gateway with Two Interfaces  102
- Gateway with Three Interfaces  106
Advanced Topics  112
- Rule Base  112
- Overlapping NAT  113
Implementation  116
- Frequently Asked Questions  116

Chapter 3  Authentication

Overview  123
- VPN-1/FireWall-1 Authentication  123
  - Three Types of Authentication  124
User Authentication  126
- Overview  127
- Deployment  127
Non-Transparent User Authentication  140
- User Authentication and the HTTP Security Server  142
Session Authentication  162
- Overview  162
- Deployment  164
Client Authentication  173
- Overview  173
- Deployment  177
Single Sign On — Additional Features  190
- Examples of Sign On Methods  193
# Table of Contents

Encrypted Client Authentication 201  
Client Authentication — Security Considerations 202  
Client Authentication — Additional Features 202

## Chapter 4  Security Servers and Content Security

Security Servers 205  
Overview 205  
Security Servers and the Rule Base 208  
Interaction with OPSEC Products 222  
Defining Security Servers 224

Content Security 227  
Resources and Security Servers 228  
Web (HTTP) 230  
Mail (SMTP) 233  
FTP 234  
CVP Inspection 234  
CVP Load Sharing and Chaining 236  
Security Server Configuration 237

fwauthd.conf file 237

## Chapter 5  ClusterXL

Installing and Licensing ClusterXL 241  
State Synchronization 243  
Full and Delta Synchronization 243  
Secured Interfaces 244  
Implementing Synchronization 244  
Selective Synchronization 245  
Different Routes for Connections (Asymmetric Routing) 246  
Timing Issues 247  
Synchronized Cluster Restrictions 248  
Troubleshooting State Synchronization 249

Check Point High Availability and Load Sharing Solutions 250  
High Availability—Overview 250  
Load Sharing—Overview 250  
High Availability Modes 251  
Improvements in Load Sharing 252  
When Does a Failover Occur? 252  
What Happens When a Gateway Recovers? 253  
VLAN Support 253  
How a Recovered Cluster Member Obtains the Latest Security Policy 253

Cluster Protocols 254  
Configuring High Availability and Load Sharing 255  
Example New CPHA and Load Sharing Topology 255  
Example Legacy CPHA Topology 257  
Moving from a Single Enforcement Module to Load Sharing or New CPHA 260  
Configuring Load Sharing or New CPHA from Scratch 264  
Moving Between New CPHA and Load Sharing 268  
Moving from Legacy CPHA to New CPHA or Load Sharing 268
<table>
<thead>
<tr>
<th>Table of Contents</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN-1/FireWall-1 HP OpenView Extension 310</td>
<td></td>
</tr>
<tr>
<td>Installing the FireWall-1 HP OpenView Extension 310</td>
<td></td>
</tr>
<tr>
<td>Uninstalling the VPN-1/FireWall-1 HP OpenView Extension 312</td>
<td></td>
</tr>
<tr>
<td>Viewing FireWalled Objects 312</td>
<td></td>
</tr>
<tr>
<td>VPN-1/FireWall-1 MIB Source 314</td>
<td></td>
</tr>
<tr>
<td><strong>Chapter 9</strong></td>
<td><strong>ConnectControl — Server Load Balancing</strong></td>
</tr>
<tr>
<td>The Need for Server Load Balancing 319</td>
<td></td>
</tr>
<tr>
<td>How Server Load Balancing Works 320</td>
<td></td>
</tr>
<tr>
<td>Load Balancing using HTTP Logical Server 320</td>
<td></td>
</tr>
<tr>
<td>Load Balancing using Non–HTTP Logical Server 321</td>
<td></td>
</tr>
<tr>
<td>Load Balancing Algorithms 322</td>
<td></td>
</tr>
<tr>
<td>Defining Logical Servers 322</td>
<td></td>
</tr>
<tr>
<td>Rule Base 325</td>
<td></td>
</tr>
<tr>
<td>Using HTTP Logical Servers in a Rule 325</td>
<td></td>
</tr>
<tr>
<td>Using non–HTTP Logical Servers in a Rule 325</td>
<td></td>
</tr>
<tr>
<td>Load Measuring 325</td>
<td></td>
</tr>
<tr>
<td><strong>Chapter 10</strong></td>
<td><strong>FAQ (Frequently Asked Questions)</strong></td>
</tr>
<tr>
<td>Defining Objects and Services 327</td>
<td></td>
</tr>
<tr>
<td>Daemons 332</td>
<td></td>
</tr>
<tr>
<td>Security Servers 333</td>
<td></td>
</tr>
<tr>
<td>Logging 337</td>
<td></td>
</tr>
<tr>
<td>Security 338</td>
<td></td>
</tr>
<tr>
<td>VPN-1/FireWall-1/n (VPN-1/FireWall-1/25, VPN-1/FireWall-1/50, etc.) Issues 339</td>
<td></td>
</tr>
<tr>
<td>Supported Protocols and Interfaces 341</td>
<td></td>
</tr>
<tr>
<td>Inspecting 342</td>
<td></td>
</tr>
<tr>
<td>342</td>
<td></td>
</tr>
<tr>
<td>Administrative Issues 343</td>
<td></td>
</tr>
<tr>
<td>Performance 344</td>
<td></td>
</tr>
</tbody>
</table>
Preface

Who Should Use this User Guide

This User Guide is written for system administrators who are responsible for maintaining network security. It assumes you have a basic understanding and a working knowledge of:

- system administration
- the Unix or Windows operating system
- the Windows GUI
- Internet protocols (IP, TCP, UDP etc.)

Summary of Contents

Chapter 1, “SmartDefense,” describes Check Point’s SmartDefense feature, which actively protects an organization from known and unknown network attacks by using intelligent security technology.

Chapter 7, “Boot Security,” describes how Check Point implements security immediately upon boot, even before VPN-1/FireWall-1 fully loads.

Chapter 2, “Network Address Translation (NAT),” describes VPN-1/FireWall-1’s Network Address Translation feature.

Chapter 3, “Authentication,” describes VPN-1/FireWall-1’s Authentication features.


Chapter 9, “ConnectControl — Server Load Balancing,” describes VPN-1/FireWall-1 ConnectControl and Connection Accounting.

Chapter 6, “VoIP (Voice Over IP),” describes Check Point protection for Voice Over IP connections.
Chapter 5, “ClusterXL,” describes State Synchronization, High Availability (redundancy) and Load Sharing features for VPN/FireWall Modules in a gateway cluster.

Chapter 8, “SNMP and Network Management Tools,” describes how VPN-1/FireWall-1 interacts with network management tools.

Chapter 10, “FAQ (Frequently Asked Questions),” is a compilation of Frequently Asked Questions about VPN-1/FireWall-1.

Check Point Documentation

User Guides are available for each product in Portable Document Format (PDF) in the Check Point Enterprise Suite. The Adobe Acrobat Reader is required to view PDF files and is also available on the Check Point Enterprise Suite CD-ROM. Alternatively, you can download the Acrobat Reader from the Adobe Web site (http://www.adobe.com).

The following User Guides are available for Check Point Enterprise Suite products.

1) Check Point Getting Started Guide — This book is an introduction to Check Point products.

2) Check Point SmartCenter Guide — This book describes the Check Point Management GUI, which is used to manage VPN-1/FireWall-1 and other Check Point products.

3) Check Point FireWall-1 — This book describes Check Point VPN-1/FireWall-1.

4) Check Point Virtual Private Networks — This book describes the Check Point VPN-1/FireWall-1 encryption features.

5) Check Point Desktop Client Guide — This book describes Check Point security as implemented by SecuRemote and SecureClient.

6) Check Point FloodGate-1 — This book describes Check Point FloodGate-1, which enables administrators to manage the quality of service on their networks.

7) Check Point Real Time Monitor — This book describes the Check Point Real Time Monitor, which enables administrators to monitor quality of service on their network links, as well as Service Level Agreement compliance.

8) Check Point Provider-1 — This book describes Check Point Provider-1/SiteManager-1, which enables service providers and managers of large networks to provide Check Point products-based services to large numbers of subscribers.
9) *Check Point Reporting Module* — This book describes the Check Point Reporting Module, which enables administrators to manage databases of Check Point log-based information.

10) *Check Point UserAuthority* — This book describes Check Point UserAuthority, which enables third-party and Web applications to leverage Check Point’s sophisticated authentication and authorization technologies.

11) *Check Point User Management* — This book describes Check Point LDAP-based user management.

**Note** - For additional technical information about Check Point products, consult Check Point’s SecureKnowledge database at [http://support.checkpoint.com/kb/](http://support.checkpoint.com/kb/)
What Typographic Changes Mean

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

**TABLE P-1** Typographic Conventions

<table>
<thead>
<tr>
<th>Typeface or Symbol</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>AaBbCc123</td>
<td>The names of commands, files, and directories; on-screen computer output</td>
<td>Edit your <code>.login</code> file. Use <code>ls -a</code> to list all files. <code>machine_name%</code> You have mail.</td>
</tr>
<tr>
<td>AaBbCc123</td>
<td>What you type, when contrasted with on-screen computer output</td>
<td><code>machine_name%</code> su</td>
</tr>
<tr>
<td>AaBbCc123</td>
<td>Command-line placeholder: replace with a real name or value</td>
<td>To delete a file, type <code>rm filename</code>.</td>
</tr>
<tr>
<td>AaBbCc123</td>
<td>Book titles, new words or terms, or words to be emphasized</td>
<td>Read Chapter 6 in <em>User's Guide</em>. These are called <code>class</code> options. <code>You must</code> be root to do this.</td>
</tr>
<tr>
<td><strong>Bold</strong></td>
<td>Text that appears on an object in a window</td>
<td>Click the <strong>Save</strong> button.</td>
</tr>
</tbody>
</table>

**TABLE P-2** Command-line Usage Conventions

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[ ]</code></td>
<td>Optional variable</td>
<td><code>fw ver [-k] [-f filename]</code> Use either or both of the <code>-k</code> and the <code>-f filename</code> options.</td>
</tr>
<tr>
<td><code>&lt; &gt;</code></td>
<td>Compulsory variable</td>
<td><code>fw converthosts &lt;input_file&gt; [output_file]</code> <code>input_file</code> is compulsory. <code>output_file</code> is optional</td>
</tr>
<tr>
<td>`</td>
<td>`</td>
<td>Use one of the alternatives</td>
</tr>
</tbody>
</table>

**Note** - This note draws the reader’s attention to important information.
**Warning** - This warning cautions the reader about an important point.

**Tip** - This is a helpful suggestion.

**Shell Prompts in Command Examples**

The following table shows the default system prompt and superuser prompt for the C shell, Bourne shell, Korn shell and DOS.

**TABLE P-3  Shell Prompts**

<table>
<thead>
<tr>
<th>Shell</th>
<th>Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td>C shell prompt</td>
<td><code>machine_name$</code></td>
</tr>
<tr>
<td>C shell superuser prompt</td>
<td><code>machine_name#</code></td>
</tr>
<tr>
<td>Bourne shell and Korn shell</td>
<td></td>
</tr>
<tr>
<td>prompt</td>
<td><code>$</code></td>
</tr>
<tr>
<td>Bourne shell and Korn shell</td>
<td></td>
</tr>
<tr>
<td>superuser prompt</td>
<td><code>#</code></td>
</tr>
<tr>
<td>DOS</td>
<td><code>current-directory&gt;</code></td>
</tr>
</tbody>
</table>

**Network Topology Examples**

Network topology examples usually show a gateway’s name as a city name (for example, Paris or London) and the names of hosts behind each gateway as names of popular sites in those cities (for example, Eiffel and BigBen).
Overview

Check Point SmartDefense creates a new category of Active Defense products that is unique to Check Point. It reactively protect organizations from known and unknown network attacks by using intelligent security technology. It frees the administrator from the need to understand technical attack details, making it possible concentrate on the task of defining the Access Control policy. SmartDefense requires a separate license.

SmartDefense blocks attacks by type and class using Check Point’s Stateful Inspection technology and provides a single, centralized console to deliver real-time information on attacks as well as attack detection, blocking, logging, auditing and alerting.
Check Point SmartDefense features:

- Centralized, Type Based, Attack Prevention — Provides a single place of control for blocking known and unknown attacks using new attack type classification technology.

- On-Line Updates & Web Worms Prevention — Enables on-line updates from Check Point's SmartDefense attack center to prevent new types of attacks, including new web worms patterns.

- Real-time Attack Information — Using Check Point's on-line attack information center, security administrators can get updated information on each attack type.

DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks, which are among the most common and damaging types of Internet attacks, are caused by attempts to flood networks or servers with mock traffic to prevent legitimate traffic from flowing through. SmartDefense actively detects and protects against these and other types of attacks, providing network resiliency to ensure mission critical resources are not affected while defending against an attack. SmartDefense mitigates risk and damage from DoS and DDoS attacks.

**Configuring SmartDefense**

To configure SmartDefense, click the SmartDefense button in the toolbar (FIGURE 1-1).

**FIGURE 1-1 SmartDefense button**

In the SmartDefense Settings window (FIGURE 1-2), configure the parameters for each of the attacks.

*Note* - In many of the SmartDefense windows, a detailed description of the attack and the defense is displayed in the window.
Update SmartDefense — Subscribers can click Update SmartDefense to obtain updated information about all attacks, as well as updated and new defenses against worms (see “General HTTP Worm Catcher” on page 43).

Open Log Manager — Open the Log Viewer to view SmartDefense-related events.

Anti Spoofing Configuration

This page indicates how anti spoofing is configured on the gateways. You can change the settings by reconfiguring the individual gateways.
Denial of Service

In contrast to an attack whose purpose is to penetrate the target system, the purpose of a Denial of Service attack is to overwhelm the target with spurious data to the point where it is no longer able to respond to legitimate service requests.

A Denial of Service (DoS) attack floods a network with so many additional requests that regular traffic is either slowed or completely interrupted for some period. A distributed denial of service (DDoS) attack uses multiple computers throughout the network that it has previously infected. The computers work together to send out bogus messages, thereby increasing the amount of spurious traffic.

Specify which of the attacks to defend against by checking the check box next to the attack's name in the tree (FIGURE 1-4).
Accumulate successive events — Scan the VPN-1/FireWall-1 Log for evidence of Denial of Service attacks and take the action specified in Action when an attack is detected.

If Accumulate successive events is not checked, you will still be protected from the attacks selected in the tree on the left.

Action — Select the action to take if an attack is detected.

Click Advanced to display the Advanced Configuration window (FIGURE 1-5).
FIGURE 1-5 Denial of Service — Advanced Configuration window

If, during the interval specified by **Time interval**, an event occurs **Attempts number**
times, then an attack is considered to have occurred. This interval is monitored in
segments of length specified by **Resolution**.

**Teardrop**

FIGURE 1-6 Denial of Service — Teardrop page

**Track** — Select the action to take if an attack is detected.
Ping of Death

FIGURE 1-7 Denial of Service — Ping of Death page

Track — Select the action to take if an attack is detected.
LAND

Denial of Service — LAND page

Track — Select the action to take if an attack is detected.

IP and ICMP

VPN-1/FireWall-1 handles ICMP with its Stateful Inspection method, so ICMP connections are fully inspected and different protocols types are identified, inspected, monitored and managed according to the packet flow security definitions. For each examined ICMP packet VPN-1/FireWall-1 identifies its protocol type, protocol header analysis and protocol flags analysis and verification.
Figure 1-8: IP and ICMP page

The figure shows a screenshot of the SmartDefense Settings window with the IP and ICMP page selected. The window includes a variety of settings with checkboxes for enabling or disabling specific features. The description text reads:

**Description:**
This page allows you to enable a comprehensive sequence of layer 3 tests (IP and ICMP protocols).
Fragment Sanity Check

FIGURE 1-9 Fragment Sanity Check page

Track — Select the action to take if an attack is detected.
Packet Sanity

Figure 1-10 Packet Sanity page

**Track** — Select the action to take if an attack is detected.

**Enable relaxed UDP length verification** — Select this option ignore cases where inconsistencies in the UDP length calculation methods used by different applications may result in spurious errors.
Max Ping Size

FIGURE 1-11 Max Ping Size page

**Track** — Select the action to take if an attack is detected.

**Ping Size** — Specify the maximum acceptable size of a PING packet.

TCP

VPN-1/FireWall-1 is able to identify the basic IP based protocols and analyze a packet in order to verify that it contains allowed options only.

In order to verify that packets are legitimate, the following tests are conducted:

- protocol type verification
- protocol header analysis
- protocol flags analysis and verification
Specify which of the attacks to defend against by checking the check box next to the attack’s name in the tree.

**SYN Attack**

For a detailed description of SYN attacks and SYNDedenger, see “SYN Attacks and SYNDedenger” on page 58.
FIGURE 1-13 SYN Attack.

Override module’s SYNDefender configuration — Select this option to specify that the settings on this page override the SYNDefender settings specified for individual Modules.

SYN attack defense can be specified in two ways:
- on a per-Module basis
- in the SmartDefense SYN Attack page (FIGURE 1-13)

Activate SYN Attack protection — If Override module’s SYNDefender configuration is checked, then you can activate protection for all Modules. Click Configure to specify the parameters of the protection method in the SYN Attack window (FIGURE 1-14).

Early Versions SYNDefender configuration — Check this option to open the window (FIGURE 1-15) to configure SYNDefender protection for earlier version Modules.
SYN Attack window (All Modules)

**FIGURE 1-14** SYN Attack window

- **Track** — Select the action to take if an attack is detected.
- **Track Level** — Select one of the following:
  - Attacks only — The action specified under **Track** will be taken only when an attack is detected and when it is over.
  - Individual SYNs — The action specified under **Track** will be taken for each SYN packet.
- **Timeout** — Specifies how long SmartDefense waits for an acknowledgment before concluding that the connection is a SYN attack.
- **Attack threshold** — If more than **Attack threshold** unacknowledged SYN packets are detected at any one time, then SmartDefense will conclude that a SYN attack is taking place.
- **Protect external interface only** — Protect against SYN attacks only on the external interface.
Logical Flow - Choose one of the following:

- **None** — SYNDefender is not deployed.
  - If you choose this option, your network will not be protected from SYN attacks.
- **SYN Gateway** — Deploy the SYN Gateway method.
- **Passive SYN Gateway** — Deploy the Passive SYN Gateway method.

**Timeout** — Specifies how long SYNDefender waits for an acknowledgment before concluding that the connection is a SYN attack.

**Maximum Sessions** — Specifies the maximum number of protected sessions.
  - This parameter is relevant only if **Passive SYN Gateway** is selected under **Method**. If **SYN Relay** is selected, all sessions are protected.
  - This parameter specifies the number of entries in an internal connection table maintained by SYNDefender. If the table is full, SYNDefender will not examine new connections.

**Display Warning Messages** — If set, SYNDefender will print console messages regarding its status.

### Small PMTU

When a connection between two hosts is established, the sides involved exchange their TCP maximum segment size (MSS) values. The smaller of the two MSS values is used for the connection. The MSS for a system is usually the MTU (Maximum Transfer Unit) at the link layer minus 40 bytes for the IP and TCP headers.
When TCP segments are destined to a non-local network, the **Don't Fragment** bit is set in the IP header. Any router or media along the path may have an MTU that differs from that of the two hosts. If a media is encountered with an MTU that is too small for the IP datagram being routed, the router will attempt to fragment the datagram accordingly. Upon attempting to do so, it will find that the **Don't Fragment** bit in the IP header is set. At this point, the router should inform the sending host with an ICMP destination unreachable message that the datagram cannot be forwarded further without fragmentation.

When a network router receives a packet larger than the Maximum Transfer Unit (MTU) of the next network segment, and that packet's IP layer **Don't Fragment** bit is flagged, the router should send an ICMP destination unreachable message back to the sending host. When this does not happen, packets can be dropped, causing a variety of errors that will vary with the application that is communicating over the failed link.

**FIGURE 1-16** Small PMTU page

**Track** — Select the appropriate tracking option.
Minimal MTU size — Define the minimal allowed MTU. An exceedingly small value will not prevent an attack, while an unnecessarily large value might result in legitimate requests to be dropped, causing “black hole” effects and degrading performance.

Sequence Verifier

The Sequence Verifier matches the current TCP packet’s sequence numbers against a state kept for that TCP connection. Packets that match the connection in terms of TCP session, but have sequence numbers that do not make sense, are either dropped, or stripped of data.

FIGURE 1-17 Sequence Verifier page

Track — Select the appropriate tracking option.

Track on — Specify the type of out of state packets to be tracked, as follows:

- **anomalous** — Track only packets that do not normally appear in legitimate connections.

- **every** — Track every out-of-state packet.
**suspicious** — Track only packets seemingly erroneous packets, unrelated to the connection.

**DNS**

**FIGURE 1-18** DNS page

![Image of DNS page](image)

**UDP protocol enforcement** — If selected, VPN-1/FireWall-1 monitors DNS traffic to ensure compliance with RFC 1035, that is, that the DNS packets are correctly formatted. This feature does not support DNS over TCP (TCP Zone Transfer).

**Track** — Select the appropriate tracking option.
FIGURE 1-19 FTP page

These pages allow you to configure various protections related to the FTP protocol.
FTP Bounce Attack

FIGURE 1-20 FTP Bounce page
FTP Security Server

FIGURE 1-21 FTP Security Server

Configurations apply to all connections — The FTP Security Server is invoked for all connections.

Configurations apply only to connections related to resources used in the Rule Base — The FTP Security Server is invoked when a rule specifies an FTP Resource and/or User Authentication is defined.
FTP Security Server — Allowed FTP Commands

FIGURE 1-22 FTP Security Server — Allowed FTP Commands

SmartDefense Settings

Allowed FTP Commands:

- Last Update: 12-April-2002
- Description: Use this page to select which FTP commands are allowed to pass through the security server.

<table>
<thead>
<tr>
<th>Acceptable commands</th>
<th>Blocked commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGET</td>
<td>FRM</td>
</tr>
<tr>
<td>ACCT</td>
<td>OWD</td>
</tr>
<tr>
<td>ALEO</td>
<td>LST</td>
</tr>
<tr>
<td>APPO</td>
<td>PUT</td>
</tr>
<tr>
<td>BINARY</td>
<td>TMP</td>
</tr>
<tr>
<td>CDUP</td>
<td>USER</td>
</tr>
<tr>
<td>DEL</td>
<td>USER</td>
</tr>
<tr>
<td>EPS</td>
<td>USER</td>
</tr>
<tr>
<td>PR0</td>
<td>USER</td>
</tr>
<tr>
<td>PR1</td>
<td>USER</td>
</tr>
<tr>
<td>PR2</td>
<td>USER</td>
</tr>
<tr>
<td>PR3</td>
<td>USER</td>
</tr>
</tbody>
</table>

Settings:
FIGURE 1-23 FTP Security Server — Prevent Known Ports Checking

In this page you can select whether to allow the FTP security server to connect to well-known ports. Thus you will provide a second protection against certain bounce attacks. Even if the attacker manages to bounce the connection, the security server will not let the bounced connect to any port running a known service. Note that toggling the checkbox on disables this sanity check.
FTP Security Server — Prevent Known Ports Checking

FIGURE 1-24 FTP Security Server — Prevent Known Ports Checking

In this page, you can select whether to allow the FTP security server to connect to well-known ports. This will provide a second protection against certain bounce attacks. Even if the attacker manages to bounce the connection, the security server will not let the bounce connect to any port running a known service. Note that enabling this checklist on disables the sanity check.
FTP Security Server — Prevent Port Overflow Checking

FIGURE 1-25 FTP Security Server — Prevent Port Overflow Checking
Prevent Port Overflow Checking

FIGURE 1-26 FTP Security Server — Prevent Port Overflow Checking

SmartDefense Settings

Prevent Port Overflow Checking

Attack description:
To conform with the FTP protocol, the PORT command has the originating machine specify an arbitrary destination machine and port for the data connection. However, this behavior allows an attacker to open a connection to a port of the attacker’s choosing on a machine that may not be the originating client. Making this connection to an arbitrary machine for unauthorized purposes is the FTP bounce attack.

SMARDefense Protections
Setting this option disables the checks that
HTTP

**FIGURE 1-27** HTTP page

HTTP (HyperText Transfer Protocol) is the communications protocol used to connect to servers on the World Wide Web. Its primary function is to establish a connection with a Web server and transmit HTML pages to the client browser.

This page allows you to configure various protections related to this protocol.
You can import updates from the Check Point Web site or add patterns manually into the **Worm Patterns** list.
HTTP Security Server

FIGURE 1-29 HTTP Security Server page

Configurations apply to all connections — The HTTP Security Server is invoked for all connections.

Configurations apply only to connections related to resources used in the Rule Base — The HTTP Security Server is invoked when a rule specifies an HTTP Resource and/or User Authentication is defined.
HTTP Security Server — HTTP Format Sizes

**FIGURE 1-30** HTTP Security Server — HTTP Format Sizes page

![SmartDefense Settings](image)

<table>
<thead>
<tr>
<th>SmartDefense Settings</th>
<th>HTTP Format Sizes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Maximum URL length</td>
<td>2410 bytes</td>
</tr>
<tr>
<td>Maximum HTTP header length</td>
<td>1101 bytes</td>
</tr>
<tr>
<td>Maximum number of HTTP headers</td>
<td>500</td>
</tr>
</tbody>
</table>

**Description:**
This page configures upper bounds to various aspects of the HTTP protocol. Connections that try to exceed the limit are dropped.
HTTP Security Server — ASCII Only Request Headers

FIGURE 1-31 HTTP Security Server — ASCII Only Request Headers page
HTTP Security Server — ASCII Only Response Headers

**FIGURE 1-32** HTTP Security Server — ASCII Only Response Headers page

**Maximum URL length** — Prevents the security server from getting unwanted data by limiting the length of the URL in HTTP client request or in redirect requests.

**Maximum HTTP header length** — Prevents the security server from getting unwanted data by limiting the maximum header length the security server will get both in the HTTP client request and in the HTTP server reply.

**Maximum number of HTTP headers** — Prevents the security server from getting unwanted data by limiting the number of headers the security server will get both in the HTTP client request and in the HTTP server reply.

In addition, all HTTP headers are by default forced to be ASCII only. This will prevent some malicious content from passing in the HTTP protocol headers.
SMTP Security Server

FIGURE 1-33 SMTP Security Server page

Configurations apply to all connections — The SMTP Security Server is invoked for all connections.

The settings in the Mail and Recipient Content window (FIGURE 1-35 on page 50) apply only if an SMTP Resource is defined, even if Configurations apply to all connections is checked.

Configurations apply only to connections related to resources used in the Rule Base — The SMTP Security Server is invoked when a rule specifies an SMTP Resource and/or User Authentication is defined.
FIGURE 1-34 SMTP Security Server — SMTP Content

The SMTP Security Server provides Content Security that enables a Security Administrator to:

- provide mail address translation by hiding outgoing mail's From address behind a standard generic address that conceals internal network structure and real internal users
- perform mail filtering based on SMTP addresses and IP addresses
- strip MIME attachments of specified types from mail
- strip the Received information from outgoing mail, in order to conceal internal network structure
- drop mail messages above a given size
- send many mail messages per single connection
- resolve the DNS address for mail recipients and their domain on outgoing connections (MX Resolving)
- control the load generated by the mail dequeeuer in two different ways:
- control the number of connections per site
- control the overall connections generated by the mail dequeuer
- provide a Rule Base match on the Security Server mail dequeuer which enables:
  - a mail-user based policy
  - better performance of different mail contents action per recipient of a given mail
  - generation of different mail contents on a per-user basis
  - application of content security features at the user level
- perform CVP checking (for example, for viruses)

Mail and Recipient Content

FIGURE 1-35 SMTP Security Server — Mail and Recipient Content
**Note** - The settings in this window apply only if an SMTP Resource is defined, even if Configurations apply to all connections in the SMTP Security Server window (FIGURE 1-33 on page 48) is checked.

Allow multiple content-type headers — If checked, the SMTP Server will allow multiple content-type headers.

Allow multiple “encoding” headers — If checked, the SMTP Server will allow multiple “encoding” headers.

Allow non-plain “encoding” headers — If checked, the SMTP Server will allow non-plain “encoding” headers.

Allow unknown encoding — If checked, the SMTP Server will allow unknown encoding methods.

Force recipient to have a domain name — If checked, the SMTP Server will force the recipient to have a domain name.

Perform aggressive MIME strip — This property controls two different levels of performing the MIME strip:

- if checked, the entire mail body will be scanned for headers such as “Content-Type: text/html; charset=utf-8” and the MIME strip will be performed accordingly
- if unchecked, only the mail headers section and the headers of each MIME part will be scanned. If a relevant header is located, the MIME strip will be performed accordingly.
VPN-1/FireWall-1’s Successive Events feature (formerly known as Malicious Activity Detection) provides a mechanism for detecting malicious or suspicious events and notifying the system administrator. This feature is implemented by reading the VPN-1/FireWall-1 Log File and matching Log entries to attack profiles. The VPN-1/FireWall-1 administrator can modify attack detection parameters, turn detection on or off for specific attacks, or disable the Successive Events feature entirely.

The feature runs on the SmartCenter Server and analyses logs from VPN/FireWall Modules. Logs which do not reach the SmartCenter Server (for example, local logs and logs sent to Log Server) are not analyzed by the Successive Events.

SmartDefense provides a mechanism for detecting malicious or suspicious events and notifying the system administrator. The mechanism allows you sending alerts when different successive malicious events are detected.
Max memory allocation size — Specify the amount of memory allocated to the detecting mechanism (in Kbytes). If more memory is required, the feature will exit. Memory requirements can be reduced by reducing the number of attacks or decreasing the value of the Reset accumulated events property.

Reset accumulated events every...sec — Define the period upon expiration of which events will be deleted from SmartDefense's internal tables. High values reduce CPU usage but increase memory requirements.

Logging attempts interval — The interval (in seconds) over which log entries corresponding to this attack are counted. A large resolution value reduces memory usage but increases the probability that attacks will not be recognized.

Max logging attempts — The number of times an event must occur within the Logging attempts interval in order for an error notification to be sent.

Address Spoofing

Action — Select the appropriate tracking option.
To configure when the tracking option specified under **Action** will be taken, click **Advanced** to display the **Advanced Configuration** window (FIGURE 1-38).

**FIGURE 1-38 Successive Events — Advanced Configuration window**

**Resolution** —

**Time Interval** —

**Attempts number** —
Port Scanning

FIGURE 1-39 Successive Events — Port Scanning page

**Action** — Select the appropriate tracking option.

To configure when the tracking option specified under **Action** will be taken, click **Advanced** to display the **Advanced Configuration** window (FIGURE 1-38).
Local Interface Spoofing

**FIGURE 1-40** Successive Events — Local Interface Spoofing page

**Action** — Select the appropriate tracking option.

To configure when the tracking option specified under Action will be taken, click Advanced to display the **Advanced Configuration** window (FIGURE 1-38 on page 54).
Successive Alerts

**FIGURE 1-41** Successive Events — Successive Alerts page

**Action** — Select the appropriate tracking option.

To configure when the tracking option specified under Action will be taken, click Advanced to display the Advanced Configuration window (FIGURE 1-38 on page 54).
**Successive Multiple Connections**

**FIGURE 1-42** Successive Events — Successive Multiple Connections page

**Action** — Select the appropriate tracking option.

To configure when the tracking option specified under Action will be taken, click Advanced to display the Advanced Configuration window (FIGURE 1-38 on page 54).

**SYN Attacks and SYDefender**

**The TCP Three-Way Handshake**

TCP (Transport Control Protocol) is a connection-oriented, reliable transport protocol. Two participating hosts must first establish a connection by a three-way handshake between them. TCP assigns sequence numbers to every byte in every segment and acknowledges all data bytes received from the other end.
For example, if host A wants to establish a connection with host B, A begins by sending a SYN packet (a TCP packet with the SYN bit set) to B. B replies with a SYN/ACK packet (a TCP packet with the SYN and ACK bits set). A completes the three-way hand-shake with a TCP ACK packet.

**FIGURE 1-43** TCP SYN handshake

When B receives the SYN packet, it allocates substantial memory for the new connection. If there were no limit to the number of connections, a busy host would quickly exhaust all of its memory trying to process TCP connections. However, there is usually a small upper limit to the number of concurrent TCP connection requests (“backlog queue”) a given application can have running on the host.

There is an upper limit for each server program (depending on the configuration) of outstanding unacknowledged (un-ACK’d) connection requests. When the backlog queue limit is reached, an attempt to establish another connection will fail until one of the backlogged connection either becomes established (SYN/ACK packet is ACK’d), is reset (a RST packet is received) or times out.

**How the Attack Works**

A client initiates a TCP connection by a request with the SYN flag set in the TCP header. Normally the server replies with a SYN/ACK identified by the source IP address in the IP header. The client then sends an ACK to the server (FIGURE 1-43 on page 59) and data exchange begins.

When the source IP address is spoofed (changed) to that of an unreachable host, the targeted TCP cannot complete the three-way hand-shake and will keep trying until it times out. This is the basis for the SYN flood attack.

The attacking host (Z) sends a small number (less than 10 is sufficient) of SYN requests to the target TCP port (for example, the Web server). The attacking host also spoofs the source IP address as that of another (Z’), currently unreachable host. The process is depicted in FIGURE 1-44.
The source IP address (Z’) must be unreachable because the attacker does not want any host to receive the SYN/ACKs from the target TCP, which would elicit a RST from that host (an RST packet is issued when the receiving host does not know what to do with a packet) and thus foil the attack (FIGURE 1-45).

Instead, until the SYN requests time out, A will not accept any connection requests. If the attacks were, for example, against A’s Web server, then that Web server will be inaccessible for some two minutes as a result of an attack that lasted less than one second.
VPN-1/FireWall-1 SYNDefender

Check Point's SYNDefender provides three different approaches for defending against a SYN flooding attack:

- SYN Gateway (supported only for pre-NG VPN/FireWall Modules)
- Passive SYN Gateway
- SYN Relay (not supported for pre-NG VPN/FireWall Modules)

All these solutions are integrated into the VPN/FireWall Module, which intercepts all packets before they are observed by the operating system and performs Stateful Inspection on these packets. The system administrator can choose which of the solutions is best suited to a particular environment.

SYN Gateway

In order for the resetting of SYN connection attempts to be effective against the SYN flooding attack, the reset timer must be short enough to keep A's backlog queue from filling up, while at the same time long enough to enable users coming over slow links to connect. The SYN Gateway solution counters the attack by ensuring that an ACK packet is sent in immediate response to A's SYN/ACK packet.

When A receives the ACK packet, the connection is moved out of the backlog queue and becomes an open connection on A. Internet servers can typically handle hundreds or thousands of open connections, so the SYN flooding attack is no more effective in creating a denial of service condition than a hacker trying to establish an excessive number of valid connections to the server. The backlog queue is effectively kept clear and it is possible to wait longer before resetting connections which have not been completed.

SYN Gateway is depicted in FIGURE 1-46.
FIGURE 1-46 SYN Gateway

1. VPN-1/FireWall-1 intercepts a SYN packet going to host A and records the event in an INPSPECT state table.

2. VPN-1/FireWall-1 lets the SYN packet continue on to A.

3. VPN-1/FireWall-1 intercepts A's SYN/ACK reply to Z and correlates with the corresponding SYN packet sent by Z.

4. VPN-1/FireWall-1 lets the SYN/ACK continue on its way to Z.

5. VPN-1/FireWall-1 sends an ACK packet to A, which moves the connection out of A's backlog queue.

6. At this point, one of two things will happen, depending on whether the connection attempt is valid.
   
a. If Z's connection attempt is valid, then VPN-1/FireWall-1 will receive an ACK from Z which it will pass on to A.

   A ignores this second redundant ACK since the three-way handshake has already been completed.

b. If Z's IP address does not exist, then no ACK packet will return from Z to A and the reset timer will expire. At this point, VPN-1/FireWall-1 resets the connection.

The effectiveness of the SYN Gateway solution is based on quickly moving connection attempts out of the backlog queue. SYN flood connection attempts then fail to fill up the backlog queue and remain as harmless as one of the host's open connections, until the VPN-1/FireWall-1 timer expires and the connection is reset or canceled.
Passive SYN Gateway

Passive SYN Gateway is similar to SYN Gateway, except that VPN-1/FireWall-1 does not simulate Z’s ACK packet to A, and instead waits for Z’s ACK before passing it on to A.

The unacknowledged connection remains in A’s backlog queue, but times out after VPN-1/FireWall-1’s timeout period, which is much shorter than the backlog queue’s timeout period.

FIGURE 1-47 depicts Passive SYN Gateway.

SYN Relay

The SYN flooding attack sends SYN packets with the source addresses of unreachable hosts which will not reply to SYN/ACK packets. SYN Relay counters the attack by making sure that the three way handshake is completed (that is, that the connection is a valid one) before sending a SYN packet to the connection’s destination (A). SYN Relay is a high-performance kernel-level process which acts as a relay mechanism at the connection level. FIGURE 1-48 depicts SYN Relay.
FIGURE 1-48 SYN Relay

1. VPN-1/FireWall-1 intercepts a SYN packet going to host A.
2. VPN-1/FireWall-1 does not pass the SYN packet to A, but rather acts on A’s behalf and replies with a SYN/ACK packet to Z.
3. If an ACK packet is received from Z, then ...
   - VPN-1/FireWall-1 sends a SYN packet to A.
   - A replies with a SYN/ACK packet.
   - VPN-1/FireWall-1 replies with an ACK packet.

At this point the connection from Z to A is established and VPN-1/FireWall-1 is able to begin passing packets between Z and A. SYNDefender correctly translates the connection sequence numbers, which are now different for each half of the connection.

If VPN-1/FireWall-1 does not receive a packet for several seconds during any of the above steps, or if it receives a RST when an ACK or SYN/ACK are expected, it terminates the connection immediately.

Note that if Z contacts an unavailable server on A, it will first connect and then get a RST, which is not normal but harmless.

Guidelines for Deploying SYNDefender

While there are no strict rules for when to use each of the SYNDefender solutions, some basic guidelines will help establish the appropriate policy for a given situation.

Passive SYN Gateway

Passive SYN Gateway has two primary advantages:
• Users establishing valid connections with the protected server will not incur any delay in connection setup time.
• There is very little overhead on VPN-1/FireWall-1.

**SYN Relay**

*Note* · SYN Relay is not supported for pre-NG VPN/FireWall Modules.

SYN Relay’s primary advantage is that the protected server does not receive any invalid connection attempts. If the server has limited memory or often reaches an overloaded state, then SYN Relay’s complete filtering of invalid connection attempts can be advantageous in case of attack. Users making valid connections to the server may experience slightly longer connection setup time than with SYN Gateway.

**SYN Gateway**

Since connections are established on the server, that is, moved from the backlog queue, it is important to consider how many established connections the protected server can support relative to the normal load handled by the server.

It is not possible to specify SYN Gateway for individual VPN/FireWall Modules. SYN Gateway is supported only for pre-NG VPN/FireWall Modules.

*Note* · It is recommended that SYN Gateway *not* be used.

**Choosing an Appropriate SYNDfinder Method**

Following are some recommendations for choosing the SYNDfinder method to deploy.

1) If you are not currently under SYN attack, then consider whether you need SYNDfinder at all. Since the SYN flooding attack is a denial of service attack rather than a security breach, it may be more effective to deploy SYNDfinder only after a SYN attack actually occurs.

2) To be notified if and when you do come under attack, use Passive SYN Gateway with *Maximum protected sessions* set to 50 or less.
Setting the timeout can be a delicate issue. If the timeout is too short, legitimate connections may fail; if it is too long, some attacks may succeed. It is therefore recommended that Passive SYN Gateway be used primarily as a monitoring tool (in conjunction with the Log Viewer) to identify attacks.

3) If SYN attacks are a real concern, then SYN Relay should be used. SYN Relay provides complete protection from a SYN attack, at the cost of increased memory usage. There may also be a (usually) undetectable delay in connection setup.

4) It is recommended that SYN Gateway *not* be used.
Network Address Translation (NAT)

In This Chapter

Introduction page 67
Configuring Network Address Translation page 70
Address Translation Modes page 70
Address Translation and Routing page 78
IANA Recommendations page 86
Supported Services page 86
Generating Address Translation Rules Automatically page 87
Network Address Translation Rule Base page 89
Address Translation Examples page 102
Advanced Topics page 112
Frequently Asked Questions page 116

Introduction

The Need for Address Translation

The need for IP address translation — replacing one IP address in a packet by another IP address — arises in two cases:

1) The network administrator wishes to conceal the network's internal IP addresses from the Internet.
The administrator may reason that there is nothing to be gained, from a security point of view, by making a network’s internal addresses public knowledge.

2) An internal network’s IP addresses are invalid Internet addresses (that is, as far as the Internet is concerned, these addresses belong to another network).

This situation may have arisen for historical reasons: an internal network was originally not connected to the Internet and its IP addresses were chosen without regard to Internet conventions. If such a network is then connected to the Internet, its long-established internal IP addresses cannot be used externally. Changing these addresses may be impractical or unfeasible.

In both cases, the internal IP addresses cannot be used on the Internet. However, Internet access must still be provided for the internal hosts with the invalid or secret IP addresses.

Application gateways (proxies) have historically served as a partial solution to these problems. For example, to hide his or her internal IP addresses, a user can TELNET to a gateway and from there continue to the Internet through a proxy. VPN-1/FireWall-1 can be easily set up to provide and enforce such a scheme for a wide variety of services (FTP, TELNET, HTTP, and almost all other TCP, UDP and RPC services). Moreover, VPN-1/FireWall-1 supplements this scheme by providing user authentication on the gateway.

On the other hand, proxies have drawbacks:

- Proxies are tailored per application, so it is impossible to use applications that are not proxied, inbound or outbound.
- Proxies are not transparent, so that even authorized outbound users need to go through the application on the gateway, and impose a large overhead on the gateway host. Once a connection is accepted by a proxy, it functions as a packet forwarder at the application layer, which is an inefficient use of resources.
- It is difficult to provide good proxies for protocols other than TCP.

In contrast, VPN-1/FireWall-1’s generic and transparent fully RFC 1631 compliant Address Translation feature provides a complete and efficient solution. The administrator can determine which internal addresses are to be hidden (that is, mapped to the FireWalled host’s IP address) and which are to be mapped to a range of IP addresses visible to the Internet. At the same time, internal hosts can be configured to be accessible from the Internet even though their internal IP addresses are invalid Internet addresses. VPN-1/FireWall-1 achieves full Internet connectivity for internal clients.
Address Translation can be used to implement “one way routing,” so that there is no route from the outside to an internal network or to hosts.

**Example**

Consider the following network configuration:

**FIGURE 2-1 Example Network Configuration**

![Network Diagram](https://via.placeholder.com/150)

Suppose the administrator of this network wishes to provide mail services to the internal (private) hosts, but the internal IP addresses cannot be used, for one of the reasons stated above (see “The Need for Address Translation” on page 67.)

One possible solution is to move the mail server (which is currently on one of the internal hosts) to the gateway. This solution is not optimal, because of:

- the significant overhead the mail server imposes on the gateway
- reduced security
- the administrative overhead incurred when modifying the configuration

A better solution might be to implement Address Translation on the gateway, as follows, using the Static Destination Mode of Address Translation (see “Static Destination Mode” on page 77):

- The mail server is assigned a valid IP address (its public IP address), which is exposed to the Internet. However, internally, the mail server retains its existing (private) IP address.
- Incoming mail arrives at the gateway, where the destination IP address (the mail server’s public IP address) is translated to its private address. The source IP address of outgoing mail is translated from the mail server’s private IP address to its public IP address.

**Note** - Address Translation changes IP addresses in the packet, so it is almost always necessary to make some changes in the routing tables to ensure that packets with translated addresses reach their proper destinations.

**Note** - The gateway has a valid IP address which cannot be hidden.
Routing tables on the gateway and router may have to be modified to implement this scheme (see “Address Translation and Routing” on page 78).

**Configuring Network Address Translation**

To configure Network Address Translation (NAT), proceed as follows:

1. Determine which NAT Mode to use: Hide Mode or Static Mode.
   See “Address Translation Modes” on page 70 for detailed information about these modes.

2. Define the NAT Rule Base.
   There are two methods of defining NAT rules: automatic (the recommended method) and manual.
   - **Automatic Definition** — The NAT rules are automatically generated, based on the properties of network objects (gateways, hosts, networks and Address Ranges).
     The object’s properties are applied whenever the object is used in the Security Policy. In addition, numerous implementation details are automatically handled correctly (for example, Anti-Spoofing). In contrast, when rules are defined manually, these implementation details must be implemented manually as well.
     Automatic definition is the simplest method to use, but it is inflexible: the generated rules cannot be modified, but you can add rules (with the second method — see below) before and after the automatically generated rules.
     For information on this method, see “Generating Address Translation Rules Automatically” on page 87.
   - **Manual Definition**
     The NAT Rule Base is defined manually. You can also add NAT rules before and after the rules generated automatically by the previous method, but you cannot modify or delete the automatically generated rules.
     This method is not as simple to use as the previous method, but is more powerful and more flexible.

3. Configure routing so that NAT packets are properly routed.
   See “Address Translation and Routing” on page 78 for more information.

**Address Translation Modes**

VPN-1/FireWall-1 supports two Address Translation Modes:
Dynamic (Hide)—Many invalid addresses are translated to a single valid address, and dynamically assigned port numbers are used to distinguish between the invalid addresses.

Dynamic Address Translation is called Hide Mode, because the invalid addresses are “hidden” behind the valid address. For details of this mode, see “Hide Mode” on page 71.

Static—Each invalid address is translated to a corresponding valid address.

There are two modes of Static Address Translation:
- Static Source Mode (see “Static Source Mode” on page 75)
- Static Destination Mode (see “Static Destination Mode” on page 77)

In This Section

Hide Mode page 71
Static Source Mode page 75
Static Destination Mode page 77

Hide Mode

Warning · The IP address of a gateway's external interface must never be hidden.

Hide Mode is used for connections initiated by hosts in an internal network, where the hosts' IP addresses are invalid. In Hide Mode, the invalid internal addresses are hidden behind a single valid external address. Different connections are distinguished from each other using both:
- dynamically assigned port numbers, and
- the destination IP address

Note · Hide Mode is supported only for TCP, UDP and ICMP.

Distinguishing Between Connections

For each destination IP address, source port numbers are dynamically assigned from two pools of numbers:
- from 600 to 1023 (low ports)
Address Translation Modes

- from 10,000 to 60,000 (high ports)

If the original source port number is less than 1024, then a port number is assigned from the first pool. If the original port number is greater than 1024, then a source port number is assigned from the second pool. VPN-1/FireWall-1 keeps track of the source port numbers assigned, so that the original source port number is correctly restored for return packets. A port number currently in use is not assigned again to a new connection.

The total number of connections that can be hidden is more than 50,000 for each destination IP address.

Limitations

Hide Mode has several limitations:

- Hide Mode does not allow access to the “hidden” hosts to be initiated from the outside, that is, an external machine cannot connect to any of the hosts whose addresses have been translated. For example, in the configuration in FIGURE 2-3 on page 73, if you run your HTTP server on 200.0.0.108 (one of the internal machines with an invalid address), external machines will not be able to connect to your HTTP server using 199.100.145.35 (the gateway’s valid address) as the destination.

This limitation can also be considered an advantage of Hide Mode.

- Hide Mode cannot be used for protocols where the source port number cannot be changed.

- Hide Mode cannot be used when the external server must distinguish between clients on the basis of their IP addresses, since all clients share the same IP address under Hide Mode.

Example

Suppose localnet is an internal network with invalid addresses are as follows:

<table>
<thead>
<tr>
<th>Valid IP address</th>
<th>Invalid IP addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>199.100.145.35</td>
<td>200.0.0.100 - 200.0.0.200</td>
</tr>
</tbody>
</table>

199.100.145.35 is the address of gateway’s external interface.

You can hide the invalid addresses behind the valid address by specifying Address Translation in the NAT tab of localnet’s Network Properties window as follows:
Source addresses of outbound packets from hosts in localnet will be translated to 199.100.145.35, as illustrated in FIGURE 2-3. The source port number serves to direct reply packets to the correct host.

In FIGURE 2-4, the first rule must be manually inserted, and the second rule is automatically generated from the above definition (FIGURE 2-2 on page 73):
FIGURE 2-4 Hide Mode Automatically Generated Rules

<table>
<thead>
<tr>
<th>No.</th>
<th>Original Packet</th>
<th>Translated Packet</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Source</td>
<td>Destination</td>
<td>Service</td>
</tr>
<tr>
<td>1</td>
<td>localnet</td>
<td>localnet</td>
<td>Any</td>
</tr>
<tr>
<td>2</td>
<td>localnet</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

The first rule (which does not translate anything) applies to connections from the gateway to localnet and prevents the address of the gateway’s internal interface from being translated.

For an explanation of why this rule is necessary, see “Can I translate the gateway’s internal address?” on page 117.

The second rule expresses the Address Translation defined in the NAT tab (FIGURE 2-2 on page 73) and illustrated in FIGURE 2-3. Note the small letter H under localnet’s icon, which indicates Hide Mode translation.

For a detailed description of the meaning of the fields in an Address Translation Rule Base, see “Structure of a NAT Rule” on page 89.

Note - Routing tables on the gateway and router may have to be modified to implement this scheme (see “Address Translation and Routing” on page 78).

Choosing the Valid External Address for Hide Mode

You can choose to hide the internal IP addresses either behind the IP address of the gateway’s external interface, or behind another IP address (that is, a valid IP address that does not belong to any of the gateway’s interfaces, but one which you can route to the gateway).

If you hide the internal IP addresses behind the IP address of the gateway’s external interface ...

You will not have to make any changes to your routing tables (see “Address Translation and Routing” on page 78), because presumably the routing tables are already correctly configured for the gateway’s external interface.

On the other hand, you may have problems when a hidden connection shadows a connection originating on the gateway itself. For example, suppose a user on the gateway TELNETs to an external server, and is allocated the local TCP port 10001 by the gateway’s TCP module. Next, a user on one of the internal hosts also TELNETs to the external server and, because the connection is hidden, it is allocated the same
TCP port 10001 by the VPN/FireWall Module on the gateway. In this event, packets returning from the external TELNET server to the first TELNET client will be (incorrectly) diverted to the internal host, where they will be ignored.

**If you hide the internal IP addresses behind another IP address ...**

You will probably have to change the routing tables (see “Address Translation and Routing” on page 78) so that replies to the other IP address are directed to the gateway, but you will not have problems with shadowed connections as described above.

**Hiding Behind 0.0.0.0**

If you select **Hide behind th einterface of the Install On gateway** in the NAT tab (FIGURE 2-2), then the client IP addresses will be hidden behind the IP address of the gateway’s “server-side” interface, that is, behind the interface through which the connection leaves the gateway on the server side.

**FIGURE 2-5** Hiding Behind 0.0.0.0

A connection initiated by the client in FIGURE 2-5 will be hidden behind the IP address of the interface through which the connection was routed on the server side of the gateway, that is, behind either interface 2 or interface 3.

Specifying **Hide behind th einterface of the Install On gateway** is convenient because the NAT is performed dynamically, and if the IP addresses of the gateway are changed, then it is not necessary to reconfigure the NAT parameters.

**Statically Translating Addresses**

**Static Source Mode**

Static Source Mode translates invalid internal IP addresses to valid IP addresses, and is used when the connection is initiated by internal clients with invalid IP addresses. Static Source Mode ensures that the originating hosts have unique, specific valid IP addresses, and is usually used together with Static Destination Mode.

When you generate Address Translation rules automatically, Static Source Mode and Static Destination Mode rules are always generated in pairs.
Example

Suppose localnet is an internal network with invalid addresses, but a corresponding set of valid addresses is available, as follows:

<table>
<thead>
<tr>
<th>Valid IP addresses</th>
<th>Invalid IP addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>199.100.73.15 – 199.100.73.115</td>
<td>200.0.0.100 – 200.0.0.200</td>
</tr>
</tbody>
</table>

You can translate the invalid addresses to the valid addresses by specifying Address Translation in the NAT tab of localnet’s Properties window as follows:

FIGURE 2-6 Static Address Translation

The invalid addresses of hosts in localnet will be translated to the valid addresses starting at 199.100.73.15.

FIGURE 2-7 Address Translation using Static Source Mode
In FIGURE 2-8, the first rule must be manually inserted, and the following two Address Translation rules (FIGURE 2-8) are automatically generated from the above definition (FIGURE 2-6 on page 76):

**FIGURE 2-8 Automatically Generated Address Translation rules for Static Translation**

<table>
<thead>
<tr>
<th>No.</th>
<th>Original Packet</th>
<th>Translated Packet</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Source</td>
<td>Destination</td>
<td>Service</td>
</tr>
<tr>
<td>1</td>
<td>localnet</td>
<td>localnet</td>
<td>Any</td>
</tr>
<tr>
<td>2</td>
<td>localnet</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>localnet (Valid Addresses)</td>
<td>Any</td>
</tr>
</tbody>
</table>

The first rule (which does not translate anything) applies to connections from the gateway to localnet and prevents the address of the gateway’s internal interface from being translated. For an explanation of why this rule is necessary, see “Can I translate the gateway’s internal address?” on page 117.

Note that two static translation rules are generated:

- The first static translation rule (rule number 2) is a Static Source Mode rule, and defines the Address Translation illustrated in FIGURE 2-7.
- The second static translation rule (rule number 3) is the corresponding Static Destination rule and defines the Address Translation illustrated in FIGURE 2-9 on page 78 (see “Static Destination Mode” on page 77).

For a detailed description of the meaning of the fields in an Address Translation Rule Base, see “Structure of a NAT Rule” on page 89.

**Static Destination Mode**

Static Destination Mode translates valid addresses to invalid addresses for connections initiated by external clients. Static Destination Mode is used when servers inside the internal network have invalid IP addresses, and ensures that packets entering the internal network arrive at their proper destinations. Static Destination Mode is usually used together with Static Source Mode.

When you generate Address Translation rules automatically, Static Source Mode and Static Destination Mode rules are always generated in pairs.
Example

Suppose localnet is an internal network with invalid addresses, but a corresponding set of valid addresses is available, as follows:

<table>
<thead>
<tr>
<th>Valid IP addresses</th>
<th>Invalid IP addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>199.100.73.15 – 199.100.73.115</td>
<td>200.0.0.100 – 200.0.0.200</td>
</tr>
</tbody>
</table>

The second static translation rule (rule number 3) in FIGURE 2-8 on page 77 (generated from the NAT tab in FIGURE 2-6 on page 76) translates the valid addresses starting at 199.100.73.15 to the corresponding invalid addresses starting at 200.0.0.100. This is illustrated in FIGURE 2-9.

FIGURE 2-9 Address Translation using Static Destination Mode

Address Translation and Routing

Configuring Routing on the Gateway

To correctly implement Address Translation, you must ensure that a return packet intended for a host whose address has been translated is routed back to that host.

There are two routing issues involved:

- ensuring that the packet reaches the gateway
- ensuring that the gateway forwards the packet to the correct interface and host

Note: You will usually have to reconfigure your routing tables on the gateway (and on any intervening routers) to implement Address Translation.

Note: Routing tables on the gateway and router may have to be modified to implement this scheme (see “Address Translation and Routing” below).
Ensuring That the Packet Reaches the Gateway

From the Inside

The internal hosts (whose addresses are being translated) need a default route to the gateway, just as they do without Address Translation.

From the Outside

The translated (valid) addresses must be published, so that replies will be routed back to the gateway.

However, a router positioned between the gateway and the Internet may fail to route reply packets to the translating gateway. Instead, the router sends ARP requests, looking for the physical (MAC) address of the imaginary translated address.

For example, consider the network configuration below (FIGURE 2-10), where the internal network's invalid addresses are hidden behind the non-existent IP address 199.100.73.3 (see FIGURE 2-11).

FIGURE 2-10: Hiding a Network

When the client (10.0.0.1) initiates a connection to the outside world, the gateway translates the packet’s source address to 199.100.73.3, so when a reply packet arrives from the server, its destination address is 199.100.73.3. If no static route exists, the router sees that the packet is destined for a directly attached network (199.100.73.x) and sends an ARP request querying for the physical address (MAC) of 199.100.73.3. But since 199.100.73.3 is an imaginary address, the router receives no response for its query and drops the packet.
There are three ways to solve this problem:

1) Reconfigure the Address Translation.
   Hide the invalid network behind the gateway’s external address (FIGURE 2-12).

Note - In each case, you should stop and then restart the VPN/FireWall Module for these changes to take effect.
2) Another way of solving the problem is to change the routing on the router.

Define a static route on the router, using the equivalent of the Unix command:

```
route add 199.100.73.3 199.100.73.1 1
```

3) A third way of solving the problem is to have the gateway respond to ARP requests for the translated IP address (proxy ARP method).

**Note**: Starting with VPN-1/FireWall-1 Version NG, the **Automatic ARP configuration** property (NAT page of the **Global Properties** window — see “NAT (Network Address Translation)” on page 281) automatically configures the gateway's ARP tables, in the manner described here. See also “Automatic ARP Configuration — Special Considerations” on page 82.

**Unix** — On the gateway, link the imaginary IP address (that is, the IP address behind which you are hiding the network) to the MAC address of the gateway's external interface, using the `arp` command, as follows:

```
arp -s <IP Address> <MAC Address> pub
```
where `<IP Address>` is the non-existent IP address and `<MAC Address>` is the external interface’s MAC address. For example,

```
arp -s 199.100.73.3 00:a0:c9:45:b5:78 pub
```

**NT**—Create a text file named `local.arp` in the `$FWDIR\conf` directory. Each line in the file should be of the form:

```
<IP Address> <MAC Address>
```

where `<IP Address>` is the non-existent IP address and `<MAC Address>` (in the format “`xx-xx-xx-xx-xx`”) is the external interface’s MAC address. For example,

```
199.100.73.3 00-a0-c9-45-b5-78
```

**Automatic ARP Configuration — Special Considerations**

When the Automatic ARP configuration property (Network Address Translation page of the Global Properties window — see “NAT (Network Address Translation)” on page 281 of Check Point SmartCenter Guide) is enabled, the ARP tables on the VPN/FireWall Module (gateway) performing NAT are automatically configured so that ARP requests for a translated (NATed) machine, network or address range are answered by the gateway.

Special care must be taken when configuring networks where this feature is used. For example, consider the configuration in FIGURE 2-13.

**FIGURE 2-13** Automatic APRP configuration — two gateways
Here two VPN/FireWall Modules (tower and bigben) on the same subnet are performing NAT for clock (IP address 10.0.0.1 — hidden behind 2xx.1yy.1zz.80, also on the same subnet).

Note - This kind of configuration (where two VPN/FireWall Modules are on the same subnet) is generally not recommended, except in Load Sharing configurations.

Suppose the following conditions are both true:

- **Automatic ARP configuration** is enabled (Network Address Translation page of the Global Properties window)
- NAT for clock is installed on All in the NAT page of clock’s Properties window (FIGURE 2-14)

Then both tower and bigben will respond to ARP requests from the router, in other words, both tower and bigben will be pretending to be 2xx.1yy.1zz.80. There may also be OS messages warning about multiple nodes with the same IP address.

This problem can be avoided if the NAT for clock is installed only on one of the gateways (FIGURE 2-14).

**FIGURE 2-14** Automatic ARP configuration — installing NAT on only one gateway
Ensuring That the Gateway Forwards the Packet to the Correct Host

**Note** - This section applies only when **Perform destination translation on the client side** is not enabled (Network Address Translation page of the Global Properties window).

When translating the destination address of a connection (Static Destination Mode), packets may be forwarded to the wrong gateway interface if there are no static routes on the gateway to the translated (new) destination IP address.

If **Perform destination translation on the client side** (Network Address Translation page of the Global Properties window) is not enabled, Address Translation takes place in the gateway only after internal routing but before transmission, so the gateway’s routing sees an external destination address. To ensure that these packets are correctly routed to an internal host (and not bounced back out to the Internet), use static routing (the OS `route` command) to define the same “next hop” for both addresses.

For example, consider the following configuration:

```
  +--------------------------------+  +-------------------------+  +---------------+
  |      router                  |  | 10.0.0.8                |  | 192.168.73.241 |
  | FireWalled Gateway           |  | 10.0.0.1                |  | router        |
  | internal network (invalid) 10.0.0.0 |
  |      (netmask 255.0.0.0)    |  | Internet               |
  |  mailsrvr 10.0.0.1          |
```

![FIGURE 2-15 Static Address Translation](image)

**FIGURE 2-15 Static Address Translation**
Static Address Translation for mailsrvr

This results in the rules below (FIGURE 2-17):

The second rule will work correctly only if the gateway knows that in order to reach the address 199.100.73.1, it should forward the packet to 10.0.0.1. To make this happen, add a static route on the gateway, using the command:

```
route add 199.100.73.1 10.0.0.1 1
```

The router also has to know that the packets to the translated address must be routed through the gateway. This can be achieved either by defining a static route on the router, or by having the gateway publish (to the router) the fact it has a route to the translated address. For additional information about this problem, see “Ensuring That the Packet Reaches the Gateway” on page 79.
IANA Recommendations

RFC 1918 documents private address spaces for organizations that will not have hosts on the Internet.

The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private networks:

**TABLE 2-1** Private Networks Address Space

<table>
<thead>
<tr>
<th>class</th>
<th>from IP address ...</th>
<th>to IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>10.0.0.0</td>
<td>10.255.255.255</td>
</tr>
<tr>
<td>B</td>
<td>172.16.0.0</td>
<td>172.31.255.255</td>
</tr>
<tr>
<td>C</td>
<td>192.168.0.0</td>
<td>192.168.255.255</td>
</tr>
</tbody>
</table>

An enterprise that decides to use IP addresses in the address spaces defined above can do so without any coordination with IANA or an Internet registry. The address space can thus be used by many enterprises. Addresses within this private address space will only be unique within the enterprise.

**Supported Services**

**Restrictions**

TABLE 2-2 lists restrictions that apply to Address Translation when used with protocols that carry IP addresses or port numbers in the packet’s data portion, as opposed to the IP or TCP or UDP header.

TABLE 2-2 lists these restrictions.

**TABLE 2-2** Address Translation — Service Restrictions

<table>
<thead>
<tr>
<th>Service</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>sqlnet2</td>
<td>If the listener and server are on two different hosts whose IP addresses are being translated, then the difference between their untranslated IP addresses must be the same as the difference between their translated IP addresses. For example, if their original IP addresses are 200.200.200.1 and 200.200.200.11 (a difference of 10), then their translated IP addresses can be 199.199.199.20 and 199.199.199.30 (also a difference of 10), but not 199.199.199.20 and 199.199.199.40 (a difference of 20).</td>
</tr>
</tbody>
</table>
**FTP port command**

The FTP port command has been rewritten to support Address Translation, as specified in RFC 1631.

**Generating Address Translation Rules Automatically**

**Overview**

You can generate NAT rules for machines, networks and Address Ranges automatically, using the **NAT** tab of the network object’s Properties window (FIGURE 2-18 on page 88).

To generate Address Translation rules for a network object, proceed as follows:

1. Define the object whose address(es) will be translated using the Network Object Manager.

   For information on the Network Object Manager, see Chapter 5, “Network Objects” of *Check Point SmartCenter Guide*.

2. In the **NAT** tab of the object’s Properties window, check **Add Automatic Address Translation Rules**.

   When this box is checked, the other fields in the window are enabled.
3 Select a **Translation Method** from the drop-down menu.

For information about translation methods, see “Address Translation Modes” on page 70.

4 Enter an IP address for the translation.

If the **Translation Method** is **Hide**, then the IP address is the one behind which the object’s addresses will be hidden (see “Hide Mode” on page 71).

If the **Translation Method** is **Static**, then the IP address is the first one in the range to which the object’s addresses will be translated (see “Statically Translating Addresses” on page 75).

5 In **Install On**, select a VPN/FireWall Module on which to install the generated Address Translation rule.
Overview

Chapter 2  Network Address Translation (NAT)  89

**Overview**

All means all VPN/FireWall Modules that are able to perform Address Translation.

**Note** - It is best to select only the VPN/FireWall Modules that will actually be performing the NAT for the object. For an example of when selecting All is incorrect, see "Automatic ARP Configuration — Special Considerations" on page 82.

6  Click on **OK** or on **Apply**.

To view the NAT Rule Base (including the automatically generated rules), select the **Address Translation** tab in the Rule Base Editor.

The automatically generated rules are colored differently from manually defined rules, and are positioned first in the NAT Rule Base. Automatically generated rules cannot be modified using the Rule Base Editor, nor can you change their sequence. The automatically generated rules themselves can only be modified by editing the fields in the **NAT** tabs.

However, you can add rules before and after the automatically generated rules (see “Network Address Translation Rule Base” on page 89). If you add rules before the automatically generated rules and then add more automatically generated rules, the new automatically generated rules will be positioned together with the other automatically generated rules.

**Note** - If a host for which Address Translation has been defined has more than one IP address (for example, if it is a gateway with multiple interfaces), the only IP address that will be translated is the IP address specified in the **General** tab of its **Properties** window.

### Network Address Translation Rule Base

#### Overview

Network Address Translation is defined in the form of a NAT Rule Base, where each rule enables you to:

- specify objects by name rather than by IP address
- restrict rules to specified destination IP addresses, as well as to the specified source IP Addresses
- translate both source and destination IP addresses in the same packet
- restrict rules to specified services (ports)
- translate ports

#### Structure of a NAT Rule

A NAT rule, like a Security Policy rule, consists of two elements:
conditions that specify when the rule is to be applied
the action to be taken when the rule is applied (that is, when the conditions are satisfied)

The NAT Rule Base Editor (FIGURE 2-19) is divided into four sections:
• **Original Packet**
• **Translated Packet**
• **Install On**
• **Comment**

FIGURE 2-19NAT Rule Base

<table>
<thead>
<tr>
<th>No</th>
<th>Original Packet</th>
<th>Translated Packet</th>
<th>Install On</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any (inside)</td>
<td>Any (inside)</td>
<td>Any (inside)</td>
<td>Any (inside)</td>
</tr>
<tr>
<td>2</td>
<td>Any (inside)</td>
<td>Any (inside)</td>
<td>Any (inside)</td>
<td>Any (inside)</td>
</tr>
</tbody>
</table>

**Original Packet** and **Translated Packet** consist of, in turn:
• **Source**
• **Destination**
• **Service**

**Original Packet** specifies the conditions, that is, when the rule is applied.

**Translated Packet** specifies the action to be taken when the rule is applied.

The action is always the same:
• translate **Source** under **Original Packet** to **Source** under **Translated Packet**
• translate **Destination** under **Original Packet** to **Destination** under **Translated Packet**
• translate **Service** under **Original Packet** to **Service** under **Translated Packet**
If an entry under Translated Packet is Original, then the corresponding entry under Original Packet is not translated. TABLE 2-3 presents the various possibilities, using Service as an example.

**TABLE 2-3** Condition vs. Translation

<table>
<thead>
<tr>
<th>Translated Packet Service is ...</th>
<th>Original</th>
<th>&lt;new service&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>no conditions on Service, and Service is not translated</td>
<td>invalid combination — Security Policy will not verify</td>
</tr>
<tr>
<td>&lt;old service&gt;</td>
<td>the rule applies only to packets whose Service is &lt;old service&gt;, and Service is not translated</td>
<td>the rule applies only to packets whose Service is &lt;old service&gt;, and &lt;old service&gt; is translated to &lt;new service&gt;</td>
</tr>
</tbody>
</table>

**NAT Rule Base Example**

FIGURE 2-20 shows an example of a manually-defined NAT Rule Base.

**FIGURE 2-20** Manually-defined NAT Rule Base

<table>
<thead>
<tr>
<th>No.</th>
<th>Original Packet</th>
<th>Translated Packet</th>
<th>Install On</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>My Network</td>
<td>natasha</td>
<td>All</td>
<td>FW：&lt;HIDE&gt;</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Legal Addresses</td>
<td>All</td>
<td>FW：&lt;SRC STATIC&gt;</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Legal Addresses</td>
<td>All</td>
<td>FW：&lt;DEST STATIC&gt;</td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>DMZ, Services</td>
<td>All</td>
<td>FW：&lt;DPORT&gt;</td>
</tr>
</tbody>
</table>

**Note** · Routing tables on the gateway and router may have to be modified to implement NAT (see “Address Translation and Routing” on page 78).

**Rule 1**

The first rule in FIGURE 2-20 (a Hide Mode rule — note the small letter H under natasha’s icon) specifies that:
**Network Address Translation Rule Base**

**Condition** — when the original packet’s **Source** address belongs to the network object **MyNetwork**

**Action** — hide its **Source** address behind the address of the network object **natasha**

**Rule 2**

The second rule in FIGURE 2-20 (a Static Source Mode rule) specifies that:

**Condition** — when the original packet’s **Source** address is in the address range **IllegalAddresses**

**Action** — translate its **Source** address to the corresponding address in the address range **LegalAddresses**

**Rule 3**

The third rule in FIGURE 2-20 (a Static Destination Mode rule) specifies that:

**Condition** — when the original packet’s **Destination** address is in the address range **LegalAddresses**

**Action** — translate its **Destination** address to the corresponding address in the address range **IllegalAddresses**

**Rule 4**

The fourth rule in FIGURE 2-20 specifies that:

**Condition** — when the original packet’s **Service** is in the service range **StandardPorts** and its **Destination** is **DMZ-Servers**

**Action** — translate its **Service** to the corresponding **Service** in the service range **NonStandardPorts**

**Note** — The first three rules in this example can be automatically generated by the method described in “Generating Address Translation Rules Automatically” on page 87. The last rule cannot be automatically generated.

**Compound Conditions**

Conditions under **Original Packet** are ANDed together. For example, the fourth rule in FIGURE 2-20 has a compound condition, that is, there are two conditions to be met, both of which must be true in order for the rule to apply.

The two conditions are:

1) The original packet’s service number is in the service range **StandardPorts**.
2) The original packet’s **Destination** is **DMZ-Servers**.
Multiple Translation

If the addresses in two internal networks are invalid, there may be problems in communications between the two networks (see “Gateway with Three Interfaces” on page 106 for further information), which arise because both the source and destination addresses of packets must be translated.

The GUI allows the specification of multiple translations in a single rule. For example, FIGURE 2-21 shows a rule in which both the source and destination addresses of packets are translated.

FIGURE 2-21 Multiple Translation rule

For a detailed example of when a rule like this is necessary, see “Gateway with Three Interfaces” on page 106.

Defining Address Translation Rules

Before defining a NAT rule, you must first define the objects that will be used in the rule.

Under Source and Destination, you can use any Machine or Network network object, including groups and Address Range objects.

Under Service, you can use any TCP or UDP Services object, including groups and Port Range objects.

Note • Routing tables on the gateway and router may have to be modified to implement NAT (see “Address Translation and Routing” on page 78).

Using the NAT Rule Base Editor

To display the NAT Rule Base Editor (FIGURE 2-22), select the Address Translation tab in the Rule Base Editor.
To return to the Rule Base Editor, select the **Rule Base** tab.

The NAT Rule Base is part of a Security Policy. If you have more than one Security Policy, then each of them can have a corresponding NAT Rule Base. The NAT Rule Base is installed when the Security Policy is installed.

**Editing a NAT Rule Base**

**Adding a Rule**

You can add a rule at any point in the NAT Rule Base, except between automatically generated rules.

**TABLE 2-4** Adding a Rule

<table>
<thead>
<tr>
<th>No</th>
<th>Original Packet</th>
<th>Translated Packet</th>
<th>Install On</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Source</td>
<td>Destination</td>
<td>Service</td>
<td>Source</td>
</tr>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Original</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Original</td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>EMZ-Servers</td>
<td>StandardPorts</td>
<td>Original</td>
</tr>
<tr>
<td>5</td>
<td>User/LocalNet</td>
<td>User/EMZ</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

To add a rule

Select from menu

<table>
<thead>
<tr>
<th>Toolbar Button</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule&gt;Add&gt;Bottom</td>
</tr>
<tr>
<td>Rule&gt;Add&gt;Top</td>
</tr>
<tr>
<td>Rule&gt;Add&gt;After</td>
</tr>
<tr>
<td>Rule&gt;Add&gt;Before</td>
</tr>
</tbody>
</table>
A new rule will be added to the NAT Rule Base, and default values will appear in all the data fields. You can modify the default values as needed.

**Note** - To select a rule or rules, select their numbers.

**Modifying a Rule’s Data Fields**

To modify a data field in a rule, right click on the value. A menu will be displayed, from which you can choose the new value.

**Original Packet — Source**

Source can consist of only one object. The types of objects allowed for Source under Original Packet depend on what is specified for Source under Translated Packet, as listed in TABLE 2-5.

**TABLE 2-5** Original Packet - Source

<table>
<thead>
<tr>
<th>If Translated Packet - Source is ...</th>
<th>Original</th>
<th>Hide</th>
<th>Static</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine, Network, Address Range or a group of one of these</td>
<td>Machine, Network, Address Range or a group of one of these</td>
<td>Machine, Network, Address Range but not a group</td>
<td></td>
</tr>
</tbody>
</table>

**Add** — The Object Manager window (FIGURE 2-23) is displayed, from which you can select a network object.

**FIGURE 2-23** Object Manager window

**Replace** — The Object Manager window (FIGURE 2-23) is displayed, from which you can select an object to replace the object currently in the rule’s Source.

**Edit** — Edit the object in the rule’s Source.

The appropriate window is opened (depending on the type of the selected object), and you can change the object’s properties.

**Delete** — Delete the object currently in the rule’s Source.

**Cut** — Delete the object currently in the rule’s Source and put it on the clipboard.
Copy — Copy the object currently in the rule’s Source to the clipboard.

Paste — Paste the object on the clipboard in the rule’s Source.

Original Packet — Destination

Destination can consist of only one object. The types of objects allowed for Destination under Original Packet depend on what is specified for Destination under Translated Packet, as listed in TABLE 2-6.

TABLE 2-6 Original Packet - Destination

<table>
<thead>
<tr>
<th>If Translated Packet - Destination is ...</th>
<th>Original</th>
<th>Static</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Packet - Destination can be ...</td>
<td>Machine, Network, Address Range or a group of one of these</td>
<td>Machine, Network, Address Range but not a group</td>
</tr>
</tbody>
</table>

Add — The Object Manager window (FIGURE 2-23) is displayed, from which you can select a network object.

Replace — The Object Manager window (FIGURE 2-23) is displayed, from which you can select an object to replace the object currently in the rule’s Destination.

Edit — Edit the object in the rule’s Destination.

The appropriate window is opened (depending on the type of the selected object), and you can change the object’s properties.

Delete — Delete the object currently in the rule’s Destination.

Cut — Delete the object currently in the rule’s Destination and put it on the clipboard.

Copy — Copy the object currently in the rule’s Destination to the clipboard.

Paste — Paste the object on the clipboard in the rule’s Destination.
Original Packet — Service

Services can consist of only one object. The types of objects allowed for Services under Original Packet depend on what is specified for Services under Translated Packet, as listed in TABLE 2-7.

TABLE 2-7 Original Packet - Services

<table>
<thead>
<tr>
<th>Original Packet - Services can be ...</th>
<th>If Translated Packet - Services is ...</th>
<th>Original</th>
<th>Hide</th>
<th>Static</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP, UDP, Range or group of one of the above</td>
<td>TCP, UDP, Range or group of one of the above</td>
<td>TCP, UDP, Range but not a group</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Add — The Services window (FIGURE 2-24) is displayed, from which you can select a service.

FIGURE 2-24 Services window

Replace — The Services window (FIGURE 2-24) is displayed, from which you can select an object to replace the object currently in the rule’s Services.

Edit — Edit the service.

The appropriate window is opened (depending on the type of the selected service), and you can change the service’s properties.

Delete — Delete the object currently in the rule’s Services.

Cut — Delete the object currently in the rule’s Services and put it on the clipboard.

Copy — Copy the object currently in the rule’s Services to the clipboard.
Paste — Paste the object on the clipboard in the rule’s Services.

Translated Packet — Source

Source can consist of only one object. The types of objects allowed for Source depend on the type of Address Translation, as listed in TABLE 2-8.

TABLE 2-8 Translated Packet - Source

<table>
<thead>
<tr>
<th>Translated Packet - Source can be ...</th>
<th>If the Address Translation is</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hide</td>
</tr>
<tr>
<td>Machine, Network, or Router, or Range of size 1</td>
<td>Machine, Network, or Router, or Range of size 1</td>
</tr>
</tbody>
</table>

Add (Static) — The Object Manager window (FIGURE 2-23 on page 95) is displayed, from which you can select a network object.

The Source object under Original Packet will be translated to Source under Translated Packet, in Source Static Mode.

Replace (Static) — The Object Manager window (FIGURE 2-23 on page 95) is displayed, from which you can select an object to replace the object currently in the rule’s Source.

Replace (Static) is only available when the Source object was added by Add (Static). If you wish to replace an Add (Hide) object by an Add (Static) object, first delete the Add (Hide) object, and then choose Add (Static) from the menu.

Add (Hide) — The Object Manager window (FIGURE 2-23 on page 95) is displayed, from which you can select a network object.

The Source object under Original Packet will be translated to Source under Translated Packet, in Hide mode.

Replace (Hide) — The Object Manager window (FIGURE 2-23 on page 95) is displayed, from which you can select an object to replace the object currently in the rule’s Source.

Replace (Hide) is only available when the Source object was added by Add (Hide). If you wish to replace an Add (Static) object by an Add (Hide) object, first delete the Add (Static) object, and then choose Add (Hide) from the menu.

Edit — Edit the Source object.

The appropriate window is opened (depending on the type of the Source object), and you can change the object’s properties.
Delete — Delete the object currently in the rule’s Source.

After you delete the object, Source is set to Original.

Cut — Delete the object currently in the rule’s Source and put it on the clipboard.

After you cut the object, Source is set to Original.

Copy — Copy the object currently in the rule’s Source to the clipboard.

Paste — Paste the object on the clipboard in the rule’s Source.

Translated Packet — Destination

Destination can consist of only one object. The types of objects allowed for Destination depend on the type of Address Translation, as listed in TABLE 2-9.

**TABLE 2-9 Translated Packet - Destination**

<table>
<thead>
<tr>
<th>Translated Packet - Destination can be ...</th>
<th>If the Address Translation is Hide</th>
<th>If the Address Translation is Static</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine, Network, or Range of same size as Original Packet - Destination</td>
<td>Machine, Network, Router, or Range of size 1</td>
<td></td>
</tr>
</tbody>
</table>

Add (Static) — The Object Manager window (FIGURE 2-23 on page 95) is displayed, from which you can select a network object.

The Destination object under Original Packet will be translated to Destination under Translated Packet, in Destination Static Mode.

Replace (Static) — The Object Manager window (FIGURE 2-23 on page 95) is displayed, from which you can select an object to replace the object currently in the rule’s Destination.

Replace (Static) is only available when the Destination object was added by Add (Static).

Edit — Edit the Destination object.

The appropriate window is opened (depending on the type of the Destination object), and you can change the object’s properties.

Delete — Delete the object currently in the rule’s Destination.

After you delete the object, Destination is set to Original.

Cut — Delete the object currently in the rule’s Destination and put it on the clipboard.
After you cut the object, **Destination** is set to **Original**.

**Copy** — Copy the object currently in the rule’s **Destination** to the clipboard.

**Paste** — Paste the object on the clipboard in the rule’s **Destination**.

**Translated Packet — Service**

**Service** can consist of only one object. The types of objects allowed for **Service** are:

- TCP
- UDP
- Port Range

**Add (Static)** — The **Service** window (FIGURE 2-24 on page 97) is displayed, from which you can select a network object.

The **Service** object under **Original Packet** will be translated to **Service** under **Translated Packet**.

**Replace (Static)** — The **Services** window (FIGURE 2-24 on page 97) is displayed, from which you can select an object to replace the object currently in the rule’s **Service**.

**Replace (Static)** is only available when the **Service** object was added by **Add (Static)**.

**Edit** — Edit the **Service** object.

The appropriate window is opened (depending on the type of the **Service** object), and you can change the object’s properties.

**Delete** — Delete the object currently in the rule’s **Service**.

After you delete the object, **Service** is set to **Original**.

**Cut** — Delete the object currently in the rule’s **Service** and put it on the clipboard.

After you cut the object, **Service** is set to **Original**.

**Copy** — Copy the object currently in the rule’s **Service** to the clipboard.

**Paste** — Paste the object on the clipboard in the rule’s **Service**.

**Install On**

The **Install On** field specifies which FireWalled objects will enforce the rule. You cannot change the **Install On** field for automatically generated rules, but you can change it for manual rules.
To modify the **Install On** field, right click on it. A menu is displayed, from which you can select one of the values listed in TABLE 2-10.

**TABLE 2-10 Install On Menu**

<table>
<thead>
<tr>
<th>Install On</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Gateway Icon]</td>
<td><strong>Gateways</strong> — Enforce on all network objects defined as gateways.</td>
</tr>
<tr>
<td>![Firewall Icon]</td>
<td><strong>Integrated FireWalls</strong> — Enforce on all network objects defined as integrated FireWalls.</td>
</tr>
<tr>
<td>![Target Icon]</td>
<td><strong>Targets</strong> — Enforce on the specified target object(s) only.</td>
</tr>
</tbody>
</table>

**Comment**

You can add comments to a rule. Double click on the **Comment** field to open the **Comment** window (FIGURE 2-25).

**FIGURE 2-25 Comment window**

Type any text you wish in the text box and click on **OK**.

**Copying, Cutting and Pasting Rules**

To copy, cut or paste, select a rule or rules by selecting their numbers.

**TABLE 2-11 Copying, Cutting and Pasting Rules**

<table>
<thead>
<tr>
<th>Action</th>
<th>Select from menu</th>
<th>Toolbar Button</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cut</td>
<td><strong>Edit&gt;Cut</strong></td>
<td>![Cut Icon]</td>
</tr>
<tr>
<td>Copy</td>
<td><strong>Edit&gt;Copy</strong></td>
<td>![Copy Icon]</td>
</tr>
<tr>
<td>Paste</td>
<td><strong>Edit&gt;Paste</strong></td>
<td>![Paste Icon]</td>
</tr>
</tbody>
</table>
If you choose **Paste**, then the **Paste** menu will be opened. You must then select **Before**, **After**, **Top**, or **Bottom** to specify where in the Rule Base to paste the rule.

**Address Translation Examples**

*Gateway with Two Interfaces*  
*Gateway with Three Interfaces*  

**Gateway with Two Interfaces**

Consider the following network and Address Translation configuration:

*FIGURE 2-26 Gateway with Two Interfaces Example - Network*

**Defining NAT**

Since the mailserver accepts and initiates connections, it requires static translation, as shown in *FIGURE 2-27*. 

---

102 Check Point FireWall-1 • September 2002
Similarly, the Address Range from 10.0.67.0 to 10.0.67.16 is meant to provide public services, such as HTTP or FTP, to the outside world, and so it too requires Static Translation.
These addresses are mirrored as the seventeen (17) addresses from 199.100.73.64 to 199.100.73.80. So, for example, when an outside machine sends a packet to IP address 199.100.73.70, the packet will actually arrive at 10.0.67.6.

Finally, localnet addresses will be hidden behind the IP address of the gateway's external interface, 199.100.73.2 (FIGURE 2-29).
The rules generated from these definitions are shown in FIGURE 2-30.

**Routing**

Assume that the Internet routes IP addresses in the network 199.100.73.0 to the router. Then you should ensure that:
1 The router routes IP addresses in the network 199.100.73.0 to the gateway.
2 The gateway routes IP address 199.100.73.3 to the internal interface (10.0.0.1).
3 The gateway routes IP addresses 199.100.73.64 to 199.100.73.80 to the internal interface (10.0.0.1).

Gateway with Three Interfaces

Hide Mode and Static Mode

Consider the following network and Address Translation configuration:

Suppose we wish to hide all the localnet and DMZ hosts behind the gateway, except for host 192.9.200.9 (HTTPServer), which will be providing public services and so must be accessible from the Internet.

Defining Address Translation

Hiding localnet

To hide localnet addresses, define Address Translation as follows for localnet:
Hiding PrivateNet

To hide PrivateNet addresses, define Address Translation as follows for PrivateNet:
HTTPServer

To statically translate HTTPServer’s address, define its Address Translation as follows:
Rules

The rules generated from these definitions are shown in FIGURE 2-35.

FIGURE 2-35 Automatically generated rules - three interfaces

<table>
<thead>
<tr>
<th>No.</th>
<th>Original Packet</th>
<th>Translated Packet</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Source</td>
<td>Destination</td>
<td>Service</td>
</tr>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>HTTPS Server (Valid Address)</td>
<td>Any</td>
</tr>
<tr>
<td>3</td>
<td>Private Net</td>
<td>Private Net</td>
<td>Any</td>
</tr>
<tr>
<td>4</td>
<td>Private Net</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>5</td>
<td>Localnet</td>
<td>Localnet</td>
<td>Any</td>
</tr>
<tr>
<td>6</td>
<td>Localnet</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

Note that the Static Mode rules are positioned before the Hide Mode rules.
Communications Between Hosts in Different Internal Networks

The NAT Rule Base works much like the Security Policy Rule Base. The Address Translation rules are scanned sequentially, one after the other, until a match is found. The Address Translation indicated by the matching rule is performed, and then the packet is sent on its way.

Suppose host 172.45.126.47 (in localnet) tries to TELNET to host 192.45.125.209 (the valid address of HTTPServer, whose invalid address is 192.9.200.9) in PrivateNet. The first rule that matches is rule 2, so the destination address 172.45.125.209 is translated to 192.9.200.9, and the packet arrives at its destination. The packet’s source address (172.45.126.47) remains untranslated, so the reply will be sent to 172.45.126.47 and arrive at its destination.

Routing

Assume that the Internet routes the IP addresses in the network 192.45.125.0 to the router.

You should ensure that:

1. The router routes the IP addresses in the network 192.45.125.0 to the gateway.
2. The gateway routes IP address 172.45.125.209 to the internal interface (192.9.200.1).

Both Networks Statically Translated

Consider the following network and Address Translation configuration:

Suppose we wish to statically translate the addresses in both networks (localnet and PublicNet). The automatically generated NAT Rule Base is show in FIGURE 2–37.

FIGURE 2-36 Three Interfaces — both networks statically translated
Communications Between Hosts Behind the Same Gateway

Suppose a host in localnet tries to TELNET to a host in PublicNet, using the PublicNet host’s valid IP address as the destination IP address. The first rule that applies is rule 3, so the destination address is translated and the packet is correctly routed to the destination. The reply packets are correctly routed as well, since the source IP address is not translated.

On the other hand, suppose a host in PublicNet tries to TELNET to a host in localnet, using the localnet host’s valid IP address as the destination IP address. The first rule that matches is rule 2, so the source address is translated, but the destination address is not translated, so the packet will not arrive at its destination.

Multiple Translation Rules

One solution is to add two rules before the automatically generated rules as follows:
Now, both source and destination IP addresses will be translated, so packets will be routed to their correct destinations.

**Simple Rules**

Another solution is to add the same two rules, but to set **Source** under **Translated Packet** to **Original**. This solution will work because there is really no need to translate the source IP address when both networks are connected to the same gateway, which knows how to route to the internal invalid IP addresses of both networks.

**Communications Between Hosts Behind Different Gateways**

Consider the case when the internal networks are connected to different gateways controlled from the same SmartCenter Server. In this case, both source and destination IP addresses must be translated, because each gateway knows how to route only to its own internal invalid IP addresses. Therefore, only the first of the above solutions (multiple translation rules) will work.

**Advanced Topics**

**Rule Base**

*Note* - This section describes anomalies which must be considered when you define Address Translation manually. If you generate Address Translation rules automatically, these considerations do not apply.

The VPN/FireWall Module sees the packet as the initiator of the connection sees it, and the Rule Base should be defined accordingly.
In the usual situation, this means that if the source (from the initiator’s point of view) is an internal host and the destination an external one, then the source object in the rule should be the internal invalid address.

If, from the initiator’s point of view, the source is an external host and the destination is an internal one, then the destination objects in the rule should be the external addresses of the FWXT_DST_STATIC translated hosts(s).

For example, consider the network configuration and Address Translation rules described in FIGURE 2-26 on page 102. A rule in the Rule Base that refers to incoming mail would specify the mail server (under Destination) as 199.100.73.3, because the initiator of the communication (the outside host) knows the mail server under that name (IP address).

On the other hand, a rule in the Rule Base that refers to outgoing mail would specify the mail server (under Source) as 10.0.0.2, because the initiator of the communication (the internal network) knows the mail server under that name (IP address).

**Overlapping NAT**

**Overview**

Where two or more internal networks have overlapping (or partially overlapping) invalid IP addresses, VPN-1/FireWall-1, makes it possible to:

- enable communications between the overlapping internal networks
- enable communications between the overlapping internal networks and the outside world
- enforce a different Security Policy for each of the overlapping internal networks, if desired.

**Network Configuration**

The network shown in FIGURE 2-39 will be used as an example.
Both network A and network B share the same address space (10.0.0.0), so the standard VPN-1/FireWall-1 NAT cannot be used to enable communications between network A and network B. Instead, overlapping NAT must be performed on a per-interface basis.

The VPN/FireWall Module will translate the IP addresses differently on each interface, as follows:

**interface 1**
- inbound source IP addresses will be translated to network 11.0.0.0
- outbound destination IP addresses will be translated to network 10.0.0.0

**interface 2**
- inbound source IP addresses will be translated to network 12.0.0.0
- outbound destination IP addresses will be translated to network 10.0.0.0

**interface 3**
Overlapping NAT will not be configured for this interface. Instead, use NAT Hide in the usual way (not on a per-interface basis) to hide source addresses behind the interface’s IP address (13.0.0.1).

**Limitations**
The Virtual Machine is unaware of overlapping NAT. The following are not supported with Overlapping NAT

- Products other than FireWall-1.
• In combination with other products (FloodGate-1 for example)
• Accounting logs cannot be chosen in the Track column

**Example**

**Between Internal Networks**

Suppose user A at IP address 10.0.0.10 in network A connects to IP address 10.0.0.10 (the same IP address) in network B. User A opens a connection to IP address 12.0.0.10.

<table>
<thead>
<tr>
<th>step</th>
<th>source IP address</th>
<th>destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface 1 — before NAT</td>
<td>10.0.0.10</td>
<td>12.0.0.10</td>
</tr>
<tr>
<td>interface 1 — after NAT</td>
<td>11.0.0.10</td>
<td>12.0.0.10</td>
</tr>
</tbody>
</table>

VPN/FireWall Module enforces Security Policy for packets from network 11 to network 12.

<table>
<thead>
<tr>
<th>step</th>
<th>source IP address</th>
<th>destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface 2 — before NAT</td>
<td>11.0.0.10</td>
<td>12.0.0.10</td>
</tr>
<tr>
<td>interface 2 — after NAT</td>
<td>11.0.0.10</td>
<td>10.0.0.10</td>
</tr>
</tbody>
</table>

**Between an Internal Network and the Internet**

Suppose user A at IP address 10.0.0.10 in network A connects to IP address 20.0.0.10 on the Internet.

<table>
<thead>
<tr>
<th>step</th>
<th>source IP address</th>
<th>destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface 1 — before NAT</td>
<td>10.0.0.10</td>
<td>20.0.0.10</td>
</tr>
<tr>
<td>interface 1 — after NAT</td>
<td>11.0.0.10</td>
<td>20.0.0.10</td>
</tr>
</tbody>
</table>

VPN/FireWall Module enforces Security Policy for packets from network 11 to the Internet.

<table>
<thead>
<tr>
<th>step</th>
<th>source IP address</th>
<th>destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface 3 — before NAT</td>
<td>11.0.0.10</td>
<td>20.0.0.10</td>
</tr>
<tr>
<td>interface 3 — after NAT Hide</td>
<td>13.0.0.1</td>
<td>20.0.0.10</td>
</tr>
</tbody>
</table>
Implementation

To implement the overlapping NAT feature, edit `Objects_5_0.c` as follows for each of the interfaces. Do not edit this file directly. Use the `dbedit` database editor GUI (or command line utility):

```
(enable_overlapping_nat:type (boolean):defvalue (false)) set to true
  : (overlap_nat_src_ipaddr:type (ip_address_or_empty)) the invalid overlapping network address
  : (overlap_nat_dst_ipaddr:type (ip_address_or_empty)) the valid (legal) network address
  : (overlap_nat_netmask:type (net_mask)) netmask of the overlapping net
```

In the example configuration, you would set the values for interface 1 and interface 2 as follows:

<table>
<thead>
<tr>
<th>parameter</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable_overlapping_nat</td>
<td>true</td>
</tr>
<tr>
<td>overlap_nat_src_ipaddr</td>
<td>The overlapping IP addresses (before NAT). In the example configuration, this would be 10.0.0.0 for both interfaces.</td>
</tr>
<tr>
<td>overlap_nat_dst_ipaddr</td>
<td>The IP addresses after NAT. In the example configuration, this would be 11.0.0.0 for interface 1, and 12.0.0.0 for interface 2.</td>
</tr>
<tr>
<td>overlap_nat_netmask</td>
<td>The net mask of the overlapping IP addresses (before NAT).</td>
</tr>
</tbody>
</table>

Note: VPN-1/FireWall-1 will drop packets from an internal networks whose source IP addresses (before overlapping NAT) does not belong to the network specified for `overlap_nat_src_ipaddr`.

Frequently Asked Questions

Question: Why do the translated addresses seem not to exist (I can't even ping them) even though the Address Translation configuration is correct?

You must modify the gateway's internal routing tables to enable this to happen.
Suppose the Address Translation is configured as follows:

<table>
<thead>
<tr>
<th>No.</th>
<th>From Original Address (Port)</th>
<th>To Original Address (Port)</th>
<th>Method</th>
<th>First Translated Address (Port)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>206.73.224.1</td>
<td>206.73.224.1</td>
<td>FWXT_SRC_STATIC</td>
<td>192.168.145.11</td>
</tr>
<tr>
<td>1</td>
<td>192.168.145.11</td>
<td>192.168.145.11</td>
<td>FWXT_DST_STATIC</td>
<td>206.73.224.1</td>
</tr>
<tr>
<td>2</td>
<td>206.73.224.85</td>
<td>206.73.224.85</td>
<td>FWXT_SRC_STATIC</td>
<td>192.168.145.12</td>
</tr>
<tr>
<td>3</td>
<td>192.168.145.12</td>
<td>192.168.145.12</td>
<td>FWXT_DST_STATIC</td>
<td>206.73.224.85</td>
</tr>
</tbody>
</table>

If you ping 192.168.145.11 (whether from outside your network or from inside it), then the gateway routes the ping request to its external interface and it is never received by 192.168.145.11. This is because the internal routing takes place before the Address Translation.

In order to be able to ping 192.168.145.11 and 192.168.145.12, you must add static routes in the gateway which tell it to forward packets destined for 192.168.145.11 and 192.168.145.12 to the internal interface.

For additional information, see “Configuring Routing on the Gateway” on page 78.

**Question: Can I translate the gateway’s internal address?**

**Note** - This section describes anomalies which must be considered when you define Address Translation manually. If you generate Address Translation rules automatically, these considerations do not apply.

You should not translate the internal address (the address of the internal interface) of the translating gateway.

For example, consider the following network and Address Translation configuration:
This example shows a simple translation scheme that hides the entire internal network, whose addresses are invalid, behind a valid address. The problem with this configuration is that the VPN/FireWall Module's internal address (10.0.0.8) is also translated to the gateway's external address, since 10.0.0.8 is in the range 10.0.0.0 – 10.255.255.255. An attempt to communicate from the gateway to an internal machine will not succeed.

For example, if you TELNET from the gateway to 10.0.0.1, the gateway’s internal address (10.0.0.8) will be translated to 199.100.73.200. The reply packet will not reach its destination, because 10.0.0.1 will not be able to route the reply to 199.100.73.200.

To solve this problem, use the following address translation scheme, which translates all the addresses except the gateway’s address:

<table>
<thead>
<tr>
<th>No.</th>
<th>From Original Address (Port)</th>
<th>To Original Address (Port)</th>
<th>Method</th>
<th>First Translated Address (Port)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>10.0.0.1</td>
<td>10.255.255.255</td>
<td>FWXT_HIDE</td>
<td>199.100.73.200</td>
</tr>
<tr>
<td>1</td>
<td>10.0.0.9</td>
<td>10.255.255.255</td>
<td>FWXT_HIDE</td>
<td>199.100.73.200</td>
</tr>
</tbody>
</table>

Question: How can I use Encryption and Address Translation together on the same system?

Note - You do not have to do anything to ensure that Encryption is performed correctly for those objects for which you generate NAT rules automatically. This section describes anomalies which must be considered when you define NAT rules manually.
For example, suppose you want to encrypt between Network-A and Network-B, where Network-A uses invalid addresses translated as follows:

<table>
<thead>
<tr>
<th>No.</th>
<th>From Original Address (Port)</th>
<th>To Original Address (Port)</th>
<th>Method</th>
<th>First Translated Address (Port)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>10.1.1.2</td>
<td>10.1.1.2</td>
<td>FWXT_SR_C_STATIC</td>
<td>192.91.18.2</td>
</tr>
<tr>
<td>1</td>
<td>192.91.18.2</td>
<td>192.91.18.2</td>
<td>FWXT_DST_STATIC</td>
<td>10.1.1.2</td>
</tr>
<tr>
<td>2</td>
<td>10.1.1.3</td>
<td>10.1.1.255</td>
<td>FWXT_HIDE</td>
<td>192.91.18.3</td>
</tr>
</tbody>
</table>

Network-B uses the valid addresses of network 195.8.5.0.

FireWall-A (Network-A’s FireWall) should specify as its Encryption Domain both the invalid addresses (10.1.1.x) and the valid addresses (192.91.18.x).

FireWall-B (Network-B’s FireWall) knows FireWall-A only by its valid address.

**Encryption Rules**

On FireWall-A, two Encryption rules are needed:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.0</td>
<td>195.8.5.0</td>
<td>Any</td>
<td>Encrypt</td>
<td>Log</td>
<td>Gateways</td>
</tr>
<tr>
<td>195.8.5.0</td>
<td>192.91.18.0</td>
<td>Any</td>
<td>Encrypt</td>
<td>Log</td>
<td>Gateways</td>
</tr>
</tbody>
</table>

As with all Address Translation, the VPN/FireWall Module see the packets as the originator of the connection sees it, so the first rule applies to outgoing connections and the second rule applies to incoming connections.

Two Encryption rules are needed on FireWall-B as well:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.91.18.0</td>
<td>195.8.5.0</td>
<td>Any</td>
<td>Encrypt</td>
<td>Log</td>
<td>Gateways</td>
</tr>
<tr>
<td>195.8.5.0</td>
<td>192.91.18.0</td>
<td>Any</td>
<td>Encrypt</td>
<td>Log</td>
<td>Gateways</td>
</tr>
</tbody>
</table>

*Overlapping NAT*
Here too the first rule applies to outgoing connections and the second rule applies to incoming connections, but the same addresses are used in both rules, since FireWall-B doesn’t know about Network-A’s invalid addresses.

**Note** - When using an encryption scheme of type Tunnel Mode, it is usually not necessary to use NAT, because the packet’s original IP header is replaced by an IP header in which the source IP address is that of the gateway’s external interface and the destination IP address is that of the peer gateway’s external interface.

The sequence of actions between Network-A and Network-B is as follows (for a connection from Network-A to Network-B):

1. The packet’s source IP address is translated by FireWall-A.
2. The packet is encrypted and encapsulated by FireWall-A.
   - The outer IP header contains the gateways’ IP addresses and the inner header contains the translated IP addresses.
3. The packet is decrypted by FireWall-B.
4. The return packet is encrypted by FireWall-B.
5. The return packet is decrypted by FireWall-A.
6. The return packet’s destination IP address is translated by FireWall-A.

**Question: What happens when an internal host with an invalid internal IP address tries to communicate with an external host that has the same IP address?**

In this case, the internal network does not conform to the IANA recommendations (see “Frequently Asked Questions” on page 116) but instead uses IP addresses that “belong” to another network.

Consider what happens when the internal host 129.1.1.1 in FIGURE 2-41 tries to talk to the external host 129.1.1.1.

**FIGURE 2-41** Invalid IP Addresses

```
localnet          Public
|                  |
| 128.1.1.1       | 129.1.1.1
|      Gateway    |      router    |
|      | Internet     |
|      |
```

120  Check Point FireWall-1  •  September 2002
The outbound packet will remain in the host, since it looks like this:

<table>
<thead>
<tr>
<th>Source IP Address</th>
<th>Destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>129.1.1.1</td>
<td>129.1.1.1</td>
</tr>
</tbody>
</table>

The host will route the packet right back to itself, and the packet will never reach the gateway.

If the internal host 128.1.1.1 tries to talk to the external host 129.1.1.1, the gateway will route the communication to the internal host 129.1.1.1 (connected to the gateway through another interface) rather than to the external host 129.1.1.1.

Using FWXT_HIDE to hide the invalid IP addresses behind the gateway’s valid address will not help, because with FWXT_HIDE the Address Translation takes place on the gateway’s external interface. The packet will not get that far because it will have been routed to the other internal interface.
CHAPTER 3

Authentication

In This Chapter

Overview ........................................................................................................ page 123
User Authentication ...................................................................................... page 126
Session Authentication ................................................................................ page 162
Client Authentication ................................................................................... page 173

Overview

VPN-1/FireWall-1 Authentication

VPN-1/FireWall-1’s Authentication feature enables you to verify the identity of a user logging on to VPN-1/FireWall-1 and to control security by allowing some users access while disallowing others. A user authenticates himself or herself by proving his or her identity according to the scheme specified under Authentication Scheme in the Authentication tab of his or her User Properties window (FIGURE 3-1).

FIGURE 3-1 User Properties window — Authentication tab
VPN-1/FireWall-1 supports three types of authentication and several authentication schemes. Because Authentication is specified in a rule’s Action field, Authentication can be combined with the other fields in a rule in a very flexible manner. In addition, VPN-1/FireWall-1 supports both Transparent and Non-transparent Authentication.

Three Types of Authentication

There are three types of Authentication:

- **User Authentication**
  
  User Authentication grants access on a per user basis. This method can only be used for TELNET, FTP, RLOGIN and HTTP, and requires a separate authentication for each connection. It is secure (because the authentication is valid only for one connection), but intrusive (because each connection requires another authentication).

- **Session Authentication**

  Session Authentication is like User Authentication in that it requires an authentication procedure for each connection, but unlike User Authentication, it can be used with any service. It is secure but requires a Session Authentication agent running on the client or another machine in the network.

- **Client Authentication**

  Client Authentication grants access on a per host basis. Client Authentication allows connections from a specific IP address after successful authentication. It can be used for any number of connections, for any service and the authentication is valid for the length of time defined by the administrator. It is less secure than User Authentication (because it allows any user access from the IP address or host) but is also less intrusive. It is best used when the client is a single-user machine, such as a PC.

Some of these authentication methods can be used together (e.g. Client and Session) in order to optimize the benefits of each without the disadvantages. For more information, see “Partially Automatic Sign On Method” on page 197 and “Fully Automatic Sign On Method” on page 198.
Comparison of Authentication Types

TABLE 3-1 compares the features of the three VPN-1/FireWall-1 Authentication types.

<table>
<thead>
<tr>
<th>User Authentication</th>
<th>Session Authentication</th>
<th>Client Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>which services</td>
<td>TELNET, FTP, RLOGIN, HTTP</td>
<td>all services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>all services</td>
</tr>
<tr>
<td>authentication is performed once per...</td>
<td>session</td>
<td>session</td>
</tr>
<tr>
<td>use when you want a user to...</td>
<td>authenticate each time he or she uses one of the supported services</td>
<td>authenticate each time he or she uses any service (this requires a Session Authentication Agent running on the client or another machine in the network)</td>
</tr>
</tbody>
</table>

Authentication Schemes

VPN-1/FireWall-1 supports the following Authentication schemes:

- **S/Key** — The user is challenged to enter the value of requested S/Key iteration.

  For an explanation of how to define S/Key authentication, see Chapter 13, “User Monitor” of Check Point SmartCenter Guide.

- **SecurID** — The user is challenged to enter the number displayed on the Security Dynamics SecurID card.

- **OS Password** — The user is challenged to enter his or her OS password.

- **VPN-1 & FireWall-1 Password** — The user is challenged to enter his or her VPN-1 & FireWall-1 password on the gateway.

  The advantage of a VPN-1 & FireWall-1 Password over the OS password is that a VPN-1 & FireWall-1 Password can be used even if the user does not have an OS account on the gateway.

- **RADIUS** — The user is challenged for the response, as defined by the RADIUS server.
For information about defining RADIUS servers, see “ACE (SecurID) Servers” on page 365 of Check Point SmartCenter Guide.

- **AXENT Pathways** — The user is challenged for the response, as defined by the AXENT Pathways server.

For information about defining Axent Pathways servers, see “AXENT Pathways Defender Servers” on page 365 of Check Point SmartCenter Guide.

- **TACACS** — The user is challenged for the response, as defined by the TACACS or TACACS+ server.

For information about defining TACACS servers, see “TACACS Servers” on page 364 of Check Point SmartCenter Guide.

- **Undefined** — No authentication is performed and access is always denied.

**Note** - A user can have different passwords on different gateways (for example, if the Authentication Scheme is OS Password), but only one Authentication scheme for all gateways.

### Transparent and Non-transparent Authentication

Authentication is considered transparent when a user does not have to explicitly connect to the VPN/FireWall Module to perform the authentication before continuing to the destination. The connection attempt (for example, when the user issues the TELNET command) is intercepted by VPN-1/FireWall-1 on the gateway and the authentication procedure is activated. If the authentication is successful, and the connection is allowed by the rule, the connection proceeds to the destination.

VPN-1/FireWall-1 also supports Non-transparent Authentication for TELNET, RLOGIN, HTTP and FTP. In Non-transparent Authentication, the user must first connect directly to the gateway and authenticate before being allowed to continue to the target host. For more information see “Non-Transparent User Authentication” on page 140.

### User Authentication

In This Section

- User Authentication — Overview
- User Authentication — Deployment
- Non-Transparent User Authentication
- User Authentication and the HTTP Security Server
User Authentication — Overview

User Authentication is provided by the TELNET, FTP, HTTP and RLOGIN VPN-1/FireWall-1 Security Servers on the gateway. When a rule specifies User Authentication, the corresponding VPN-1/FireWall-1 Security Server is invoked in order to mediate the connection.

The Security Server then authenticates the user, in accordance with the authentication scheme defined for the user in the Authentication tab of the User Properties window.

- If no authentication scheme is specified for a user, the user will be denied access.
- If an external authentication scheme is specified (that is, RADIUS, TACACS, or Axent Defender) the Security Server queries the appropriate third-party server regarding the user’s permissions. The third-party server returns the appropriate data to the Security Server.

If authentication is successful, the TELNET Security Server opens a separate connection to the target server. Altogether, there are two connections, one to the Security Server on the gateway, and another from the Security Server to the final destination. The final destination server sees the connection as originating from the gateway, not the client. Authentication is transparent — the user TELNETs to the target server, and not to the gateway.

User Authentication rules allow users if they authenticate successfully, but do not necessarily reject the connection if the user fails authentication. If the user authenticates successfully, he or she matches the user limitation and the Authentication rule limitation for of the user group her or she belongs to. In the case of no Authentication Rule match, the connection proceeds to the next non-Authentication rule that may apply.

In addition, the fact that a user successfully authenticates does not necessarily mean that there is a rule that allows that user access. This is because the authenticating Security Server first checks if the connection can be allowed by a rule which does not require authentication. For more information, see “The ‘Insufficient Information’ Problem” on page 208.

User Authentication — Deployment

This section describes a deployment example for User Authentication. A deployment example consists of:

- an example network configuration
- what the Security Administrator must define in the VPN-1/FireWall-1 Rule Base
- what a user must do to authenticate
User Authentication

This example is not intended as a set of step by step instructions, but rather to illustrate how and where different components of User Authentication are configured in the VPN-1/FireWall-1 GUI.

Example Configuration

FIGURE 3-2 depicts an example configuration in which London, the VPN/FireWall Module, protects a local network and a DMZ.

The Security Administrator for this configuration may want to allow only localnet managers access to files on BigBen, the FTP server. The following rule allows a user group (LocalManagers) to access the FTP server after successful User Authentication.

Defining User Authentication

In order to implement User Authentication for this configuration and rule, you must define the following:

- the permitted user group
- authentication schemes supported by the gateway
- tracking and timeout parameters
- User Authentication action properties

Defining Permitted User Groups

In a User Authentication rule, the Source must be a user group (i.e., LocalManagers). You must first define the permitted users, their authentication scheme or schemes and the network objects from which each user is allowed access. These properties are defined in the tabs of the User Properties window.
Next, define a user group called “LocalManagers” consisting of the users who are allowed access.

For more information on defining users and user groups, see Chapter 4, “Managing Users and Administrators” of Check Point SmartCenter Guide.

**Defining the Gateway's Authentication Schemes**

The gateway must support the same authentication schemes you defined for your users. For example, if some users in the group “LocalManagers” are using a VPN-1 & FireWall-1 Password, and others are using S/Key authentication, you must make sure...
the gateway supports both **VPN-1 & FireWall-1 Password** and **S/Key** authentication schemes. The gateway’s authentication schemes are defined in the **Authentication** page of its **Properties** window (FIGURE 3-6).

**FIGURE 3-6 Gateway Properties window — Authentication page**

**Tracking and Timeout Parameters**

Specify tracking for failed authentication attempts and timeout parameters in the **Authentication Settings** field in the **Authentication** page of the gateway’s **Properties** window (FIGURE 3-8 on page 134). These parameters apply to all rules.

**User Authentication session timeout (minutes)** — the session will time out if there is no activity for this time period. See TABLE 3-2 on page 131 for the meaning of the term “no activity.”
This applies to the FTP, TELNET, and RLOGIN Security Servers.

**TABLE 3-2** Meaning of “No Activity”

<table>
<thead>
<tr>
<th>service</th>
<th>the term “no activity” means</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>no data transferred</td>
</tr>
<tr>
<td>TELNET</td>
<td>no keyboard (or mouse) activity</td>
</tr>
<tr>
<td>RLOGIN</td>
<td>no keyboard (or mouse) activity</td>
</tr>
</tbody>
</table>

*User Authentication session timeout* has a different meaning for HTTP. Users of one-time passwords will not have to reauthenticate for each request during this time period. Each successful access resets the timer to zero.

Because each connection requires authentication, VPN-1/FireWall-1 extends the validity of one-time passwords for this period. In this way, users of HTTP do not have to generate a new password and reauthenticate for each connection.

**Authentication Failure Track** — the action to take if authentication fails (applies to all authentication rules)

- **None** — no tracking
- **Log** — Create a log of the authentication action
- **Popup Alert** — Run the *Popup alert* command in the *Global Properties* window, *Log and Alert* page, *Track Options* field.

The tracking for a successful authentication attempt is determined by the *Track* field of the enabling rule. If authentication is successful then:

- If access is allowed, the *Track* specified in the rule which allows the access is applied.
- If access is denied, the *Track* specified in the rule which denies the access is applied.

The fact that a user successfully authenticates does not necessarily mean that there is a rule that allows that user access. For more information, see “The ‘Insufficient Information’ Problem” on page 208.

For example, the rule depicted in FIGURE 3-3 on page 128 specifies logging in Log format. If authentication is successful, and access is allowed by this rule, the Log format is applied. A failed authentication attempt (for example, using an unauthorized password) is tracked according to the entry under *Authentication Failure Track* in the *Authentication* page of the gateway’s *Properties* window.
HTTP Security Server

The HTTP Security Server field in the Authentication tab of the gateway’s Properties window must be defined if it is to be implemented in the current VPN-1/FireWall-1 Firewall Module.

- Use HTTP Next Proxy (Authentication tab) — This specifies the Host name and Port number of the HTTP proxy that is implemented with the HTTP Security Server (if there is one). This option is useful if internal users have defined the HTTP Security Server as the proxy to their Web browsers (see “The HTTP Security Server as an HTTP Proxy” on page 148). The HTTP Security Server does not cache pages used by its client (the browser). If you wish to provide caching for HTTP users, you can implement an HTTP proxy for use with the HTTP Security Server by specifying the host and port of the proxy in the HTTP Next Proxy field in the Security Servers page of the Global Properties window.

Note - If you choose to enable an HTTP proxy along with the HTTP Security Server then both the Host and Port fields are mandatory and must be defined in the Next proxy configuration.

Changing the HTTP Next Proxy fields takes effect after the VPN-1/FireWall-1 database is downloaded to the authenticating gateway, or after the Security Policy is re-installed.

UserAuthority

When the UserAuthority AuthCenter Module is selected in the products installation field of the gateway’s Properties objects tree, the UserAuthority AuthCenter settings button will appear by selecting the Authentication page.
Chaining Options — Specify the UserAuthority Gateways to which to direct queries regarding connection information when that information is not available on this UserAuthority Gateway.

The other UserAuthority Gateways are all queried simultaneously. Priority is given to their replies in the order they are listed below (that is, backup gateways take precedence over VPN tunnels etc.)

- **Redirect connection queries to backup gateways** — If the connection passed through a VPN/FireWall Module that is configured in a MEP cluster with this VPN/FireWall Module, query the UserAuthority Gateway on the other VPN/FireWall Module.

For information about MEP configurations, see “Multiple Entry Point (MEP) Example Configuration” on page 169 of Virtual Private Networking.

- **Redirect connection queries over VPN tunnel** — If the connection passed through a VPN peer, query the UserAuthority Gateway on the VPN peer.
Redirect connection queries to UserAuthority group — If a pre-defined group of UserAuthority Servers has been created IP information can be queried. Create a UserAuthority Server Group from the Network Objects window under New, select Group and then UserAuthority Server Group.

Export Policy — Specify the information that will be exported to external UserAuthority Gateways (that is, VPN peers that are not managed by this SmartCenter Server). There is no restriction on information made available to internal UserAuthority Gateways.

- Export User Name
- Export DN
- Export Authentication Scheme
- Export Source IP Address
- Export User Group

Client Sign On Properties

Allow deriving connection information from Client Sign On — Specify whether to infer connection information from Client Sign On.

Client information is available in the following cases:

- When a SecuRemote Client has exchanged keys with a SecuRemote Server.
When a SecureClient has connected to a Policy Server.
- When Client Authentication has taken place.

Client information is available in these cases even if there is currently no active connection. If Allow deriving connection information from Client Sign On is enabled, then Client information is assumed (during the time period specified by Sign On information expires after), to be valid for all connections originating from the Client.

**Note** - Client information is considered to be less reliable than connection information. For example, a Client’s IP address may be unreliable because NAT took place.

**User Authentication Action Properties**

You must also define the User Authentication properties of the enabling rule. The User Authentication Action Properties window specifies the parameters that apply to an individual rule. You can use this window to restrict user access to and from specific network objects.

To display the User Authentication Action Properties window, double-click on the rule’s Action.

**FIGURE 3-9 User Authentication Action Properties window**

**Source** — Reconcile Source in the rule with the allowed Sources in the Location tab of the User Properties window.

The allowed Sources in the Location tab of the User Properties window may specify that the user to whom this rule is being applied is not allowed access from the source address, while the rule itself may allow access. This field indicates how to resolve this conflict.

- Choose Intersect with User Database to apply the intersection of the access privileges specified in the rule and in the User Properties window.
User Authentication

- Choose **Ignore User Database** to allow access according to the **Source** specified in the rule.

**Destination** — Reconcile **Destination** in the rule with the allowed **Destinations** specified in the **Location** tab of the **User Properties** window.

The **Allowed Destinations** field in the **User Properties** window may specify that the user to whom this rule is being applied is not allowed access to the destination address, while the rule itself may allow access. This field indicates how to resolve this conflict.

- Choose **Intersect with User Database** to apply the intersection of the access privileges specified in the rule and in the **User Properties** window.
- Choose **Ignore User Database** to allow access according to the **Destination** specified in the rule.

**Ignore User Database** allows you to grant access privileges to a user without regard to the user’s IP address. For example, if a user is temporarily away from the office and logging in from a different host, you may wish to allow that user access regardless of the network objects listed under the allowed **Source** specified in the **Location** tab of that user’s **Properties** window (see FIGURE 3-4 on page 129). You can allow the user to work on the local network without extending access privileges to all users on that host.

**HTTP** — This option allows you to restrict access to specific HTTP servers. For more information, see “HTTP Servers (Security Server)” on page 144.
Example

Suppose the **Location** tab of a user's **User Properties** window (FIGURE 3-4 on page 129) lists the network objects **Tower** and **localnet** under **Source**. This means that the user's properties allow access from Tower and localnet. TABLE 3-3 summarizes various access possibilities.

**TABLE 3-3** Access Possibilities

<table>
<thead>
<tr>
<th>rule’s Source allows access from...</th>
<th>Source is “Intersect with User Database”</th>
<th>Source is “Ignore User Database”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tower</td>
<td>The user is allowed access only from <strong>Tower</strong>, because only <strong>Tower</strong> is in both Sources in the <strong>Location</strong> tab and in the rule’s <strong>Source</strong>.</td>
<td>The user is allowed access only from <strong>Tower</strong> because <strong>Tower</strong> is in the rule’s <strong>Source</strong>.</td>
</tr>
<tr>
<td>Thames</td>
<td>The user is denied access, because there is no network object that is in both Sources in the <strong>Location</strong> tab and the rule’s <strong>Source</strong>.</td>
<td>The user is allowed access only from <strong>Thames</strong>, because only <strong>Thames</strong> is in the rule’s <strong>Source</strong>.</td>
</tr>
</tbody>
</table>

**How the User Authenticates**

When a user authenticates, he or she must provide the following information:

- user name on the gateway
- authentication data (password) on the gateway
- user name on the target host
- authentication data (password) on the target host

**Stealth Authentication**

For VPN-1/FireWall-1 Next Generation, unknown users no longer receive an error message indicating that the VPN/FireWall Module does not know the user name on the gateway. VPN-1/Firewall-1 implements stealth authentication, rather, by allowing the connection and then subsequently prompting the user for his or her authentication data (password), thus hiding VPN-1/FireWall-1 from the user. If correct authentication data (password) is not supplied, the connection is dropped.
This user specifies this information using the syntax below.

**To enter user name:**

\[ \text{dst}_{-}\text{user}_{-}\text{name} \ [\text{@auth}_{-}\text{user}_{-}\text{name}] \ @ \text{dst} \]

where:
- \( \text{dst}_{-}\text{user}_{-}\text{name} \) is the user name on the destination host
- \( \text{auth}_{-}\text{user}_{-}\text{name} \) is the user name on the gateway
- \( \text{dst} \) is the name of the destination host

**To enter password:**

\[ \text{dst}_{-}\text{password} \ [\text{@auth}_{-}\text{password}] \]

where:
- \( \text{dst}_{-}\text{password} \) is the password on the destination host
- \( \text{auth}_{-}\text{password} \) is the password on the gateway

This information is entered at the command line or, for FTP and TELNET, using a third-party GUI Client (such as the one in FIGURE 3-10).

**FIGURE 3-10** GUI FTP Authentication

Note: The user will always be prompted for his or her user name even though the authentication data (password) may not be recognized by the VPN-1/Firewall-1 user database.
Parsing the Password String — FTP

For FTP, VPN-1/FireWall-1 parses the password string as follows:

- Whatever is to the left of the last @ is interpreted as the password to the FTP server.
- Whatever is to the right of the last @ is interpreted as the User Authentication password.

For example, if the user types jimb@BigBen.com@secret, then jimb@BigBen.com is the FTP server password, and secret is the VPN-1/FireWall-1 User Authentication password.

This feature is important when using anonymous FTP and entering an email address as the password.

Note: If the user wishes to postpone entering the VPN-1/FireWall-1 User Authentication password, then he or she should type the FTP server password and add @ at the end. The user will be prompted for the VPN-1/FireWall-1 Authentication password later.

Example Configuration - FTP Using O/S Password

In the example configuration depicted in FIGURE 3-2 on page 128, suppose a user in the LocalManagers group requests an FTP session on BigBen, the target server. The session might look something like this:

tower # ftp bigben
Connected to london.
220 london CheckPoint FireWall-1 secure ftp server running on London
Name (bigben:jim): jimb
331-aftpd: FireWall-1 password: you can use password@FW-1-password
Password: <Unix password on bigben>@<FireWall-1 password>
230-aftpd: User jimb authenticated by FireWall-1 authentication.
230-aftpd: Connected to bigben. Logging in...
230-aftpd: 220 bigben ftp server (UNIX(r) System V Release 4.0) ready.
230-aftpd: 331 Password required for jimb.
230-aftpd: 220 User jimb logged in.

The steps involved were as follows:

1. The user requested an FTP session on BigBen, the target server, by typing ftp bigben.

The connection was intercepted by the FTP Security Server on London, the gateway. The Security Server prompted the user for his name on the gateway.
2 The user typed `jimb`, meaning that his user name on the target (BigBen) is jimb and his user name on the gateway is jimb.

3 The FTP Security Server challenged the user for his VPN-1/FireWall-1 password, in accordance with the authentication scheme specified for the user in the Authentication tab of the User Properties window.

4 The user correctly entered his VPN-1/FireWall-1 password and was connected to BigBen, the target server.

The FTP Security Server on London supplied FTP on BigBen with the user’s password, so the user did not have to enter it again.

**Non-Transparent User Authentication**

In This Section

- Non-Transparent User Authentication — Example page 140
- Enabling Non-Transparent User Authentication page 141

Non-transparent User Authentication can be implemented for user authenticated services (FTP, HTTP, RLOGIN, TELNET). Under Non-transparent User Authentication, a user working with one of these services must first start a session for that service on the gateway. After successful authentication, VPN-1/FireWall-1 opens a connection to the “true” destination. This method is known as non-transparent because the user does not directly request the target host, but must explicitly connect the gateway first.

**Note** - Transparent User Authentication is the default action for VPN-1/FireWall-1 Version NG FP1.

**Non-Transparent User Authentication — Example**

Consider the following network configuration.
In the above configuration, the user who wants to begin a TELNET session on Big Ben must first TELNET to London (the gateway) where the VPN-1/FireWall-1 TELNET Security Server is installed on the TELNET port in place of the standard TELNET daemon. The user must then specify BigBen as the ultimate destination. The VPN-1/FireWall-1 TELNET Security Server authenticates the user, and if the authentication is successful, opens a connection to BigBen, the “true” destination.

The user must provide the following information:

- user name on the gateway
- authentication data (password) on the gateway
- name of the target host — this is the major difference between Transparent and Non-transparent Authentication
- user name on the target host
- authentication data (password) on the target host

**Enabling Non-Transparent User Authentication**

Non-transparent user authentication is controlled by the `prompt_for_destination` parameter in the file `objects_5.0.C`.

The `prompt_for_destination` parameter determines what to do when the user connects directly to the VPN/FireWall Module. In this case, there are two possibilities:

- prompt_for_destination is false

This is the default value for VPN-1/FireWall-1 Version 3.0 and higher. If `prompt_for_destination` is false, VPN-1/FireWall-1 implements Transparent User Authentication. The VPN/FireWall Module assumes the user’s “true” destination is the FireWalled machine, and does not prompt the user for the “true” destination.

- prompt_for_destination is true
If \texttt{prompt\_for\_destination} is true, VPN-1/FireWall-1 implements non-Transparent User Authentication. If the user requests the gateway as the destination, the VPN/FireWall Module assumes the user’s “true” destination is some other server, and prompts the user for the “true” destination.

Non-transparent User Authentication will be implemented only if the user first requests the gateway. If the user requests a host behind the gateway, VPN-1/FireWall-1 will implement Non-transparent authentication, regardless of the setting for \texttt{prompt\_for\_destination}.

\textbf{Note} - The \texttt{objects\_5\_0.C} file should not be edited directly. Instead, use \texttt{dbedit} (see Chapter 18, "Command Line Interface" of \textit{Check Point SmartCenter Guide}) to edit the \texttt{objects\_5\_0.C} file on the SmartCenter Server.

\textbf{Note} - After making changes to \texttt{objects\_5\_0.C}, you must download the database from the SmartCenter Server to the VPN/Firewall Module in order for the changes to take effect. For more information, see, “\texttt{fwm dbload}” on page 564 of \textit{Check Point SmartCenter Guide}.

\section*{User Authentication and the HTTP Security Server -}

\begin{itemize}
  \item \textit{HTTP Security Server — Overview} \hfill page 142
  \item \textit{HTTP Security Server — Configuration} \hfill page 143
  \item \textit{HTTP Security Server — User Authentication Rules} \hfill page 146
  \item \textit{HTTP Security Server — Proxy Mode} \hfill page 147
  \item \textit{HTTP Security Server — When the User Connects} \hfill page 151
  \item \textit{HTTP Security Server — Security Considerations} \hfill page 154
  \item \textit{HTTP Security Server — Non-Transparent Authentication} \hfill page 154
\end{itemize}

\section*{HTTP Security Server — Overview}

The VPN-1/FireWall-1 HTTP Security Server provides a mechanism for authenticating users of HTTP services. An HTTP Security Server on the gateway can protect any number of HTTP servers behind the gateway, and authenticate users accessing HTTP or HTTPS (HTTP encrypted by SSL).

The HTTP Security Server is invoked when a rule’s action specifies \texttt{User Authentication}. The rule’s \texttt{Service} can specify either the HTTP service or a Resource. This section describes the behavior of the HTTP Security Server for User Authentication rules. For more information on how the HTTP Security Server handles Resources, see Chapter 4, “Security Servers and Content Security”.

142 \hspace{1cm} Check Point FireWall-1 • September 2002
HTTP Security Server Configuration

HTTP Security Server parameters are defined by navigating from the FireWall-1 objects tree in the **Global Properties** window to **Authentication and Security Server**.

**FIGURE 3-12** Global Properties window — Authentication and Security Server pages

The fields relating to the HTTP Security Server are explained below.

- **User Authentication: Session timeout** *(Authentication page)* — For HTTP, this applies to one-time passwords only. Users of one-time passwords do not have to reauthenticate during this time period. The HTTP Security Server extends the validity of a one-time password for this time period so the user does not have to generate a new password and reauthenticate for each connection. Each successful access resets the timer to zero. For more information, see “HTTP Security Server — Security Considerations” on page 154.

- **HTTP Next Proxy** *(Security Server page)* — This specifies the **Host** name and **Port** number of the HTTP proxy behind the HTTP Security Server (if there is one). This specific field is applicable to Modules whose versions are prior to Version NG FP1. This field allows for backward compatibility with previous versions.
This option is useful if internal users have defined the HTTP Security Server as the proxy to their Web browsers (see “The HTTP Security Server as an HTTP Proxy” on page 148). The HTTP Security Server does not cache pages used by its client (the browser). If you wish to provide caching for HTTP users, you can put an HTTP proxy behind the HTTP Security Server.

Changing the HTTP Next Proxy fields takes effect after the VPN-1/FireWall-1 database is downloaded to the authenticating gateway, or after the Security Policy is re-installed.

HTTP Servers (Security Server)

The HTTP Servers list in Security Server page of the Global Properties window specifies the host names and port numbers of HTTP servers.

Defining HTTP servers allows you to restrict incoming HTTP. You can control access to specific ports on specific hosts. You can also specify whether users must reauthenticate when accessing a specific server.

If you are implementing Non-transparent authentication, then the HTTP Servers list provides a list of hosts and port numbers to which the HTTP Security Server can direct connections from the gateway. For more information, see “HTTP Security Server and Non-Transparent Authentication” on page 154.

If you change the location of an HTTP server (i.e., you install it on a new host or port), you must update the HTTP Servers list. For more information, see “Controlling Access to HTTP — User Authentication Rules” on page 146.

Configuring HTTP Servers

To add a new server, click on New. The HTTP Server Definition window (FIGURE 3-13) is then displayed.

To delete a server from the list, select it and click on Remove. More than one server can be selected at a time.

To modify a server’s host or port number, click on the server’s logical name in the HTTP Servers list and click on Edit. The server’s details are then displayed in the HTTP Server Definition window (FIGURE 3-13).

HTTP Server Definition window

This window defines an HTTP server.
The fields in the **HTTP Server Definition** window are explained below:

- **Logical Name** — the server's logical name
- **Host** — the host on which the server runs
- **Port** — the port number on the host
- **Server For Null Requests** — this option is relevant only if Non-transparent authentication is enabled. For more information, see “Configuring a Server for Null Requests” on page 160.

**Reauthentication Options**

Reauthentication options define whether a user must reauthenticate every time the HTTP server is accessed. Reauthentication options apply only when **Predefined Servers** is specified under **HTTP** in a rule’s **User Authentication Action Properties** window (FIGURE 3-9 on page 135).

Select one of the following options:

- **Standard Authentication** — The user will not be required to enter a password again during the authorization period (as specified in the **Session Timeout** field in the **Authentication** page of the **Global Properties** window). Each successful access resets the timer to zero.

- **Reauthentication for POST Requests** — Every request sent by the client which may change the server's configuration or data requires the user to enter a new password.

  If the password is not a one-time password, this option has no effect.

- **Reauthentication for Every Request** — Every request for a connection requires the user to enter a new password.

  If the password is not a one-time password, this option has no effect.

This option is useful when access to some pages must be severely restricted. It is recommended that pages such as these be handled by a separate server.
User Authentication

The Reauthentication status of each HTTP Server is displayed under Reauthentication in the HTTP Servers list.

Controlling Access to HTTP — User Authentication Rules

Restricting Incoming HTTP

If you wish to restrict access to internal HTTP services by external users, proceed as follows:

1 Define a rule similar to the following:

<table>
<thead>
<tr>
<th>NO</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
<th>INSTALL ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>All Users Any</td>
<td>Local Net</td>
<td>HTTP</td>
<td>User Auth</td>
<td>Log</td>
<td>Gateways</td>
</tr>
</tbody>
</table>

The above rule requires external users to authenticate before accessing HTTP services in the local network. Incoming HTTP is intercepted by the HTTP Security Server on the gateway.

2 In the rule’s User Authentication Action Properties window (FIGURE 3-9 on page 135), choose Predefined Servers under HTTP.

This restricts external access to the HTTP servers listed in the Security Server page of the Global Properties window. This will also activate the Reauthentication options specified for the HTTP servers. For more information, see “HTTP Servers (Security Server)” on page 144.

Restricting Internal Users’ Access to External HTTP

To restrict internal users’ access to external HTTP, proceed as follows.

1 Define a rule similar to the following:

<table>
<thead>
<tr>
<th>NO</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
<th>INSTALL ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>All Users Any</td>
<td>Any</td>
<td>HTTP</td>
<td>User Auth</td>
<td>Log</td>
<td>Gateways</td>
</tr>
</tbody>
</table>

This rule allows internal users to use external HTTP if they first authenticate themselves on the gateway.

2 In the rule’s User Authentication Action Properties window (FIGURE 3-9 on page 135), choose All Servers from the HTTP options. This allows the connection to continue on to any port.

If All Servers is chosen, then the options defined in the HTTP Server window for predefined servers are ignored.
Define another rule as follows:

This rule prevents the use of HTTP without User Authentication on the gateway.

### Restricting Incoming and Outgoing HTTP

Assume the following Rule Base:

<table>
<thead>
<tr>
<th>NO</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
<th>INSTALL ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
<td>http</td>
<td>Login</td>
<td>Log</td>
<td>Gateway</td>
</tr>
</tbody>
</table>

The first rule requires users of incoming HTTP to authenticate before accessing internal HTTP servers defined in the HTTP servers window (FIGURE 3-13 on page 145).

The second rule applies to internal users accessing external HTTP. According to the second rule, internal users must be authenticated before accessing external HTTP.

### The HTTP Security Server in Proxy Mode

For internal users, the behavior of the HTTP Security Server also depends on whether it is defined as the proxy to the users’ Web browser (in the browser’s proxy settings). There are two different proxy settings. Each setting has specific advantages and implications for local users.

- **HTTP proxy**
  
The HTTP Security Server can be defined as the HTTP proxy to the user’s Web browser. This provides several advantages regarding entering user passwords and managing authentication. For more information, see “The HTTP Security Server as an HTTP Proxy” on page 148.

- **Security proxy**
  
The HTTP Security Server can be defined as the Security Proxy to the user’s Web browser. The HTTP Security Server proxies HTTPS (HTTP encrypted by SSL) connections. Although it does not inspect content of HTTPS connections, the...
administrator can provide security by specifying User Authentication for outgoing HTTPS. For more information, see “HTTP Security Server as a Security Proxy — Authenticating Outgoing HTTPS” on page 149.

Note - Proxy settings are not mutually exclusive and can be used together.

The HTTP Security Server as an HTTP Proxy

Internal users can define the HTTP Security Server as the HTTP proxy to their Web browsers. The HTTP Security Server is defined as an HTTP proxy in the proxy settings of the user's Web browser.

Note - The VPN-1/FireWall-1 HTTP Security Server will only handle proxy requests for authenticated HTTP connections and resources. If you do not use authentication or resources, you cannot use the VPN-1/FireWall-1 HTTP Security Server as an HTTP proxy.

FIGURE 3-14 shows the proxy settings window for Netscape 4.7.

FIGURE 3-14 Defining the gateway as the HTTP proxy — Netscape 4.7

Defining the HTTP Security Server as a proxy offers several advantages:
- You can centralize Authentication information to one location, the VPN-1/FireWall-1 machine.
When defined as the HTTP proxy, the HTTP Security Server can handle FTP requests through a Web browser. For more information, see “HTTP Security Server” on page 217.

When a local user requests a URL in the Web browser, the browser sends the entire URL path to the HTTP Security Server. When the HTTP Security Server is not defined as a proxy, it only receives the name of the requested server from the Web browser. This means HTTP Security Server must retrieve the entire URL.

All outgoing HTTP connections are mediated by the HTTP Security Server.

HTTP in proxy mode supports multiple connections to the HTTP Security Server across the network. This feature allows the Client to request multiple connections to HTTP Security Servers for multiple and simultaneous downloads from several HTTP Web Servers.

In addition, the HTTP Security Server offers several advantages over other Authentication Servers.

- VPN-1/FireWall-1 supports S/Key, SecurID, RADIUS, TACACS and AXENT Defender authentication.
- VPN-1/FireWall-1 supports restriction by day of week and/or time of day.
- VPN-1/FireWall-1 can automatically expire a user according to the Expiration Date specified in the General tab of the User Properties window.

Note: Although it is defined as the HTTP proxy to the Web browser, the HTTP Security Server is not an official HTTP proxy, that is, it does not relay HTTP traffic in the way that, for example, the CERN HTTP proxy does. It is not an independent application that runs outside of FireWall.

HTTP Security Server as a Security Proxy — Authenticating Outgoing HTTPS

HTTPS (HTTP encrypted by SSL) connections can be handled by the HTTP Security Server when it is defined as the Security Proxy to the local user’s Web browser. The HTTP Security Server proxies outgoing HTTPS connections, but does not inspect content. This option is used to authenticate internal users accessing external HTTPS.

The user can configure a Security Proxy for the following Web browsers:

- Internet Explorer version 3.0x and higher
- Netscape version 4.0x and higher

For details, see “Security Proxy Mode” on page 219 of Chapter 4, “Security Servers and Content Security.”
Authenticating Internal Users Accessing External HTTPS (Security Proxy Mode)

To authenticate users of outgoing HTTPS, proceed as follows:

1. Internal users must define the HTTP Security Server as the Security Proxy on port 443. This is done in the proxy settings of the user’s Web browser. For more information, see “Security Proxy Mode” on page 219 of Chapter 4, “Security Servers and Content Security.”

2. Add the following line to the file $FWDIR/conf/fwauthd.conf:

   ```
   443 fwssd bin/in.ahttpd wait 0
   ```

   This enables the HTTP Security Server to run on the port specified for the Security Proxy.

3. In the HTTPS service properties, set the **Protocol Type** to **URI** (FIGURE 3-15). This assures that the HTTPS service (using port 443) will be mediated by the HTTP Security Server.

4. Define a rule similar to the following:

<table>
<thead>
<tr>
<th>NO.</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
<th>INSTALL ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>All Users@Local</td>
<td>Any</td>
<td>HTTPS</td>
<td>User Auth</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   According to this rule, internal users must authenticate before accessing external HTTPS.
In the rule’s **User Authentication Action Properties** window, check **All Servers** under **HTTP**.

This assures that the outgoing connections will be allowed to continue from the HTTP Security Server to any external host or port.

**Tip** - You can also configure the HTTP Security Server to encrypt and decrypt HTTPS connections on the gateway. For more information, see “Support For HTTPS — Controlling External Access to Internal HTTPS” on page 155.

**HTTP Security Server — When the User Connects**

**Password Prompt**

When a user is intercepted by the HTTP Security Server, a password prompt window is displayed in which the user is asked to enter a user id and a password. The format of the window depends on the HTTP browser in use, since it is the browser that displays the window, not VPN-1/FireWall-1. However, some of the data displayed in the window is supplied to the browser by the HTTP Security Server.

![FIGURE 3-16 A Typical User ID and Password Window](image)

The information given in the password prompt window usually includes:

- the Authentication scheme required by VPN-1/FireWall-1
- whether Authentication is required for the HTTP server, and if so, the server’s realm name
- an “error” message giving the reason for the last Authentication failure

**Multiple Users and Passwords**

This applies only when the HTTP Security Server is not being used as a user’s Web proxy. This is relevant for external users accessing internal HTTP, and internal users who have not defined the HTTP Security Server as a proxy.

In HTTP, the Web browser automatically supplies the user’s password to the server once the user authenticates. If the user requests another server, the browser cannot send the password to the new server, and the user must reauthenticate.
The user can specify different user names (and passwords) at the password prompt for the HTTP server and VPN-1/FireWall-1, as follows:

\[ \text{server\_username@VPN-1/FireWall-1\_username} \]

In the same way, the user can enter two passwords, as follows:

\[ \text{server\_password@VPN-1/FireWall-1\_password} \]

If there is no password for the server, only the VPN-1/FireWall-1 password should be entered.

If the user enters one user name and two passwords, the same user name is used for both the HTTP server and VPN-1/FireWall-1, but the different passwords are used as indicated.

If @ is part of the password, the user should type it twice (for example if the password is \texttt{mary@home}, type \texttt{mary@@home}).

**Error Messages**

Authentication attempts may be denied for any of the following reasons. The browser displays these messages in the password prompt.

**TABLE 3-4** HTTP Security Server error messages

<table>
<thead>
<tr>
<th>error</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>no user</td>
<td>No user id was entered.</td>
</tr>
<tr>
<td>no password</td>
<td>No password was entered.</td>
</tr>
<tr>
<td>wrong password</td>
<td>The OS or VPN-1/FireWall-1 password was incorrect.</td>
</tr>
<tr>
<td>S/Key</td>
<td>S/Key authentication failed.</td>
</tr>
<tr>
<td>SecurID</td>
<td>SecurID authentication failed.</td>
</tr>
<tr>
<td>WWW server</td>
<td>The VPN-1/FireWall-1 password was correct, but the server did not authorize the user (probably because the server password was incorrect).</td>
</tr>
<tr>
<td>user limitations</td>
<td>The user is not authorized for the given day of week, time of day, source or destination, or the user has expired.</td>
</tr>
<tr>
<td>FW-1 rule</td>
<td>The VPN-1/FireWall-1 password was correct, but the user was not authorized because there was no matching rule in the Rule Base.</td>
</tr>
</tbody>
</table>
These messages may be customized by editing the .cpsc file in the $FWDIR/conf directory. (For more complete information, see “Customizing Security Server Messages” on page 225.) In addition to error messages, additional messages may be displayed by the browser.

### TABLE 3-5 Browser Messages

<table>
<thead>
<tr>
<th>message</th>
<th>meaning and/or corrective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed to connect to the WWW server</td>
<td>Notify your system manager.</td>
</tr>
<tr>
<td>Unknown WWW server</td>
<td>VPN-1/FireWall-1 could not determine to which server the URL should be sent. This can happen for two reasons: The URL is incorrect, or there is a resolution problem.</td>
</tr>
<tr>
<td>Authentication Services are unavailable</td>
<td>Notify your system manager.</td>
</tr>
<tr>
<td>VPN-1/FireWall-1 is currently busy - try again later</td>
<td>Wait and try again. If the problem persists, notify your system manager.</td>
</tr>
<tr>
<td>Simple requests (HTTP 0.9) are not supported</td>
<td>HTTP 0.9 clients are not supported by the VPN-1/FireWall-1 HTTP Security Server. Note that HTTP 0.9 servers are supported.</td>
</tr>
</tbody>
</table>

Additional messages may be displayed if VPN-1/FireWall-1 encounters an error, such as no OS password defined for a user who is required to supply a OS password, or problems with SecurID server etc. In the event one of these messages is encountered, the user should notify the system administrator.

### Differences Between Clients

Some clients do not display authorization information in the password prompt window, or display only some of the information.

When using such a client, the user can sometimes view the missing information by clicking on **Cancel** (to view the information) and then **Reload** (to display the password prompt window again), or by performing the equivalent functions.
If the password prompt window does not display what kind of password must be entered (this can happen if the user name is unknown), the user should enter the user name without the password and click on **OK**. If the client requires a non-empty password, the user should type a single space. The window will be displayed again, including the password type.

**HTTP Security Server — Security Considerations**

In HTTP, the Web browser automatically supplies the password to the server for each connection. This creates special security considerations when using the HTTP Security Server with one-time passwords.

To avoid forcing users of one-time passwords to generate a new password for each connection, the HTTP Security Server extends the validity of the password for the time period defined in **Session timeout** in the **Authentication** menu of the **Global Properties** window. Users of one-time passwords do not have to reauthenticate for each request during this time period.

Each successful access resets the timer to zero. Because the authorization period is renewable, and the Web browser keeps supplying the password, the time period during which a one-time password can be used can be unlimited.

This problem can be solved by using the Reauthentication options in the HTTP Server definition (“HTTP Servers (Security Server)” on page 144). For example, you can specify that every request to a specific HTTP server requires a new password, or that requests that change a server’s configuration require a new password. For more information, see “HTTP Servers (Security Server)” on page 144.

**HTTP Security Server and Non-Transparent Authentication**

This section describes how the HTTP Security Server is configured when implementing Non-transparent Authentication. In Non-transparent Authentication, the user must explicitly connect to the VPN/FireWall Module in order to authenticate before continuing to the target host. For an overview see “Non-Transparent User Authentication” on page 140.

If you are implementing Non-transparent Authentication, the HTTP Security Server can be configured to encrypt and decrypt HTTPS connections. This option enables the HTTP Security Server to inspect the contents of HTTPS connections.

The connection can be encrypted between the client and the HTTP Security Server, and then possibly again from the HTTP Security Server to the target server. For example, you can specify that connections between the client and HTTP Security Server are encrypted. The HTTP Security Server on the gateway decrypts and inspects the connection. The connection can then be encrypted again from the HTTP Security Server to the target host. The authentication session is encrypted as well.
Because the HTTP Security Server is not defined as a Security Proxy to the user’s Web browser, Non-transparent Mode is best used to authenticate external users accessing internal servers. For information on putting an existing HTTP server behind the HTTP Security Server, see “Putting Existing HTTP Servers Behind the HTTP Security Server” on page 160.

**Support For HTTPS — Controlling External Access to Internal HTTPS**

To configure support for HTTPS for NG modules of VPN-1/FireWall-1, proceed as follows:

1. In the `objects_5_0.C` file, set the `prompt_for_destination` parameter to `true`.

2. The Certificate Key on the SmartCenter Server must be generated and distributed to the VPN-1/FireWall-1 Module. For complete instructions, see “Secure Internal Communication” on page 90 in the book, *Check Point Getting Started Guide*. This should have occurred during installation.

   **Note** - The certificate exchange should have occurred during the installation process. Trust between the Module and the SmartCenter Server should already have been established, and the modules should be able to communicate, if installation was successful.

**Modifying the Security Server Configuration File**

3. Next modify the file `$FWDIR/conf/fwauthd.conf` by adding a line which enables the HTTP Security Server to run on an additional service port dedicated to HTTPS. According to the example below, HTTPS connections will connect to the gateway on port 443.

   For example:

   ```
   443 fwssd in.ahttpd wait 0 ec: certificate name
   ```

   The last field specifies what to do with HTTPS (SSL) connections. TABLE 3–6 lists the available options:

**TABLE 3–6 HTTPS options**

<table>
<thead>
<tr>
<th>option</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ec</td>
<td>encrypt connections between the client and the gateway</td>
</tr>
</tbody>
</table>
Leaving this field empty is the same as specifying `ns`.

For more information about the file `FWDIR/conf/fwauthd.conf`, see “Security Server Configuration” on page 237.

To configure support for HTTPS for earlier version modules of VPN-1/FireWall-1, proceed as follows:

1. In the `objects_5_0.C` file, set the `prompt_for_destination` parameter to `true`.
   
   This value indicates that if the user requests the gateway as the destination, the
   VPN/FireWall Module assumes the user’s “true” destination is some other server, and
   prompts the user for the “true” destination.

2. Generate the CA Key for the SmartCenter Server using the `fw ca genkey` command. This command is entered on the SmartCenter Server as follows:

   ```
   fw ca genkey DN
   ```

   `DN` is the Distinguished Name of the Certificate Authority. The following shows the `fw ca genkey` command with the DN of an example Certificate Authority:

   ```
   fw ca genkey ou=research,o=widgetcorp,c=us
   ```

   where `ou` is the organizational unit, `o` is the organization, and `c` is the country of the
   Certificate Authority.

3. Distribute the CA Key to the VPN/FireWall Module using the `fw ca putkey` command. This command is entered on the SmartCenter Server as follows: `target`

   ```
   fw ca putkey [-p password] target
   ```

   is the IP address or resolvable name of the machine on which you are installing the
   CA key (the VPN/FireWall Module).

### Table 3-6 HTTPS options

<table>
<thead>
<tr>
<th>option</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>es</code></td>
<td>encrypt connections between the gateway and the server</td>
</tr>
<tr>
<td><code>eb</code></td>
<td>encrypt both — encrypt connections between the client and the gateway, and then between the gateway and the server.</td>
</tr>
<tr>
<td><code>ns</code></td>
<td>no SSL (no encryption)</td>
</tr>
</tbody>
</table>

| TABLE 3-6 HTTPS options |
password will be used to authenticate future communication between the SmartCenter Server and the gateway. The password can be entered on the command line (using the -p argument). If you do not enter a password on the command line, you will be prompted for one.

4. On the VPN/FireWall Module, generate a Certificate. You must enter the following command on the VPN/FireWall Module:

```
fw certify ssl management target
```

management is the IP address or resolvable name of the VPN/FireWall Module’s SmartCenter Server. target is the IP address or resolvable name of the machine on which you are installing the CA key.

You will be prompted for a password. You must enter the same password you used when you issued the `fw ca putkey` Command on the SmartCenter Server in step 3.

**Modifying the Security Server Configuration File for earlier version modules of VPN-1/FireWall-1**

5. Next modify the file `$FWDIR/conf/fwauthd.conf` by adding a line which enables the HTTP Security Server to run on an additional service port dedicated to HTTPS. According to the example below, HTTPS connections will connect to the gateway on port 443.

For example:

```
443 fwssd bin/in.ahttpd wait 0 ec
```

Refer to TABLE 2-6, “HTTPS options” on page 155 for a list of HTTPS options.

**HTTP Servers**

6. Define the HTTP servers to which HTTPS connections are allowed.

HTTP servers are defined in the **HTTP Server Definition** window (FIGURE 3-17). For information on defining HTTP servers, see “HTTP Servers (Security Server)” on page 144.
You must specify the **Logical Name**, **Host** and **Port** number on which you installed the servers which will handle HTTPS connections.

**HTTPS Service Properties**

7 Modify HTTPS properties to assure that the service will be mediated by the HTTP Security Server. In the HTTPS service definition, set the **Protocol Type** to **HTTP** (see FIGURE 3-15 on page 150).

**User Authentication Rule**

8 Next, define a rule similar to the following:

<table>
<thead>
<tr>
<th>NO</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
<th>INSTALL ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>All Users/Group</td>
<td>Tower</td>
<td>HTTP</td>
<td>User Auth</td>
<td>Log</td>
<td>Gateway</td>
</tr>
</tbody>
</table>

In the rule’s **User Authentication Action Properties** window, specify **Predefined Servers** under **HTTP**. This restricts incoming HTTPS to the servers listed in the **Security Server** page of the **Global Properties** window (the HTTP Servers you defined in step 6 on page 157).

**How the User Connects**

An external user of HTTP must specify the name of the VPN/FireWall Module and the logical name of the target server in the requested URL. This assures that the request will be intercepted by the HTTP Security Server on the gateway. The URL is set up as follows:

```
https://<gateway_name>/<logical_server_name>/...
```

For example, if the gateway name is London, and the target server (behind London) is Tower, then the user specifies the following URL:

```
https://www.london.com/tower/...
```
For information on how to set up URLs for Non-transparent Authentication, see "Configuring URLs" below.

**Configuring URLs**

Suppose that in the configuration depicted in FIGURE 3-18 on page 159, there are HTTP servers on all the hosts (Tower, Palace, and BigBen) which are protected by an HTTP Security Server on the gateway London.

The URLs should be set up as follows:

```
http://gateway/logical server name/...
```

where the ellipsis (...) indicates the part of the URL that the server receives and parses. This is usually a file name.

For example, assume HTTP servers running on London-net, as listed in FIGURE 3-18.

![HTTP Servers behind a VPN/FireWall Module](image)

**TABLE 3-7 Servers and URLs**

<table>
<thead>
<tr>
<th>server name</th>
<th>URL</th>
<th>host</th>
<th>port</th>
</tr>
</thead>
<tbody>
<tr>
<td>info</td>
<td><a href="http://www.London.com/info/info.html">http://www.London.com/info/info.html</a></td>
<td>BigBen</td>
<td>80</td>
</tr>
<tr>
<td>reviews</td>
<td><a href="http://www.London.com/reviews/clips.html">http://www.London.com/reviews/clips.html</a></td>
<td>Tower</td>
<td>8080</td>
</tr>
</tbody>
</table>

In this case, the gateway is www.London.com and the server names are those specified under **HTTP Servers** in the **Security Server** page of the **Global Properties** window (see FIGURE 3-12 on page 143), where the connection between the server name and the host and port is defined. The only externally known name is www.London.com.
A user who wishes to access the HTTP server “actors” on the host Tower, must specify a URL of http://www.London.com/actors/bios.html (where bios.html is a specific page maintained by the server). The connection is intercepted by the HTTP Security Server on the gateway London.

**Configuring a Server for Null Requests**

A Server for Null Requests is used when the URL is of the form http://gateway/ or http://gateway. In this case, the URL passed to the server is “/”. In Non-Transparent Authentication, this allows a user to connect to the gateway without having to specify the name of a target server behind the gateway. The Server for Null Requests is defined using the **HTTP Server Definition** window (FIGURE 3-19).

![FIGURE 3-19 HTTP Server Definition — Server for Null Requests](image)

For example, a user connects to London, the VPN/FireWall Module, as follows:

http://www.london.com

If you have specified an HTTP server as a **Server for Null Requests** and checked **Predefined Servers** in the **User Authentication Action Properties** window of the relevant rule, the HTTP Security Server on the gateway directs the connection to the Server for Null Requests.

You can configure this server to display a Web page with links to internal servers. This server then provides an “entry point” to other internal servers. In this way, the user does not have to know the names of the target servers behind the gateway. All the user needs to know is the name of the VPN/FireWall Module.

**Putting Existing HTTP Servers Behind the HTTP Security Server**

This section applies to users who wish to implement Non-transparent authentication.

To put an existing HTTP server behind the HTTP Security Server, proceed as follows:
If you have only one HTTP server, and it is on your gateway

1. Replace the HTTP server with the HTTP Security Server.

2. Put the HTTP server elsewhere.

3. For security reasons, it is recommended that you put the HTTP server on a different computer. However, you can also put it on a different port on the same computer.

4. Update the HTTP Servers list in the Security Server page of the Global Properties window in accordance with where you put the HTTP server (see previous step).

If you have only one HTTP server, and it is NOT on your gateway

1. Arrange for the server address to be directed to the HTTP Security Server (host name) on the gateway.

   This is done outside of VPN-1/FireWall-1, either by publicizing the new address for the existing host name, or by creating a new host name and notifying your authorized users.

2. Add the server to the list of HTTP servers in the HTTP field of the Security Server page.

   Even if there is only one server behind VPN-1/FireWall-1, you should still give it a name and add it to the HTTP server list in the HTTP field of the Security Servers page (see “HTTP Servers (Security Server)” on page 144). However, the server name may be omitted from the URLs that refer to it (if there is only one server), so there is no need to change URLs when putting a single server behind VPN-1/FireWall-1 if the host name for the FireWall and the server are the same.

If you have more than one HTTP server

1. Arrange for the server address to be directed to the HTTP Security Server (host name) on the gateway.
This is done outside of VPN-1/FireWall-1, either by publicizing the new addresses for the existing host name, or by creating a new host name and notifying your authorized users.

Add the servers to the list of HTTP servers in the HTTP field of the Security Servers page.

Modify all the HTML source code so that absolute references point to the appropriate servers.

This step is necessary for Non-transparent Authentication only.

The first field of an absolute URL should be replaced by "gateway/logical server name/".

It is not necessary to modify relative references.

**Session Authentication**

In This Section

- Session Authentication — Overview
- Session Authentication — Deployment

**Session Authentication — Overview**

Session Authentication can be used to authenticate users of any service. FIGURE 3-20 shows what happens when a rule's Action specifies Session Authentication.

The Session Authentication process is as follows:

1. The user initiates a connection directly to the server.
2. The VPN-1/FireWall-1 Inspection Module intercepts the connection. The Inspection Module connects to a Session Authentication Agent on the client. In the above configuration, the Session Authentication Agent is running on the client, but it can run on another machine (on any of the supported platforms).
The Session Authentication Agent prompts the user for authentication data and returns this information to the Inspection Module.

If the authentication is successful, then the VPN/FireWall module allows the connection to pass through the gateway and continue on to the target server.

In contrast to User Authentication, Session Authentication does not result in an additional connection to the server. The advantage of Session Authentication is that it can be used for every service. It requires a Session Authentication Agent which prompts the user through a series of pop-up screens.

The Session Authentication Agent is an application that communicates with the VPN/FireWall Module using the VPN-1/FireWall-1 Session Authentication Agent Protocol. The Session Authentication Agent can be running on the following network objects:

- the source of the connection (i.e., the client that initiated the connection)
- the destination of the connection
- a specific host
Session Authentication — Deployment

This section describes a deployment example for Session Authentication. This example consists of the following:

- an example network configuration
- what the Security Administrator must define in the VPN-1/FireWall-1 Rule Base
- what the user must do to authenticate

This example is not intended as a set of step by step instructions, but rather to illustrate how and where different components of Session Authentication are configured in the VPN-1/FireWall-1 GUI.

Example Configuration

In the configuration depicted in (FIGURE 3-22), all localnet users must be authenticated before accessing the Internet.

**FIGURE 3-22** Example configuration

The following rule allows users of any service external access after successful Session Authentication.

**FIGURE 3-23** Example Session Authentication Rule

<table>
<thead>
<tr>
<th>NO</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
<th>INSTALL ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><em>AllUsers</em></td>
<td>Any</td>
<td>Any</td>
<td>Session Auth</td>
<td>Log</td>
<td>All</td>
</tr>
</tbody>
</table>

Defining Session Authentication

To enable Session Authentication for this configuration, you must do the following:

- install and configure the Session Authentication Agent
- pre-configure the Session Authentication Agent for distribution to multiple users, if desired
- configure Session Authentication for encryption, if desired
- define Session Authentication action properties
• define logging and tracking

Installing and Configuring the Session Authentication Agent

Windows

To install the Session Authentication agent for Windows, run the setup program in the DESKTOP PRODUCTS\SESSIONAGENT directory on the CD-ROM.

Opening the Session Authentication Agent

To open the Session Authentication agent, double-click on its icon in the system tray. The FireWall-1 Session Authentication window (FIGURE 3-24) is displayed.

FIGURE 3-24 VPN-1/FireWall-1 Session Authentication window

Perform one of the following:

• To terminate the Session Authentication agent, click on Yes.
• To configure the Session Authentication agent, click on Configure.
• To close the FireWall-1 Session Authentication window, click on No.

Configuration

When you click on Configure in the Session Authentication window, the Configuration window (FIGURE 3-25) is displayed.
The **Configuration** window has three tabs, explained below.

**Passwords Tab**

The **Passwords** tab of the **Configuration** window enables you to specify how frequently the user is asked to supply a password (that is, to authenticate himself or herself). One-time passwords (such as SecurID) cannot be cached.

Check one of the available choices:

- **Every request** — The user will be prompted for the password each time the VPN/FireWall Module requests authentication.
  
  Each time the user initiates a session to which a Session Authentication rule applies, the user will be prompted for a password. In this case, no password caching occurs.

- **Once per session** — The user will be prompted for a password once per Session Authentication agent session.
  
  In this case, the user supplies the password once and the Session Authentication agent caches the password indefinitely. This option cannot be used with one-time passwords.

  If the Session Authentication agent is terminated and then re-started, the user will have to supply the password again.

- **After ... minutes of inactivity** — This option is the same as **Once per session**, except that the user will be prompted again for a password if there has been no authentication request for the specified time interval.
Allowed FireWall-1 Tab

The **Allowed FireWall-1** tab of the **Configuration** window enables you to specify the VPN/FireWall Modules for which this Session Authentication agent may provide authentication services.

**Any IP Address** — This Session Authentication agent may provide authentication services for any VPN/FireWall Module.

**IP Address** — This Session Authentication agent may provide authentication services only for a VPN/FireWall Module running on the specified IP address.

You can specify up to three IP addresses.

Options Tab

The **Options** tab of the **Configuration** window (FIGURE 3-27) enables you to specify whether to allow clear passwords and resolve addresses.
Pre-configuration

The PRODUCT.INI file in the DESKTOP PRODUCTS\SESSIONAGENT directory enables you to pre-configure the Session Authentication agent. This feature is useful if you plan to distribute the Session Authentication agent to many users and you do not want them to configure the agent themselves.

The file is in the standard .INI format. It is divided into sections, each of which consists of a list of parameters and their values (FIGURE 3-28).

```
[Startup]
AppName=CheckPoint Session Authentication NG
FreeDiskSpace=0
EnableDlg=Y

[ISUPDATE]
UpdateURL=

[Languages]
Default=0x0009
count=1
key0=0x0009
```

FIGURE 3-28 PRODUCT.INI file

The Session Authentication agent for Windows included with VPN-1/FireWall-1 provides for password caching and for restricting authentication to specific FireWalls.

When you start the Session Authentication agent, it is minimized and its icon appears in the system tray. From this point on, one of two things can happen:

- The user can open the Session Authentication agent and configure it.
- The Session Authentication agent can receive an authentication request from a VPN/FireWall Module.

Configuring Session Authentication with SSL

By default the user’s name and password are sent over the network unencrypted. To ensure security with fixed passwords, such as O/S passwords or VPN-1/FireWall-1 Passwords, Session Authentication communications can be encrypted using SSL.

To use Session Authentication with SSL, you must modify the following:

- VPN-1/FireWall-1 objects_5_0.C configuration file
- Session Authentication Agent configuration

Modifying the VPN-1/FireWall-1 Configuration

1. On the SmartCenter Server, issue the cpstop command.
2. Modify the file $FWDIR/conf/objects_5_0.C as follows:
under the line that includes the token :props 
add one of the following lines:

| :snauth_protocol (“none”) |
| :snauth_protocol (“ssl”) |
| :snauth_protocol (“ssl + none”) |

Note: The objects.C file should not be edited directly. Instead, use dbedit (see “dbedit” on page 589 of Check Point SmartCenter Guide) to edit the objects_5_0.C file on the SmartCenter Server.

The ssl option in the :snauth_protocol line specifies how to encrypt communications with the Session Authentication agent. TABLE 3-8 explains each option.

**TABLE 3-8 SSL options**

<table>
<thead>
<tr>
<th>option</th>
<th>explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>communication with the Session Authentication agent is not encrypted</td>
</tr>
<tr>
<td>ssl</td>
<td>activate SSL on all Session Authentication agents. Previous versions of the Session Authentication agent will not be able to authenticate users.</td>
</tr>
<tr>
<td>ssl+none</td>
<td>activate SSL on all Session Authentication agents. Previous versions of the Session Authentication agent will be able to authenticate users.</td>
</tr>
</tbody>
</table>

3 On the SmartCenter Server, issue the cpstart command.
4 Reinstall the Security Policy.

**Modifying the Session Authentication Agent Configuration**

The SSL Configuration tab of the Configuration window (FIGURE 3-27) enables you to specify whether to accept Session Authentication requests from VPN/FireWall Modules that do not support SSL encryption (For example, version 3.0 modules).
When an agent is configured to support SSL, a lock icon appears on the screen after the SSL encryption channel is set to indicate that user parameters are sent encrypted.

**Defining Session Authentication Action Properties**

To display the **Session Authentication Action Properties** window (FIGURE 3-30) for a Session Authentication rule, double-click on the rule’s **Action**.

In the **Session Authentication Action Properties** window, specify parameters that define Session Authentication for the rule.

**Source** — Reconcile **Source** in the rule with **Allowed Sources** in the **User Properties** window.

The **Allowed Sources** field in the **User Properties** window may specify that the user to whom this rule is being applied is not allowed access from the source address, while the rule may allow access. This field indicates how to resolve this conflict.
• Choose **Intersect with User Database** to apply the intersection of the access privileges specified in the rule and in the **User Properties** window.

• Choose **Ignore User Database** to allow access according to the **Source** specified in the rule.

See “Example” on page 137 for more information.

**Destination** — Reconcile **Destination** in the rule with **Allowed Destinations** in the **User Properties** window.

The **Allowed Destinations** field in the **User Properties** window may specify that the user to whom this rule is being applied is not allowed access to the destination address, while the rule may allow access. This field indicates how to resolve this conflict.

• Choose **Intersect with User Database** to apply the intersection of the access privileges specified in the rule and in the **User Properties** window.

• Choose **Ignore User Database** to allow access according to the **Destination** specified in the rule.

See “Example” on page 137 for more information.

**Contact Agent At** — Select the computer on which the Session Authentication Agent for this rule is running.

• Choose **Src** to specify that the Session Authentication Agent on the session’s **Source** object will authenticate the session.

  This is the most commonly used option.

• Choose **Dst** to specify that the Session Authentication Agent on the session’s **Destination** object will authenticate the session.

  This option would normally be used for the X protocol.

• Choose one of the computers in the list to specify that the Session Authentication Agent that will authenticate this session is running on that computer. The computers displayed in the list are the network objects defined as machines (both internal and external).

  This option enables an administrator to manually authorize connections.

**Verify secure configuration with Policy Server** — Apply the rule only if the SecureClient is properly configured.

Select a Policy Server from the drop-down list. A misconfigured SecureClient is denied access under the rule. The configuration components verified are the components checked in the **Desktop Security** page of the **Global Properties** window.
Accept only if connection is encrypted — Apply the rule only if the connection is encrypted, in other words, only if the source is a SecureClient machine.

**Defining Logging and Tracking**

Logging and tracking is specified in two places for Session Authentication:

- **Authentication Failure Track** in the Authentication page of the Global Properties window

  The options under Authentication Failure Track specify the action to take for failed authentication. These options apply to all rules.

- **Rule Base Track**

  The tracking for a successful Authentication attempt is determined by the Track field of the applied Session Authentication rule.

**How the User Authenticates**

When a local user in the rule depicted in FIGURE 3-23 on page 164 initiates a connection to the Internet, the VPN/FireWall Module on the gateway intercepts the connection and requests that the Session Authentication agent authenticate a user. The Session Authentication agent displays the Session Authentication window (FIGURE 3-31).

The user enters his or her user name, and is then prompted to enter a password (FIGURE 3-32).

![Session Authentication window — user prompt](image)
The form of the password prompt depends on the user’s Authentication method.

**Client Authentication**

In This Section

- Client Authentication — Overview  
  page 173
- Client Authentication — Deployment  
  page 177
- Client Authentication — Examples of Sign On Methods  
  page 193
- Encrypted Client Authentication  
  page 201
- Client Authentication — Security Considerations  
  page 202
- Client Authentication — Additional Features  
  page 202

**Client Authentication — Overview**

Client Authentication allows connections from a specific IP address after successful authentication. In contrast to User Authentication, which allows access per user, Client Authentication allows access per IP address. The user working on a client performs the authentication by providing a name and password, but it is the client that is granted access.

Client Authentication is less secure than User Authentication because it allows multiple users and connections from the authorized IP address or host. The authorization is per machine, because the supported services do not have an initial login procedure. For example, if FINGER is authorized for a client machine, then all users on the client are authorized to use FINGER, and will not be asked to supply a password during the authorization period. For this reason, Client Authentication is best enabled for single user machines.
The advantage of Client Authentication is that it can be used for any number of connections, for any service and the authentication is valid for any length of time.

Consider the following rules:

**FIGURE 3-33 Example Client Authentication Rule Base**

<table>
<thead>
<tr>
<th>NO</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACT</th>
<th>INSTALL ON</th>
<th>TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Towing_Tower</td>
<td>DatabaseHost</td>
<td>Lotus</td>
<td>Client_Auth</td>
<td>Log</td>
<td>Gateways</td>
<td>Any</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>DatabaseHost</td>
<td>Lotus</td>
<td>Reject</td>
<td>Alert</td>
<td>Gateways</td>
<td>Any</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Reject</td>
<td>Log</td>
<td>Gateways</td>
<td>Any</td>
</tr>
</tbody>
</table>

In the example rules shown in FIGURE 3-33, the first rule specifies Client Authentication for lotus service connections whose destination is a database server. The **Source** of a Client Authentication rule indicates the group of users that can authenticate, and the host or hosts from which they can authenticate. A user is authenticated according to the scheme defined in the **Authentication** tab of his or her **User Properties** window.

Unauthorized attempts to use the lotus service on the database host will be detected by the second rule, and an alert will be issued.

Administrators can also define authorization periods and the number of permitted sessions. For example, a user working on Tower can sign on and authenticate at the start of the day and remotely access the database host throughout the day. At the end of the day, the user signs off and closes the connection with the database host.

**Sign On Methods**

Sign On methods specify how a user begins a Client Authentication session. Sign On methods are specified in the **Client Authentication Action Properties** window of a rule. There are five Sign On methods:

- **Manual Sign On**

The Manual Sign On method requires a user to initiate the Client Authentication session on the gateway. Manual Sign On is not transparent, because the user must first connect to the gateway. The user may initiate the Client Authentication session in one of the following ways:

- **TELNET session** — the user starts a TELNET session on port 259 of the gateway
- **Web Browser** — the user requests an HTTP connection to port 900 on the gateway using a Web browser.
VPN-1/FireWall-1 also supports encrypted Client Authentication through a Web browser. This feature is available for HTTPS (HTTP encrypted by SSL) only. The user can request an HTTPS connection to a specific port on the gateway. For more information on configuring the gateway to support HTTPS, see “Encrypted Client Authentication” on page 201.

For examples using Manual Sign On, see “Manual Sign On Method” on page 193.

- **Partially Automatic Sign On**

  Partially Automatic Sign On provides Transparent Client Authentication for authenticated services (HTTP, TELNET, RLOGIN, and FTP). A user working with one of these services can directly request the target host. The user is then prompted and signed on through the User Authentication mechanism. If authentication is successful, access is granted from the IP address from which the user initiated the connection. The disadvantage of using this method is that it is available only for authenticated services.

  For an example using Partially Automatic Sign On, see “Partially Automatic Sign On Method” on page 197.

  Also see “HTTP Requests — Redirection According to Host Header” on page 202.

- **Fully Automatic Sign On**

  Fully Automatic Sign On provides Transparent Client Authentication for all services. A user working with any service directly requests the target server. Users of authenticated services are signed on through the User Authentication mechanism, while users working with all other services are signed-on using the VPN-1/FireWall-1 Session Authentication Agent. If authentication is successful, access is granted from the IP address that initiated the connection.

  Fully Automatic Sign On is available for all services, but requires a VPN-1/FireWall-1 Session Authentication Agent on the client in order to handle non-authenticated services.

  It is recommended to use Fully Automatic Sign On only if you know users have the Session Authentication Agent installed on their machines. If users do not have the Session Authentication Agent, it is recommended to use the Partially Automatic sign on method. This at least allows users of authenticated services to open a Client Authentication session on the target host without having to connect to the gateway first.

  For an example using Fully Automatic Sign On, see “Fully Automatic Sign On Method” on page 198.
For more information on the VPN-1/FireWall-1 Session Authentication Agent, see “Session Authentication” on page 162.

Also see “HTTP Requests — Redirection According to Host Header” on page 202.

- Agent Automatic Sign On

Agent Automatic Sign On provides Transparent Client Authentication for all services. Users are signed on through the VPN-1/FireWall-1 Session Authentication Agent. If authentication is successful, access is granted from the IP address that initiated the connection.

Agent Automatic Sign On requires that a VPN-1/FireWall-1 Session Authentication Agent be installed on each client.

If users do not have the Session Authentication Agent, it is recommended to use the Partially Automatic sign on method. This at least allows users of authenticated services to open a Client Authentication session on the target host without having to connect to the gateway first.

For an example using Agent Automatic Sign On, see “Agent Automatic Sign On Method” on page 199.

For more information on the VPN-1/FireWall-1 Session Authentication Agent, see “Session Authentication” on page 162.

- Single Sign On

Single Sign On is enabled through integration with Meta IP. This is Check Point’s address management feature which provides transparent network access. In this method, the VPN-1/FireWall-1 consults the user IP address records to determine which user is logged on at a given IP address. For more information see “Integration with Meta IP” on page 191.

For more information, see “Single Sign On — Additional Features” on page 190.

For an example using Single Sign On, see “Single Sign On Method” on page 200.

Partially and Fully Automatic Client Authentication rules allow users if they authenticate successfully, but do not necessarily reject the connection if the user fails authentication. In addition, the fact that a user successfully authenticates does not necessarily mean that there is a rule that allows that user access. This is because if the service is an authenticated service, the appropriate Security Server is invoked. The authenticating Security Server first checks if the connection can be allowed by a rule which does not require authentication. For more information, see “The ‘Insufficient Information’ Problem” on page 208.
How Services are Authorized

After successful authentication, the user can work with the services and hosts permitted by the rule, depending on the rule's authorization parameters. The **General** tab of the rule's **Client Authentication Action Properties** window specifies how the user works with the services permitted by the rule, as follows:

- **Standard Sign On**

  Standard Sign On enables the user on the client machine to use all the services permitted by the rule for the authorization period without having to perform authentication for each service.

- **Specific Sign On**

  With Specific Sign On, only connections that match the original connection are allowed without additional authentication. If a rule specifies more than one service or host, the user on the client must reauthenticate for each service or host. Specific Sign On enables you to limit access to services and target hosts. Specific Sign On can only be enabled by manually selecting this option when Client Authentication is initiated.

For example, consider the following Partially Automatic Sign On rule:

<table>
<thead>
<tr>
<th>NO.</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
<th>INSTALL ON</th>
<th>TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sales_Tower</td>
<td>BigBenHost</td>
<td>FTP Idle</td>
<td>Client Auth</td>
<td>Log</td>
<td>Gateways</td>
<td>Any</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>BigBenHost</td>
<td>FTP Idle</td>
<td>Reject</td>
<td>Fail</td>
<td>Gateways</td>
<td>Any</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Reject</td>
<td>Fail</td>
<td>Gateways</td>
<td>Any</td>
</tr>
</tbody>
</table>

Suppose a user on Tower initiates an FTP session on BigBen and is successfully authenticated. The user can now work with FTP on BigBen for the specified authorization period without having to reauthenticate for each FTP connection. If the user on Tower closes the initial FTP session, and decides to initiate a new FTP session (within the authorized time period) to download additional files, he or she does not have to reauthenticate.

If the same user initiates an RLOGIN session to BigBen, he or she will have to reauthenticate if **Specific Sign On** is required. If **Standard Sign On** is required, then the user will not have to reauthenticate in order to use RLOGIN.

For more information, see “Defining Client Authentication Action Properties” on page 182.

**Client Authentication — Deployment**

This section describes a deployment example for Client Authentication. This example consists of the following:
an example network configuration
what the Security Administrator must define in the VPN-1/FireWall-1 Rule Base

This example is not intended as a set of step by step instructions, but rather to illustrate how and where different components of Client Authentication are configured in the VPN-1/FireWall-1 GUI.

**Example Configuration**

FIGURE 3-34 depicts a configuration in which a VPN/FireWall Module (London) protects a PC network (localnet) and a DMZ network, which includes a database server on the host Palace.

A group of users in the QA department requires frequent access to the database on Palace. Access to Palace is allowed from localnet hosts. Each user can sign on at the beginning of the day and can use the service for a specified time period and number of sessions. If a user forgets to sign off, the connection to Palace is timed out at end of authorization period.

Access to the database server from QA users on Tower is enabled by the following rule:

![Example Client Authentication rule](image)

**Defining Client Authentication**

To enable Client Authentication for this configuration, you must define the following:

- the users who must authenticate before accessing the target server
- the gateway’s supported authentication schemes
- Client Authentication rule properties
Client Authentication properties that apply to all rules (i.e., tracking for unsuccessful authentication)
- logging and tracking

**Defining User Properties**

In a Client Authentication rule, the **Source** must be a user group. You must first define the properties of the permitted users, such as their authentication schemes and the network objects from which they are allowed access. These properties are defined in the tabs of the **User Properties** window.

**FIGURE 3-36** User Properties window - Authentication tab and Location tab

You must then define a group which includes the users who must authenticate before they access the database server.
Defining User Access

The Source field also specifies the host or network object from which the user group is allowed access.

You can add a user group to a rule using the User Access window, as follows:

1. To display the User Access window, right-click on the rule’s Source, and choose Add User Access from the drop-down menu.

2. Click on the user group you want to add.
3 Using the options under Location, specify the objects from which the users in the selected group are allowed access.

If you choose No Restriction, then the users will be allowed access from any source.

If you choose Restrict To, you must then select the network object from which the users will be allowed access.

In the example depicted in FIGURE 3-38, users in the QA group will be allowed access only from the Local_Net hosts.

**Defining the Gateway’s Authentication Schemes**

The gateway must support the same authentication schemes you defined for your users. Gateway authentication schemes are defined in the Authentication page of the gateway’s Properties window.

**FIGURE 3-39** Gateway Properties window — Authentication page
Defining Client Authentication Action Properties

You must define the Client Authentication properties of the enabling rule. These properties are defined in the tabs of the Client Authentication Action Properties window, and include the following:

- how allowed sources and destinations should be reconciled
- how services are authorized
- how authentication is initiated
- tracking for successful authentication
- authorization timeout periods
- the number of sessions allowed

To display the Client Authentication Action Properties window, double-click on the rule’s Action.

FIGURE 3-40 Client Authentication Action Properties window — General tab

Reconciling Allowed Sources and Destinations

Source — Reconcile Source in the rule with Allowed Sources in User Properties window (Location tab).

- Choose Intersect with User Database to apply the intersection of the access privileges specified in the rule and in the User Properties window.
- Choose Ignore User Database to allow access according to the Source specified in the rule.
For the configuration depicted in FIGURE 3-34 on page 178, if the Location tab of a QA user allowed access only from Thames on localnet, you would choose Ignore User Database to allow that user access from Tower, the allowed Source in the rule. See “Example” on page 137 for more information.

**Destination** — Reconcile **Destination** in the rule with **Allowed Destinations** in the **User Properties** window.

- Choose **Intersect with User Database** to apply the intersection of the access privileges specified in the rule and in the **User Properties** window.
- Choose **Ignore User Database** to allow access according to the **Destination** specified in the rule.

See “Example” on page 137 for more information.

**Note** - If **Standard** is specified in **Required Sign On** then **Destination** is automatically set to **Ignore User Database** because, under Standard Sign On, the user can access all the destinations allowed by the rule. You can change this setting only if you specify **Specific Sign On** (see FIGURE 3-40 on page 182).

**How services are authorized**

**Required Sign On** — Specify how the services permitted by the rule are authorized by selecting one of the following values:

- **Standard** — All the services allowed for the user are authorized together. For an example of how Standard Sign On is used, see “Example — Standard Sign On” on page 195.
- **Specific** — The user must request each service and destination individually. For example, if a rule specifies more than one service, then each service must be authorized separately. For an example of how Specific Sign On is used, see “Example — Specific Sign On” on page 196.

**How Client Authentication is initiated**

**Sign On Method** — Specify the sign on method by selecting one of the following values:

- **Manual** — The user must initiate Client Authentication on the gateway through either a TELNET session on port 259 or an HTTP session on port 900.
  
  
  For an example using Manual Sign On through a Web browser (HTTP), see “Example—Manual Sign On Using HTTP” on page 197.
• **Partially Automatic** — If a connection matches the rule, and the service is an authenticated service (RLOGIN, TELNET, HTTP, FTP), the user is signed on through User Authentication.

  For an example using Partially Automatic Sign On, see “Partially Automatic Sign On Method” on page 197.

• **Fully Automatic** — If a connection using a non-authenticated service matches the rule, and the VPN-1/FireWall-1 Session Authentication Agent is installed on the client, the user is signed on by the Session Authentication Agent. If a connection using an authenticated service matches the rule, then the user is signed on through User Authentication.

  For an example using Fully Automatic Sign On, see “Fully Automatic Sign On Method” on page 198.

• **Agent automatic Sign On** — If a connection matches the rule, and the VPN-1/FireWall-1 Session Authentication Agent is installed on the client, the user is signed on by the Session Authentication Agent.

  For an example using Agent Automatic Sign On, see “Agent Automatic Sign On Method” on page 199.

• **Single Sign On** — If a connection matches the rule, then VPN-1/FireWall-1 sends a query to the UAM server with the source IP. In return, the UAM Server sends VPN-1/FireWall-1 the user name that is registered to the source IP. If the user name is authenticated by VPN-1/FireWall-1, then the user connection is allowed to continue.

**Tracking**

**Successful Authentication Tracking** — logging option for the sign on session. Choose one of the following:

- **None** — no tracking
- **Log** — creates a Log of the authentication session
- **Alert** — the **Authentication Alert Command** in the **Log and Alert** page of the **Global Properties** window

These settings specify logging and tracking for the sign on session only. For information on additional logging and tracking parameters for Client Authentication, see “Defining Logging and Tracking” on page 188.

The **Limits** tab of the **Client Authentication Action Properties** window specifies the period during which the user is authorized to work with permitted services, and how many sessions are allowed.
Authorization Timeout Periods

**Authorization Timeout** — Specifies the length of time after the client is authenticated during which the user (at the source IP address specified under **Source** in the relevant rule in the Rule Base) may start the specified service.

Once the service is started, there is no restriction on how long it can remain open.

If you do not wish to restrict the authorization timeout period, check **Indefinite**.

**Refreshable Timeout** — the **Authorization Timeout** period is reset with every new connection authorized by the rule.

This option is useful if the user remains at the authorized client after successful authentication. For example, suppose that the **Authorization Timeout** is set to 15 minutes, **Refreshable Timeout** is checked, and the service allowed by the rule is FINGER. Then, a user who initiates a FINGER connection after 10 minutes resets the authorization period to 15 minutes.

If **Refreshable Timeout** is not checked, and the user does not start a FINGER connection during the 15-minute authorization timeout period, the session times out and the user must reauthenticate.

See also “Timeouts” on page 202.
Client Authentication

**Number of Sessions Allowed**

*Sessions Allowed* — the number of sessions (connections) allowed after the authentication

If you do not wish to restrict the number of sessions, check *Infinite*.

If the rule specifies a service group, and *Sessions Allowed* is not set to *Infinite*, then the number of sessions allowed for the services in the group depends on what is specified under *Required Sign On* in the General tab of the Client Authentication Action Properties window:

- If *Specific Sign On* is used, then each service in the group will be allowed the number of sessions specified. For example, if *Sessions Allowed* is set to 2, and the service group consists of FINGER and RSTAT, then each service will be allowed two sessions.

- If *Standard Sign On* is used, then the number of sessions applies to all the services in the group together.

**Defining Client Authentication Properties for all Rules**

The *Authentication* page of the Global Properties window specifies Client Authentication parameters that apply to all rules. To display this window, choose Properties from the Policy menu.
The user must either accept the default setting of 3 attempts, or define the number of failed authentication attempts before terminating the connection for the following services:

- rlogin connection
- telnet connection
- Client Authentication connection
- Session Authentication connection

**Authentication of Users with certificates:**

**Authenticate internal users with this suffix only:** This feature is enabled by default, and is relevant for users (not administrators) defined in the internal DB using PKI authentication only. This feature when checked, enforces a specific suffix to users DN, to make sure that only certificates with a specified suffix in their DN are accepted. The suffix is set by default to the suffix of the ICA's DN in order to enable authentication of user certificates issued by the ICA (user certificates issued by the ICA is a new feature in FP1.)

**Session timeout** — defines the authorized timeout period for a user to successfully authenticate him or herself.
Enable Wait Mode — This option applies only when the user initiates Client Authentication through a TELNET session to port 259 on the gateway. For information on using TELNET to initiate Client Authentication, see “Example—Manual Sign On Using TELNET” on page 193.

If Enable Wait Mode is checked, the initial TELNET session remains open. The Client Authentication session is closed when the TELNET session is closed or timed out. VPN-1/FireWall-1 regularly pings the client during the authorization period. If for some reason the client machine has suddenly stopped running (for example, because of a power failure), VPN-1/FireWall-1 closes the TELNET session and Client Authentication privileges from this IP address are withdrawn.

If Enable Wait Mode is not checked, the initial TELNET session is automatically closed when the user chooses Standard Sign On or Specific Sign On. The user must initiate another TELNET session to the gateway in order to sign off the Client Authentication session.

Note - Enable Wait Mode works only with Client Authentication rules which specify Standard Sign On. If you select Enable Wait Mode, Client Authentication rules which require Specific Sign On are not applied.

Authentication Failure Track — these options specify tracking for unsuccessful authentication attempts. These tracking options apply to all rules.

Defining Logging and Tracking

There are three places in which logging and tracking for Client Authentication is specified:

1) Rule Base Editor — Track

The tracking in this window applies to the initial communication attempt to the gateway for the authentication, and to the authenticated session.

2) Authentication page of the Global Properties window — Authentication Failure Track (FIGURE 3-42 on page 187)

The tracking in this window applies to all authentication failures.

3) The General tab of the Client Authentication Action Properties window — Successful Authentication Track (FIGURE 3-40 on page 182)
The tracking in this window applies to successful authentications.

**Example 1**

Suppose that a Manual Sign On rule specifies **Client Authentication** for the user group **QAOnTower**. Next suppose that a QA user logs in to the gateway and attempts to initiate a TELNET session under the rule.

- The tracking for the login attempt to the gateway is determined by the entry in the Rule Base **Track** for that rule.
- If the user is successfully authenticated, then the tracking for the successful authentication attempt is determined by the entry in the rule’s **Client Authentication Action Properties** window.
- If the user fails the authentication, the tracking is determined by the entry in the **Authentication** page of the **Global Properties** window.

**Example 2**

Consider the following rule:

<table>
<thead>
<tr>
<th>NO</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
<th>INSTALL ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>QA@Group@loc</td>
<td>Palace</td>
<td>FINGER</td>
<td>Client Auth</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Suppose a user wishes to start a Client Authentication session for the FINGER service on the host Palace. The target host is behind the London VPN/FireWall Module. The **Manual Sign On** method is specified in the **General** tab of the rule’s **Client Authentication Action Properties** window.

First, the user attempts to TELNET to the gateway (London) by typing:

```
telnet london 259
```

The logging in effect for this step is defined in the **Track** column of the rule in the Rule Base that controls this user's ability to access TCP port 259 on London.

Next, the user is asked to specify the user name, password, and optionally host name and service.

If the user is successfully authenticated, then the tracking for the successful authentication attempt is determined by the entry in the **General** tab of the rule’s **Client Authentication Action Properties** window. The user then starts a FINGER session on the target server. The tracking for the FINGER session is determined by the **Track** column of the above rule.

If the user fails the authentication, the tracking is determined by the entry in the **Authentication** page of the **Global Properties** window.
**Single Sign On — Additional Features**

**Single Sign On on Behalf of Multiple Users**

The **Single Sign On** method for Client Authentication enables a privileged user to sign on and sign off on behalf of other users. The privileged user does not necessarily have to be a person, but can also be an application that enables special access privileges to users based on data in its own database. Consider the following configuration and Rule Base.

**FIGURE 3-43** Single Sign On Extension

A user on Tower would, in the usual case, TELNET to port 259 on London and authenticate himself or herself, and then request access to BigBen. With the Single Sign On System Extension, another user can open the connection to BigBen in advance on behalf of a user on Tower.

The system administrator must define a user named `sso-root`. `sso-root` must be given Client Authenticated TELNET access to London. `sso-root` can then open and close connections on behalf of other users as follows:

1. `sso-root` TELNETs to port 259 on London and authenticates himself or herself. It makes no difference from which machine `sso-root` TELNETs to London.

2. After the authentication is successful, the following prompt appears:

   ```
   [real-name@] real source: 
   ```

   This prompt only appears for `sso-root`.

3. `sso-root` now enters the name and client of another user for whom access is to be allowed, for example:

   ```
   [real-name@] real source: lisa@tower
   ```
Client Authentication — Examples of Sign On Methods

This section contains examples of the different Sign On methods:

- Manual Sign On
- Partially Automatic Sign On
- Fully Automatic Sign On
- Agent Automatic Sign On
- Single Sign On

For a general overview, see “Sign On Methods” on page 174.

**Manual Sign On Method**

The Manual Sign On method requires a user to initiate the Client Authentication on the gateway. The user may initiate Client Authentication by requesting a TELNET connection or an HTTP connection to the gateway.

**Example—Manual Sign On Using TELNET**

The rule depicted in FIGURE 3-44 allows Engineering users on a single host, Tower, access to the hosts Palace or Thames after successful Client Authentication. Palace is protected by London, a VPN/FireWall Module.

---

4 Next, **sso-root** must choose (on behalf of lisa):

<table>
<thead>
<tr>
<th>Choose:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Standard Sign On</td>
</tr>
<tr>
<td>(2) Sign Off</td>
</tr>
<tr>
<td>(3) Specific Sign On</td>
</tr>
</tbody>
</table>

5 From this point on, lisa on the host tower (IP address 203.33.44.55) can TELNET or FTP to BigBen (under the rule shown above) without having to first authenticate herself on London.

If **sso-root** had entered only the client name (in step 3 above), then all users on tower with open Client Authenticated sessions would have been immediately signed off.
An Engineering user wishing to access the destination hosts must first TELNET to London, the gateway:

```
telnet london 259
```

The user is then prompted for the following data:
- user name
- password

Next, the user is asked to choose:

<table>
<thead>
<tr>
<th>Choose:</th>
<th>1</th>
<th>Standard Sign On</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td>Sign Off</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Specific Sign On</td>
</tr>
</tbody>
</table>

If there is at least one matching rule that specifies Standard in Required Sign On in the Client Authentication Action Properties window (FIGURE 3-40 on page 182), then the user can choose Standard Sign On from this menu. Otherwise, the user may choose only Specific Sign On or Sign Off.

If the user chooses Standard Sign On, then the authentication is for all services on all destination hosts, as allowed by the relevant rule or rules. The number of relevant rules is displayed by the Security Server if the authentication is successful (see FIGURE 3-45 on page 195).

If the user chooses Specific Sign On, then the user is prompted for the service name and host name (FIGURE 3-46 on page 196).

If the user chooses Sign Off, then all permissions accorded to this IP address (the host from which the user initiated the session) are withdrawn and the session is terminated (see FIGURE 3-47 on page 197).

**Note** - When Client Authentication is defined, VPN-1/FireWall-1 adds an implicit rule allowing TELNET connections to the authorization port (default 259) on the gateway. It is not necessary for the system administrator to explicitly add such a rule to the Rule Base. At the same time, the system administrator should not block access by another rule.

Once this data has been entered, the user receives either an “authorized” or “unauthorized” message, and the TELNET session is automatically closed (if Enable Wait Mode is not checked in the Authentication page of the Global Properties window).

If Enable Wait Mode is checked in the Authentication page of the Global Properties window, the TELNET session remains open. Client Authentication privileges are withdrawn from this IP address only when the TELNET session is closed or timed out.
Timeout periods and sessions allowed depend on what is specified in the **Limits** tab of the rule’s **Client Authentication Action Properties** window:

- If the user is authorized, the client machine is allowed to use the service on the specified host for the period specified in **Authorization Timeout**, unless the user signs off earlier.
- The number of connections (sessions) allowed in the given time frame is determined by the **Sessions Allowed** parameter.

**Example — Standard Sign On**

tower 1% **telnet london 259**
Trying 191.23.45.67 ...
Connected to london.
Escape character is ‘^]’.
CheckPoint FireWall-1 Client Authentication Server running on london
Login: **jim**
FireWall-1 Password: ********
User authenticated by FireWall-1 auth.

Choose:
(1) Standard Sign On
(2) Sign Off
(3) Specific Sign On

Enter your choice: **1**

User authorized for standard services (1 rules)
Connection closed by foreign host.

**FIGURE 3-45** Client Authentication — Standard Sign On for all Services and Destinations Allowed Under Rule
**Example — Specific Sign On**

```
tower 3% telnet london 259
Trying 191.23.45.67 ...
Connected to london.
Escape character is '^]'.
CheckPoint FireWall-1 Client Authentication Server running on london
Login: jim
FireWall-1 Password: ********
User authenticated by Internal auth.

Choose:
   (1) Standard Sign On
   (2) Sign Off
   (3) Specific Sign On

Enter your choice: 3
Service: rstat
Host: palace
Client Authorized for service
Another one (Y/N): Y
Service: finger
Host: thames
Client Authorized for service
Another one (Y/N): n
Connection closed by foreign host.
```

**FIGURE 3-46** Client Authentication - Specific Sign On for two Services (Each One on a Different Host)
Example — Sign Off

tower 2% telnet london 259
Trying 191.23.45.67 ... 
Connected to London.
Escape character is '^]'.
CheckPoint FireWall-1 Client Authentication Server running on
London
Login: jim
FireWall-1 Password: ********
User authenticated by Internal auth.

Choose:
  (1) Standard Sign On
  (2) Sign Off
  (3) Specific Sign On

Enter your choice: 2
User was signed off from all services
Connection closed by foreign host.

FIGURE 3-47 Client Authentication — Signing Off

Example—Manual Sign On Using HTTP

A user can also initiate a Client Authenticated session by beginning an HTTP session on port 900 on the gateway. The requested URL must specify the gateway name and port as follows:

FIGURE 3-48 HTTP session on port 900

The browser prompts the user for a name and password. The browser then presents HTML pages listing the Client Authentication options described in “Example—Manual Sign On Using TELNET” on page 193.

**Note** - When Client Authentication is defined, VPN-1/FireWall-1 adds an implicit rule allowing HTTP connections to the authorization port (default 900) on the gateway. It is not necessary for the system administrator to explicitly add such a rule to the Rule Base. At the same time, the system administrator should not block access by another rule.

Partially Automatic Sign On Method

Partially Automatic Sign On provides Transparent Client Authentication for authenticated services including HTTP, TELNET, RLOGIN, and FTP. A user working with one of these services directly requests the target host. If a connection using one of
these services matches a partially automatic Client Authentication rule, the user is prompted and signed on through the User Authentication mechanism. If authentication is successful, access is granted from the IP address from which the user initiated the connection.

Suppose the following rule specifies Partially Automatic Sign On in the rule’s Client Authentication Action Properties window (FIGURE 3-40 on page 182).

According to the above rule Jim, a Sales user at the host Tower can FTP directly to BigBen. The user on Tower is authenticated by the FTP Security Server on the London, the gateway.

```
tower # ftp bigben
Connected to london.
220 london CheckPoint FireWall-1 secure ftp server running on London
Name (bigben:jim): jim
331-aftpd: FireWall-1 password: you can use password@FW-1-password
Password: <Unix password on bigben>@<FireWall-1 password>
230-aftpd: User jimb authenticated by FireWall-1 authentication.
230-aftpd: Connected to bigben. Logging in...
230-aftpd: 220 bigben ftp server (UNIX(r) System V Release 4.0) ready.
230-aftpd: 331 Password required for jimb.
230 User jimb logged in.
```

**Note** - Although the user is authenticated by the Security Server, the connection is entered as a Client Authentication connection in the VPN-1/FireWall-1 connections table, and access is authorized from the IP address from which the user initiated the connection.

### Fully Automatic Sign On Method

Suppose the following rule specifies Fully Automatic Sign On in the rule’s Client Authentication Action Properties window (FIGURE 3-40 on page 182).
A user on Tower who initiates a connection to BigBen using any authenticated service is signed on through User Authentication. A user on Tower working with any other service, such as FINGER, is signed on through the VPN-1/FireWall-1 Session Authentication Agent (FIGURE 3-49).

Note - To enable Fully Automatic Sign On for non-authenticated services, the VPN-1/FireWall-1 Session Authentication Agent must be installed on the client.

The user can work with services and destinations in the rule according to what is specified under Required Sign On in the General tab of the rule’s Client Authentication Action Properties window (FIGURE 3-40 on page 182).

If Standard Sign On is specified, then the user can work with the all the services and destinations permitted by the rule without having to reauthenticate.

If Specific Sign On is specified, only connections which match the connection which opened the rule do not have to be reauthenticated.

The authorization period and the number of connections (sessions) allowed are specified in the Limits tab of the rule’s Client Authentication Action Properties window.

Agent Automatic Sign On Method

Suppose the following rule specifies Agent automatic Sign On in the rule’s Client Authentication Action Properties window (FIGURE 3-40 on page 182).
Then, for any service, a user on Tower who initiates a connection to BigBen is signed on through the VPN-1/FireWall-1 Session Authentication Agent (FIGURE 3-49 on page 199).

**Note** - To enable Agent Automatic Sign On for non-authenticated services, the VPN-1/FireWall-1 Session Authentication Agent must be installed on the client.

### Single Sign On Method

Suppose an ISP wishes to make a special service available only to dial-up customers who have paid an additional fee. One way to accomplish this is as follows:

1. Define a rule allowing access to the service only after Client Authentication.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>All_Users</td>
<td>special server</td>
<td>special service</td>
<td>Client Auth</td>
<td>Log</td>
<td>Gateways</td>
</tr>
</tbody>
</table>

2. After a customer dials in, gains access to the ISP and is assigned an IP address (presumably after some authentication procedure), a user-written application determines whether the customer is authorized to use the special service.

3. If the customer is authorized to use the special service, a user-written application TELNETs to port 259 on the FireWall and authenticates itself as follows:

<table>
<thead>
<tr>
<th>parameter</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>sso-root</td>
</tr>
<tr>
<td>password</td>
<td>sso-root’s password</td>
</tr>
<tr>
<td>[real-name@]</td>
<td>customer@dynamically-assigned IP address</td>
</tr>
</tbody>
</table>

From this point on, the customer can access the special service without undergoing any additional authentication procedures.

4. When the customer logs off from the ISP (or if the dial-up connection drops), the user-written application signs the client off.
The user-written application TELNETs to port 259 on the FireWall and authenticates itself as follows:

<table>
<thead>
<tr>
<th>parameter</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>sso-root</td>
</tr>
<tr>
<td>password</td>
<td>sso-root’s password</td>
</tr>
<tr>
<td>[real-name@]real source:</td>
<td>dynamically-assigned IP address</td>
</tr>
</tbody>
</table>

See also “Single Sign On — Additional Features” on page 190”.

### Encrypted Client Authentication

#### HTTPS Connections
VPN-1/FireWall-1 Client Authentication also supports HTTPS (HTTP encrypted by SSL) connections. This feature is supported only for Client Authentication sessions initiated through a Web browser. To enable encrypted Client Authentication, you must modify the gateway and Security Server configuration file, as follows:

1. **Generating CA Keys**
   - Generate the CA Key pair to be used by the SmartCenter Server and the gateway. For more information on generating CA Keys, see Chapter 3, “Certificate Authorities” of *Check Point Virtual Private Networks*.

2. **Modifying the Security Server Configuration File**
   - Modify the file `/FWDIR/conf/fwauthd.conf` by specifying SSL encryption for the HTTP Client Authentication application on an additional service port:
     ```
     950 fwssd bin/in.ahclientd wait 950 ssl
     ```

### How the User Connects
In the Web browser, the user initiates an HTTPS session on the gateway. The user must specify the gateway name and the port to which to connect, for example:

**FIGURE 3-50** Beginning an encrypted Client Authentication Session

The above example uses port 950, but any unused port number can be specified.
Client Authentication — Security Considerations

Timeouts
The Client Authentication authorization period is specified in the Limits tab of the Client Authentication Action Properties window. When the authorization period for the rule times out, the user must sign on and reauthenticate.

When using HTTP (for example, in a Partially Automatic Sign on rule), the User Authentication Timeout period in the Global Properties window also affects the period of time during which the user may work without having to reauthenticate. For HTTP, a one-time password is considered valid for this time period. A user working with HTTP does not have to generate a new password and reauthenticate for each connection. Each successful access resets the User Authentication timeout to zero.

If the User Authentication Timeout period is longer than the Client Authentication timeout, an authorized user with a one-time password can continue working without having to reenter the password, even after the Client Authentication timeout has expired. This is because the browser automatically re-sends the password for each connection. If the user initiates an HTTP connection after the Client Authentication authorization times out, the browser automatically sends the previously used password.

If the User Authentication period has not timed out, then the password is still valid.

Client Authentication — Additional Features

HTTP Requests — Redirection According to Host Header
As in all types of transparent authentication, when the user attempts to connect to a certain host, the connection is redirected through VPN-1/FireWall-1. Once the user is authenticated, VPN-1/FireWall-1 completes the connection to the requested destination. By default, this is done using the destination's IP address. However, for HTTP requests authenticated by Fully or Partially Automatic Client Authentication, it is possible to configure VPN-1/FireWall-1 so that the connection is completed according to the destination specified in the HTTP host header. This handles the case where several HTTP hosts share the same virtual IP address.

To enable redirection according to the HTTP host header, follow these steps:

1. On the SmartCenter Server, issue the cpstop command.

2. In the file $FWDIR/conf/objects.C, under the line that includes the token :props { add the following line:

```plaintext
: http_use_host_h_as_dst (true)
```

200 Check Point FireWall-1 • September 2002
On the SmartCenter Server, issue the `cpstart` command.

**Authorizing All Standard Sign On Rules**

By default, the automatic sign on methods (Partially or Fully Automatic) open one rule after successful authentication — the rule for which the sign on was initiated. For example, if a user successfully authenticates according an automatic sign on rule, that user is allowed to work with the services and destinations permitted only by that rule.

You can configure VPN-1/FireWall-1 to automatically open all Standard Sign On rules after successful authentication through Partially or Fully Automatic Sign On. If a user successfully authenticates according to an automatic sign on rule, then all Standard Sign On rules which specify that user and source are opened. The user is then permitted to work with all the services and destinations permitted by the relevant rules. In other words, VPN-1/FireWall-1 knows which user is on the client, and additional authentication is not necessary.

To authorize all relevant Standard Sign On Rules after successful Partially or Fully Automatic authentication, set the `automatically_open_ca_rules` property in the file `objects.C` to `true`. The new value will take effect after you install the Security Policy.

**Changing the Client Authentication Port Number**

To change the port number used for the Client authentication feature, proceed as follows:

1. Stop VPN-1/FireWall-1 (`cpstop`).
2. Modify the port number in the Manage‰Service‰Show‰TCP Services window for the following services:
   - If you want to modify the port number for TELNET sign on, then modify the port number of the `FW1_clntauth_telnet` service.
   - If you want to modify the port number for HTTP sign on, then modify the port number of the `FW1_clntauth_http` service.

   These services are special VPN-1/FireWall-1 services provided as part of the Client Authentication feature.
3. In the file `$FWDIR/conf/fwauthd.conf`, change the port number for the Client Authentication application to the same port number as in the previous step.
• For TELNET Sign On, modify the first column in the `in.aclientd` line.
• For HTTP Sign On, modify the first column in the `in.ahclientd` line.

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>fwssd</td>
<td>in.aftpd</td>
<td>wait</td>
</tr>
<tr>
<td>80</td>
<td>fwssd</td>
<td>in.ahttpd</td>
<td>wait</td>
</tr>
<tr>
<td>513</td>
<td>fwssd</td>
<td>in.arlogind</td>
<td>wait</td>
</tr>
<tr>
<td>25</td>
<td>fwssd</td>
<td>in.asmtpd</td>
<td>wait</td>
</tr>
<tr>
<td>23</td>
<td>fwssd</td>
<td>in.atelnetd</td>
<td>wait</td>
</tr>
<tr>
<td>259</td>
<td>fwssd</td>
<td>in.aclientd</td>
<td>wait</td>
</tr>
<tr>
<td>10081</td>
<td>fwssd</td>
<td>in.lhttpd</td>
<td>wait</td>
</tr>
<tr>
<td>900</td>
<td>fwssd</td>
<td>in.ahclientd</td>
<td>wait</td>
</tr>
<tr>
<td>0</td>
<td>fwssd</td>
<td>in.pingd</td>
<td>respawn</td>
</tr>
<tr>
<td>0</td>
<td>fwssd</td>
<td>in.asessiond</td>
<td>respawn</td>
</tr>
<tr>
<td>0</td>
<td>fwssd</td>
<td>in.aufpd</td>
<td>respawn</td>
</tr>
<tr>
<td>0</td>
<td>vpn</td>
<td>vpnd</td>
<td>respawn</td>
</tr>
<tr>
<td>0</td>
<td>fwssd</td>
<td>mdq</td>
<td>respawn</td>
</tr>
<tr>
<td>0</td>
<td>xrm</td>
<td>xrdm</td>
<td>respawn</td>
</tr>
</tbody>
</table>

**FIGURE 3-51** $FWDIR/conf/fwauthd.conf file

**Warning** - Do not change anything else in the line.

For a description of the fields in this file, see “Security Server Configuration” on page 237.

4 Make sure that there is no rule that blocks the connection to the new port.

5 Restart VPN-1/FireWall-1 (`cpstart`).

Not all of the parameters shown in the sample file above will necessarily be present in your file.
CHAPTER 4

Security Servers and Content Security

In This Chapter

Security Servers ................................................ page 205
Content Security ....................................................... page 227
Security Server Configuration ............................... page 237

Security Servers

Overview

When the first packet of a new connection arrives at a VPN/FireWall Module (a gateway or host with VPN-1/FireWall-1 installed), the Inspection Module examines the Rule Base to determine whether or not the connection is to be allowed. VPN-1/FireWall-1 applies the first rule that describes the connection (Source, Destination and Service); if this rule’s Action is Accept or Encrypt, then the connection is allowed.

Once a connection is established, VPN-1/FireWall-1 adds the connection to the connections table (see “Auxiliary Connections” on page 347 in the book Check Point Management Guide). Subsequent packets of the connection are verified against the connections table rather than against the Rule Base. The packet is allowed to pass only if the connection is listed in the connections table.

In a connection such as this, the entire connection is handled by the VPN-1/FireWall-1 Inspection (Kernel) Module (FIGURE 4-1).
When the relevant rule specifies a **Resource** under **Service**, or **User Authentication** under **Action**, the corresponding VPN-1/FireWall-1 Security Server is invoked in order to mediate the connection.

The VPN-1/FireWall-1 Security Servers provide two features:

1) **Authentication**

   For information about Authentication, see Chapter 3, “Authentication.”

2) **Content Security**

   For information about Content Security, see “Content Security” on page 227.

When a VPN-1/FireWall-1 Security Server is invoked, the Inspection (Kernel) Module diverts all the packets in the connection to the Security Server, which performs the required authentication and/or Content Security inspection. If the connection is allowed, then the Security Server opens a second connection to the final destination. Altogether, there are two connections: one from the client to the Security Server, and another from the Security Server to the final destination (the server, from the client’s point of view). Both of these connections are maintained in the **connections** table.
There are five VPN-1/FireWall-1 Security Servers, as described in TABLE 4-1.

**TABLE 4-1** VPN-1/FireWall-1 Security Servers — features

<table>
<thead>
<tr>
<th>Server</th>
<th>Authentication</th>
<th>Content Security</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>TELNET</td>
<td>yes</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>RLOGIN</td>
<td>yes</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>FTP</td>
<td>yes</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>HTTP</td>
<td>yes</td>
<td>yes</td>
<td>secure sendmail</td>
</tr>
<tr>
<td>SMTP</td>
<td>no</td>
<td>yes</td>
<td></td>
</tr>
</tbody>
</table>

**TELNET**

The TELNET Security Server provides Authentication services, but not Content Security.

**RLOGIN**

The RLOGIN Security Server provides Authentication services, but not Content Security.

**FTP**

The FTP Security Server provides Authentication services, and Content Security based on FTP commands (PUT/GET), file name restrictions, and CVP checking (for example, for viruses).

In addition, the FTP Security Server logs FTP *get* and *put* commands, as well as the associated file names, if the rule’s Track is Log.

**HTTP**

The HTTP Security Server provides Authentication services, and Content Security based on schemes (HTTP, FTP, GOPHER etc.), methods (GET, POST, etc.), hosts (for example, “*.com”), paths and queries. Alternatively, a file containing a list of IP addresses and paths to which access will be denied or allowed can be specified.

Built in protocol support allows for the chunking of data for outgoing HTTP data packets. The chunking of data occurs in the application layer of the TCP/IP Protocol Stack on the packet stream. Data is chunked by adding header and title information to the data packets which indicate the size of the data chunk. After the data chunk is processed, or rather, tested for total packet size, it is “de-chunked” (the header and title are removed). It is then treated as a single packet for content inspection purposes and “re-chunked” before being released back into the packet stream to proceed to its destination.
SMTP

The SMTP Security Server provides Content Security based on From and To fields in the envelope and header and attachment types. In addition, it provides a secure sendmail application that prevents direct online connection attacks.

The SMTP Security Server also serves as an SMTP address translator, that is, it can hide real user names from the outside world by rewriting the From field, while maintaining connectivity by restoring the correct addresses in the response.

Security Servers and the Rule Base

The ‘Insufficient Information' Problem

At the time the Rule Base is examined, it is not always possible for VPN-1/FireWall-1 to know which rule applies to a connection. This is because the connection’s first packet, on the basis of which VPN-1/FireWall-1 must determine whether to allow or disallow the connection, does not contain all the information VPN-1/FireWall-1 needs in order to determine which rule applies to the connection.

For example, consider the following network configuration and Rule Base:

Suppose the user Alice FTPs to Tower. Should VPN-1/FireWall-1 authenticate her (in accordance with the first rule) or accept the connection without authentication (in accordance with the second rule)? The answer depends on whether Alice belongs to the group Professors@Any, but VPN-1/FireWall-1 can only find out who she is (and on the basis of who she is, to which user groups she belongs) by invoking the Authentication process.
However, VPN-1/FireWall-1 cannot first authenticate Alice (to find out who she is) and then decide which rule to apply, because this can lead to the absurd situation where a user fails the Authentication process but the connection is still allowed.

**The Solution**

The VPN-1/FireWall-1 Authentication procedure, depicted in FIGURE 4-6 on page 210, solves this problem. The procedure prevents an Authentication rule from being applied when another less restrictive rule (that is, a rule without Authentication) can also be applied to the connection.

**Examples**

Consider the following Rule Base:

**FIGURE 4-4 Sample Rule Base with user groups**

<table>
<thead>
<tr>
<th>NO</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
<th>INSTA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Professors@Any</td>
<td>Tower</td>
<td>FTP</td>
<td>User Auth</td>
<td>Log</td>
<td>Gateways</td>
</tr>
<tr>
<td>2</td>
<td>Teachers@Any</td>
<td>Tower</td>
<td>FTP</td>
<td>User Auth</td>
<td>Log</td>
<td>Gateways</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Reject</td>
<td>Log</td>
<td>Gateways</td>
</tr>
</tbody>
</table>

Suppose a user FTPs to Tower. VPN-1/FireWall-1 matches the first rule, and invokes the FTP Security Server and authentication process. However, if the user belongs to Teachers@Any, then the second rule is the one which applies to the connection. Since both rules specify Authentication, it does not matter that the Authentication was invoked by a rule other than the one that was applied to the connection. This is because Authentication scheme and password are attributes of the user, not of the group, and are the same whether the user is being authenticated as a member of Professors@Any or of Teachers@Any. Next, consider this Rule Base:

**FIGURE 4-5 Sample Rule Base employing a more permissive rule**

<table>
<thead>
<tr>
<th>NO</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
<th>INSTALL ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Professors@Any</td>
<td>Tower</td>
<td>FTP</td>
<td>User Auth</td>
<td>Log</td>
<td>Gateways</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Tower</td>
<td>FTP</td>
<td>Accept</td>
<td>Log</td>
<td>Gateways</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Reject</td>
<td>Log</td>
<td>Gateways</td>
</tr>
</tbody>
</table>
Suppose a user FTPs to Tower. The first matching rule is the first rule (whose **Action** is **User Auth**), but it is the second rule that is applied, because it also matches but its **Action** is **Accept**. In this case, it is important that the original rule was not applied, that is, that there was no Authentication even though the Security Server was invoked.

**Note** - In this case, the connection is mediated by the Security Server, even though there was no Authentication.

You can verify this by stepping through the Authentication procedure depicted in **FIGURE 4-6** on page 210.
Outgoing Connections

User Authentication and Resource rules are applied only to connections incoming to a FireWalled machine. An outgoing connection originating on a FireWalled machine will not be folded into a Security Server on that machine, but will be dropped (because of the third rule depicted in FIGURE 4-4 on page 209).

FTP Security Server

When an FTP connection is mediated by the VPN-1/FireWall-1 FTP Security Server, then the user’s requested FTP commands and file names are matched against the FTP Resource defined in the relevant rule.

The FTP Security Server is invoked when a rule specifies an FTP Resource in the Service field and/or User Authentication in the Action field. If no FTP Resource is specified in the rule (that is, if the Security Server is invoked because the Action is User Authentication), then an FTP Resource of GET and PUT allowed for all files is applied.

FTP Resource Matching

FTP Resource matching consists of matching methods and file names to the Resource definition.
Methods

TABLE 4-2 lists the FTP commands that correspond to the methods specified in the FTP Resource definition.

### TABLE 4-2 FTP actions and commands

<table>
<thead>
<tr>
<th>method (defined in the FTP Resource)</th>
<th>applies to these FTP commands</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>RETR</td>
<td>retrieve</td>
</tr>
<tr>
<td></td>
<td>RNFR</td>
<td>rename from</td>
</tr>
<tr>
<td></td>
<td>XMD5</td>
<td>MD5 signature</td>
</tr>
<tr>
<td>PUT</td>
<td>STOR</td>
<td>store</td>
</tr>
<tr>
<td></td>
<td>STOU</td>
<td>store unique</td>
</tr>
<tr>
<td></td>
<td>APPE</td>
<td>append</td>
</tr>
<tr>
<td></td>
<td>RNFR</td>
<td>rename from</td>
</tr>
<tr>
<td></td>
<td>RNTO</td>
<td>rename to</td>
</tr>
<tr>
<td></td>
<td>DELE</td>
<td>delete</td>
</tr>
<tr>
<td></td>
<td>MKD</td>
<td>make directory</td>
</tr>
<tr>
<td></td>
<td>RMD</td>
<td>remove directory</td>
</tr>
</tbody>
</table>

The VPN-1/FireWall-1 FTP Security Server passes all other FTP commands to the FTP server for execution.

File Names

File name matching is based on the concatenation of the file name in the command and the current working directory (unless the file name is already a full path name) and comparing the result to the path specified in the FTP Resource definition.

When specifying the path name in the FTP Resource definition, only lower case characters and a directory separator character / can be used.

The Security Server modifies the file name in the command as follows:

- for DOS, the drive letter and the colon (:) is stripped for relative paths
- the directory separator character (/ or \) is replaced, if necessary, with the one appropriate to the FTP server's OS

In some cases, the Security Server is unable to resolve the file name, that is, it is unable to determine whether the file name in the command matches the file name in the resource.
Example - DOS

Suppose the current directory is `d:\temp` and the file name in the resource is `c:x`. Then the Security Server is unable to determine the absolute path of the file name in the command because the current directory known to the Security Server is on disk `D:` and the file is on disk `c:`, which may have a different current directory.

Example - Unix

If the file name in the command contains `..` references (which refer to symbolic links), then it is possible that the file name in the command matches the resource's path, but that the two in fact refer to different files.

When the Security Server cannot resolve a file name, the action it takes depends on the `Action` specified in the rule being applied:

- If the rule's `Action` is `Reject` or `Drop`, then the rule is applied and its `Action` taken.
- If the rule's `Action` is `Accept`, `Encrypt` or `Authenticate`, then:
  - If the resource path is `*` or there is no resource, the rule is applied.
  - Otherwise, the rule is not applied. Instead, VPN-1/FireWall-1 scans the Rule Base and applies the next matching rule (which may be the default rule that drops everything). In this case, a potential problem is that the rules may specify different entries in their `Track` fields. For example, it may happen that the original rule specifies `Accounting` in the `Track` field while the rule that is applied does not.

SMTP Security Server

The SMTP Security Server does not provide Authentication because there is no human user at a keyboard who can be challenged for authentication data. However, the SMTP Security Server provides Content Security that enables a Security Administrator to:

- provide mail address translation by hiding outgoing mail's `From` address behind a standard generic address that conceals internal network structure and real internal users
- perform mail filtering based on SMTP addresses and IP addresses
- strip MIME attachments of specified types from mail
- strip the `Received` information from outgoing mail, in order to conceal internal network structure
- drop mail messages above a given size
- send many mail messages per single connection
- resolve the DNS address for mail recipients and their domain on outgoing connections (MX Resolving)
- control the load generated by the mail dequeuer in two different ways:
• control the number of connections per site
• control the overall connections generated by the mail dequeuer

- provide a Rule Base match on the Security Server mail dequeuer which enables:
  • a mail-user based policy
  • better performance of different mail contents action per recipient of a given mail
  • generation of different mail contents on a per-user basis
  • application of content security features at the user level

- perform CVP checking (for example, for viruses)

In addition, the SMTP Security Server provides additional security over standard sendmail applications. Its functionality is split between two separate modules (see FIGURE 4-7, so there is no direct path connecting mail servers, preventing direct online connections to the real sendmail application.

**FIGURE 4-7** VPN-1/FireWall-1 SMTP Security Server

One process writes incoming messages to a disk cache, and the other process empties the cache.
Functionality

The VPN-1/FireWall-1 SMTP Security Server supports the following SMTP commands:

**TABLE 4-3 Supported SMTP commands**

- RCPT
- DATA
- SIZE
- MAIL
- NOOP
- EHLO
- HELO
- HELP
- QUIT
- RSET

The VPN-1/FireWall-1 SMTP Security Server supports the ESMTP feature:

`SIZE= "message size declaration"`

**SMTP Security Server Configuration**

The SMTP Security Server configuration is in the **SMTP** page in the **Gateway Properties** window (FIGURE 4-8).
FIGURE 4-8 SMTP page — Gateway Properties window

The SMTP fields and their meanings are listed in TABLE 4-3.

TABLE 4-4 SMTP field meanings

<table>
<thead>
<tr>
<th>field</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Timeout</td>
<td>number of seconds after which the connection times out</td>
</tr>
<tr>
<td>Dequeuer Scan Period</td>
<td>how frequently the Dequeuer spool directory is scanned</td>
</tr>
<tr>
<td>Mail Resend Period</td>
<td>number of seconds after which the SMTP Security Server resends the message after failing to deliver the message</td>
</tr>
<tr>
<td>Mail Abandon Time</td>
<td>number of seconds after which the SMTP Security Server abandons attempts to resend</td>
</tr>
</tbody>
</table>
Alerts

The SMTP Security Server can be configured to issue alerts in the event of various SMTP–related system error conditions, such as insufficient disk space (possibly caused by a denial–of–service attack).

**HTTP Security Server**

**Support for FTP**

The HTTP Security Server supports FTP requests through a Web browser. The HTTP Security Server must be defined as the HTTP proxy to the user’s Web browser. This is done in the user’s Web browser proxy settings.

FIGURE 4-9 shows the proxy configuration windows for Netscape and Internet Explorer.

**TABLE 4-4  SMTP field meanings**

<table>
<thead>
<tr>
<th>field</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Number of Recipients</td>
<td>the maximum number of recipients of a mail message</td>
</tr>
<tr>
<td>Maximum generated concurrent connections</td>
<td>the maximum number of concurrently generated connections</td>
</tr>
<tr>
<td>Maximum generated concurrent connections per site</td>
<td>the maximum number of generated concurrent connections on a per site basis</td>
</tr>
<tr>
<td>Don’t accept mail larger than:</td>
<td>the maximum mail size to be accepted</td>
</tr>
<tr>
<td>Maximum number of mail messages in spool</td>
<td>the maximum number of mail messages to be accepted in the spool If the number of mail messages exceeds the designated limit, new mails will not be accepted.</td>
</tr>
<tr>
<td>Check if spool goes over/under the limit every...Sec</td>
<td>how frequently the SMTP server and mail dequeuer check the spool_limit</td>
</tr>
<tr>
<td>Spool Directory:</td>
<td>the location of the spool directory If you do not choose to use the default fw–1 spool directory and instead create a new one, you must verify that read/write permission is set on the new spool directory. You should copy all the mail from the old spool directory to the new spool directory. Then perform cpstart; cpstop via the command line.</td>
</tr>
<tr>
<td>Postmaster Name:</td>
<td>to whom to send error messages</td>
</tr>
</tbody>
</table>

**Alerts**

The SMTP Security Server can be configured to issue alerts in the event of various SMTP–related system error conditions, such as insufficient disk space (possibly caused by a denial–of–service attack).

**HTTP Security Server**

**Support for FTP**

The HTTP Security Server supports FTP requests through a Web browser. The HTTP Security Server must be defined as the HTTP proxy to the user’s Web browser. This is done in the user’s Web browser proxy settings.

FIGURE 4-9 shows the proxy configuration windows for Netscape and Internet Explorer.
When a user requests an FTP URL through a browser:

1. The browser connects to the Security Server and sends an HTTP request with FTP as the method.
2. The Security Server opens an FTP session with the requested server.
3. The Security Server sends the FTP request to the server and formats all responses as HTTP messages, which it sends to the browser. These messages are listed in the file 
\texttt{/conf/f2ht-msgs}.

   The Security Server sends an RETR request to the FTP server to determine whether the requested URL specifies a directory or file. If the FTP server returns an error message with a text line indicating the request is not a file, the Security Server assumes the requested URL is a directory. The Security Server then sends the directory listing to the browser as an HTML page.

   If the requested URL is a file, the Security Server determines whether it is a text file or a binary file. If the requested file ends with one of the suffixes listed in the file 
\texttt{/conf/f2ht-bin-sfxs}, it is considered a binary file.

FTP requests through a web browser are enabled by both User Authentication and URI Resource rules. If the relevant rule specifies a URI Resource, then \texttt{ftp} must be defined as one of the enabled \texttt{Schemes} in the \texttt{URI Definition} window (see FIGURE 4-20 on page 232 of \textit{Check Point Management Guide}).

For more information on URI Resources, see “URI Resources” in Chapter 6, “Services and Resources”, in the book \textit{Check Point Management Guide}.
Support for HTTPS

HTTPS (HTTP encrypted by SSL) connections are handled by the HTTP Security Server in the following ways:

- **Security Proxy Mode** — In Security Proxy mode, the HTTP Security Server is defined as the “security proxy” in the user’s Web browser settings. The HTTP Security Server acts as a proxy for HTTPS connections, but does not inspect content.
- **Non-transparent Mode** — The HTTP Security Server is configured to encrypt and decrypt HTTPS connections. This option is known as “Non-transparent”, because the HTTPS user must initiate the connection on the gateway before connecting to the target server.

Security Proxy Mode

HTTPS (HTTP encrypted by SSL) connections can be handled by the HTTP Security Server when it is defined as the Security Proxy to the local user’s Web browser. The HTTP Security Server proxies outgoing HTTPS connections, but does not inspect content. This option can be used with User Authentication rules to authenticate outgoing HTTPS, and with Resource rules. User Authentication and Resource rules can be used together.

The user can configure a Security Proxy for the following Web browsers:
- Internet Explorer version 3.0x and higher
- Netscape version 4.0x and higher

**FIGURE 4-10** HTTP Proxy and Security Proxy Settings — Netscape 4.0x and Internet Explorer 3.0x
HTTPS requests generally use the HTTP “CONNECT” method (tunneling mode). Because the CONNECT method only specifies a hostname and port, the HTTP Security Server does not have access to the content of the communication, not even the URL. In addition, the Security Server does not verify that the connections are really using HTTPS — it only checks the requested hostname and port number. All communication between the client and the target server is encrypted — the HTTP Security Server mediates the connection. This is useful if internal users want to send encrypted information over the Internet.

**Note** - Although the connection is encrypted between the local client and the external server, the authentication session between the local client and the HTTP Security Server is clear (unencrypted).

**User Authentication Rules**

In Security Proxy mode, you can provide security by requiring internal users to authenticate before accessing external HTTPS servers. For more information, see “Authenticating Internal Users Accessing External HTTPS (Security Proxy Mode)” on page 150.

**URI Resource rules**

The **URI Definition** window must specify the following:

- **Connection Methods** (on the **General** tab) — check **Tunneling**

**FIGURE 4-11 URI Definition window - Connections Methods**

---

*Check Point FireWall-1  •  September 2002*
When **Tunneling** is checked, HTTP requests using the CONNECT method are matched. The HTTP Security Server does not inspect the content of the request, not even the URL. Only the host and port number can be checked. Therefore, when **Tunneling** is checked, some Content Security options in the URI Resource specification, (for example, CVP options, HTML weeding) are disabled.

If you check **Tunneling**, you can still use the URI File or UFP specifications. A URI File specification must define a file that lists only server names and their port numbers. The UFP specification must use a UFP server that maintains a list of only server names and port numbers.

**Host** (on the **Match** tab)— Specify the host and port of a known HTTPS server, for example:

```
https server host:443
```

The field to the left of the colon specifies the URI’s host. The field to the right of the colon specifies the port.

A wildcard character (“*”) indicates any host or any port. For example, you can specify “*:443” or “*:443”. For HTTPS, “*” (a single wildcard character) is not a valid entry, though “**” is a valid entry for HTTP or FTP resources.

For more information on URI Resources, see “URI Resources” in Chapter 6, “Services and Resources”, in the book, *Check Point Management Guide*.

**Non-transparent Mode and HTTPS**

To enable the HTTP Security Server to inspect the contents of HTTPS connections, you can configure the HTTP Security Server to encrypt and decrypt HTTPS connections. This requires the implementation of Non-transparent Authentication.

This option is known as “Non-transparent Mode” because the user of HTTPS must access the gateway before being allowed to continue to the target host. Because the HTTP Security Server is not defined as a Security Proxy to the user’s Web browser, Non-transparent Mode is best used to authenticate external users accessing internal servers.

For information on configuring support for HTTPS in Non-transparent Mode, see “HTTP Security Server and Non-Transparent Authentication” on page 154 in Chapter 3, “Authentication.”
Interaction with OPSEC Products

The VPN-1/FireWall-1 Security Servers support third-party products working with Check Point’s OPSEC SDK. In the OPSEC framework, the enterprise security system is composed of several components, each of which is provided by a different vendor and may be installed on a different machine or run simultaneously on the same machine in different processes. VPN-1/FireWall-1 distributes security tasks to the OPSEC components. Transactions between VPN-1/FireWall-1 and OPSEC security components take place using open, industry standard protocols.

Information about OPSEC is available at http://www.opsec.com.

Samples of OPSEC components are:
- a CVP (Content Vectoring Protocol) server that examines files for content
- a UFP (URL Filtering Protocol) server that categorizes URLs

For a more complete description of OPSEC Servers and Clients see “OPSEC Servers and Clients” in Chapter 10, “Server Objects and OPSEC Applications” of Check Point Management Guide.

In a common OPSEC model, a VPN-1/FireWall-1 Security Server acts as a client sending requests to an OPSEC server. The Security Server intercepts a connection and generates a request to the OPSEC server. The server processes the request and sends a reply to the Security Server, which processes the original connection based on the reply.

FIGURE 4-12 shows how the HTTP Security Server handles a connection request to a URL using an OPSEC UFP Server:
1. **VPN-1/FireWall-1** intercepts a connection request to a URL. The connection matches a rule which specifies a URI Resource under the Rule Base **Service** field. The Resource definition specifies a UFP server which maintains a list of URLs and their categories. VPN-1/FireWall-1 determines that the UFP server must be invoked.

2. **VPN-1/FireWall-1** diverts the connection to the HTTP Security Server. The Security Server connects to the UFP server and initiates the URL Filtering Protocol.

3. The HTTP Security Server sends a request containing the name of the URL.

4. The UFP server checks the URL against lists of URLs and their categories. The UFP server returns a message notifying the HTTP Security Server of the categories to which the URL belongs.

5. The HTTP Security Server takes the action defined for the resource, either allowing or disallowing the connection attempt.

For information on defining UFP or CVP OPSEC applications, see “OPSEC UFP and CVP Groups” in Chapter 10, “Server Objects and OPSEC Applications” of *Check Point Management Guide*.

For more information on OPSEC-certified products, see http://www.opsec.com.
Defining Security Servers

The properties of the VPN-1/FireWall-1 Security Servers are specified on the **Security Server** page (see FIGURE 4-13 below). To access the **Security Server** page, proceed as follows:

1) From the main toolbar, choose **Policy > Global Properties**,

2) Select **FireWall-1** from the **Global Properties** objects tree and select **Security Server** by double-clicking.

**FIGURE 4-13** Global Properties window - Security Server page

**Telnet Welcome Message File** — the name of a file whose contents are to be displayed when a user begins an Authenticated TELNET session (optional)

**SMTP Welcome Message File** — the name of a file whose contents are to be displayed when the SMTP Security Server starts (optional)

**FTP Welcome Message File** — the name of a file whose contents are to be displayed when a user begins an Authenticated FTP session (optional)
Rlogin Welcome Message File — the name of a file whose contents are to be displayed when a user begins an Authenticated RLOGIN session (optional)

Client Authentication Welcome Message File — the name of a file whose contents are to be displayed when a user begins a Client Authenticated session (optional) For more information, see “Client Authentication” on page 173.

Note - Client Authenticated sessions initiated through the Manual Sign On method are not mediated by a Security Server.

Customizing Security Server Messages

The default Security Server messages may be customized by editing the default content file, cpsc.en_us, in the $FWDIR/conf/cpsc directory. Consider the following message string:

CPSC_HTTP_FW_AT_HOST 1024 "FW-1 at #host#:" (host)

The possible fields in the message string are described in TABLE 4-5.

<table>
<thead>
<tr>
<th>field</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPSC_HTTP_FW_AT_HOST</td>
<td>file identification</td>
</tr>
<tr>
<td>1024</td>
<td>maximum file message size (in Bytes)</td>
</tr>
<tr>
<td>&quot;FW-1 at #host#:&quot;</td>
<td>message body</td>
</tr>
<tr>
<td>(host)</td>
<td>allowed parameter</td>
</tr>
<tr>
<td>#date#</td>
<td>calendar date Security Server message is implemented (can be used with any message string)</td>
</tr>
<tr>
<td>#time#</td>
<td>time of day when Security Server message is implemented (allowed to be used with any message string)</td>
</tr>
</tbody>
</table>

Within the $FWDIR/conf/cpsc directory, the message body file, msg_cnt.C, defines the names of the files which contain the strings in the message database. Each of these files contain a number of entries, each represented by a line in the file. These files define one message in the message database.

The second file, the cpsc.en_us file, is the default content file which may be edited by adding or removing the syntax for this field to define the names of the content files. By editing this file, the Security Server messages may be customized.
In the following three message string examples, first and last files are read only, while
the third file, the message body string has been edited for customization. The defined
content files may be used multiple times within the message string.

Consider the following three examples:

**Example Using Host Name Content Defined**

The following string:

```
CPSC_HTTP_FW_AT_HOST 1024 "FW-1 at #host#:" (host)
```

produces the following Security Server message:

**FIGURE 4-14** Customized Security Server message defining host content as “FW-1”

where “ronaldo” has been defined as the Firewall Module.

**Example Using Security Server Content Defined**

The following string:

```
CPSC_HTTP_FW_AT_HOST 1024 "Security Server at #host#:" (host)
```

produces the following Security Server message:

**FIGURE 4-15** Customized Security Server message with “Security Server at” as defined

In this case, the message string has defined the HTTP Security Server as “Security
Server” and the FireWall Module (host) as “ronaldo”.

226 Check Point FireWall-1 • September 2002
Example Using Proxy Authorization Content Defined

The following string:

CPSC_HTTP_FW_AT_HOST 1024 "Proxy Authorization:" (host)

produces the following Security Server message:

**FIGURE 4-16 Customized Security Server message with “Proxy Authorization” as defined**

![Customized Security Server message](image)

In this particular case, the message string is defined as “Proxy authentication”.

The following fields specify parameters for the HTTP Security Server:

**HTTP Next Proxy** — For information about this field, see “HTTP Security Server Configuration” on page 143 of Chapter 3, “Authentication.”

**HTTP Servers:** — You can define HTTP Servers to restrict HTTP access to specific hosts and ports. For more information, see “HTTP Servers (Security Server)” on page 144.

### Content Security

**In This Section**

- Resources and Security Servers: page 228
- Web (HTTP): page 230
- Mail (SMTP): page 233
- FTP: page 234
- CVP Inspection: page 234
- CVP Load Sharing and Chaining: page 236
**Resources and Security Servers**

Content Security extends the scope of data inspection to the highest level of a service’s protocol, achieving highly tuned access control to network resources. VPN-1/FireWall-1 provides content security for HTTP, SMTP and FTP connections using the VPN-1/FireWall-1 Security Servers and Resource object specifications.

A VPN-1/FireWall-1 Resource specification defines a set of entities which can be accessed by a specific protocol. You can define a Resource based on HTTP, FTP and SMTP. For example, you might define a URI resource whose attributes are a list of URLs and the HTTP and FTP schemes. The resource can be used in the Rule Base in exactly the same way a service can be used, and the standard logging and alerting methods are available to provide monitoring of resource usage.

When a rule specifies a Resource in the **Service** field of the Rule Base, the VPN-1/FireWall-1 Inspection Module diverts all the packets in the connection to the corresponding Security Server, which performs the required Content Security inspection. If the connection is allowed, the Security Server opens a second connection to the final destination.

FIGURE 4-17 depicts what happens when a rule specifies the use of an HTTP Resource.

**FIGURE 4-17** A connection mediated by the HTTP Security Server

For each connection established through a VPN-1/FireWall-1 Security Server, the Security Administrator is able to control specific access according to fields that belong to the specific service: URLs, file names, FTP PUT/GET commands, type of requests and others. Major security enhancements enabled by the Content Security feature are CVP checking (for example, for viruses) for files transferred and URL filtering.

When a Resource is specified, the Security Server diverts the connection to one of the following servers:

- Content Vectoring Protocol (CVP)
A CVP server examines and reports on the contents of files, for example, whether a file contains a virus. A CVP server can also examine the content of outgoing data packets prior to establishing an outgoing connection to an HTTP Web Server.

- **URL Filtering Protocol (UFP)**

A UFP server maintains a list of URLs and their categories.

The server performs the requested content inspection and returns the results to the Security Server. The Security Server allows or disallows the connection, depending on the results.

Communication between the Security Server and the CVP or UFP server is enabled through Check Point’s OPSEC (Open Platform for Secure Enterprise Connectivity) framework. For more information about OPSEC integration within VPN-1/FireWall-1, see [http://www.checkpoint.com/opsec](http://www.checkpoint.com/opsec).

**FIGURE 4-18** shows what happens when a VPN-1/FireWall-1 Security Server passes a file to a Content Vectoring Server for inspection during an FTP connection.

**FIGURE 4-18 Content Vectoring Server**

1. VPN-1/FireWall-1 determines that the Content Vectoring Server must be invoked.

   The relevant rule for the connection specifies a resource which includes CVP checking.

2. The FTP Security Server connects to the Content Vectoring Server and initiates the Content Vectoring Protocol.
The FTP Security Server sends the Content Vectoring Server the file to be inspected.

The Content Vectoring Server inspects the file, and returns a Validation Result message notifying the FTP Security Server of the result of the inspection.

The Content Vectoring Server optionally returns a modified version of the file to the FTP Security Server.

The FTP Security Server takes the action defined for the resource, either allowing or disallowing the file transfer.

For more information on CVP inspection, see “CVP Inspection” on page 234.

**Web (HTTP)**

A URI is a Uniform Resource Identifier, of which the familiar URL (Uniform Resource Locator) is a specific case. URI resources can define schemes (HTTP, FTP, Gopher, etc.), methods (GET, POST, etc.), hosts (for example, “*.com”), paths and queries. Alternatively, a file containing a list of IP addresses of servers and paths can be specified.

In addition, the Security Administrator can define how to handle responses to allowed resources, for example, that JAVA applets not be allowed even on resources that are allowed. JAVA applets, JAVA scripts and ActiveX can be removed from HTML. A customizable replacement URL, for example a page containing a standardized error message, can be displayed when access to a response is denied.

**FIGURE 4-19** URI Resource Definition
URL Filtering

URL filtering provides precise control over Web access, allowing administrators to define undesirable or inappropriate Web pages. VPN-1/FireWall-1 checks Web connection attempts using URL Filtering Protocol (UFP) servers. UFP servers maintain lists of URLs and their appropriate categories (i.e. permitted or denied). URL databases can be updated to provide a current list of blocked sites. All communication between VPN-1/FireWall-1 and the URL Filtering server is in accordance with the URL Filtering Protocol.

In order to implement URL filtering, proceed as follows:

1. Define a UFP Server.
2. Define a URI Resource that specifies a list of URL categories from the UFP server.
4. Specify whether Content Vectoring Protocol (CVP) is to be implemented.

Defining a UFP Server

UFP Servers are defined in the OPSEC Application properties window.

UFP Server groups are defined in the UFP Group Properties window (see “OPSEC UFP and CVP Groups” in Chapter 10, “Server Objects and OPSEC Applications” of Check Point Management Guide).

Defining a Resource

The URI resource is defined in the URI Definition window (UFP Specification). The URI Resource specifies the UFP server and a list of URL categories provided by the server. In the Resource depicted in FIGURE 4-20 on page 232, “WebCop” is the UFP Server, and the URL categories are “alcohol” and “drugs.” The “alcohol” category is selected. This means that if WebCop assigns the category “alcohol” to a URL, then the URL matches the resource’s definition, and the rule is applied.
For example, suppose the Security Administrator defines two URI resources:

- **Allowed** — HTTP and FTP schemes, GET and POST methods
- **Not Allowed** — a list of “forbidden” URLs categories

Then the following rules prevent local users from accessing the **NotAllowed** resource and allow users access to the **Allowed** resource after authentication.

When a Resource in a rule specifies a list of permitted or denied URLs, the HTTP Security Server sends a request to the UFP server containing the name of the URL in question. The UFP server checks the URL against lists of URLs and their categories. The UFP server returns a message notifying the HTTP Security Server of the categories to which the URL belongs.

For example, if a user requests a connection to a URL that belongs to a category specified in the Resource denied HTTP, VPN-1/FireWall-1 denies the connection request. If the URL does not belong to the categories defined by this Resource, the Security Server opens a separate connection to the destination.
Defining Content Vectoring Protocol (CVP) Checking

The URI Resource must also specify whether CVP checking is to be implemented. CVP fields are defined in the CVP tab of the URI Definition window. The user must define whether or not Content Vectoring Protocol is to be used.

FIGURE 4.22 URI Definition window - CVP tab

The user must then select the CVP Server and define whether or not the CVP server is allowed to modify content and whether to send HTTP Headers to the CVP server.

For complete configuration information on defining URI resources, see “URI Resources” in Chapter 6, “Services and Resources”, in the book, Check Point Management Guide.

Mail (SMTP)

VPN-1/FireWall-1 offers an SMTP server that provides highly granular control over SMTP connections. A new spool dequeuer mechanism provides more efficient spool scanning by performing FIFO, which enables mail to be put in the mail dequeuer and gives priority to new mail over undeliverable old mail by using a multiple queue mechanism. The Security Administrator can:

- hide outgoing mail’s From address behind a standard generic address that conceals internal network structure and real internal users
- perform mail filtering based on SMTP addresses and IP addresses
- strip MIME attachments of given types from mail
- strip files from emails by specifying their names (including wild cards), for example (*.doc) will remove all file whose suffix is “.doc”
- drop mail messages above a given size
Content Security

- send many mail messages per single connection
- resolve the DNS address for mail recipients and their domain on outgoing connections (MX Resolving)
- control the load generated by the mail deqeuer in two different ways:
  - control the number of connections per site
  - control the overall connections generated by the mail deqeuer
- perform a mail-user based policy enabling
  - perform different mail actions per recipient of a given mail,
  - enabling the generation of different mail contents on a per user basis and
  - apply content security features at the user level

For information on defining SMTP resources, see “URI Resources” in Chapter 6, “Services and Resources”, in the book, Check Point Management Guide.

FTP

The FTP Security Server provides Content Security based on FTP commands (PUT/GET), file name restrictions, and CVP inspection for files.

For information on defining FTP resources, see “URI Resources” in Chapter 6, “Services and Resources”, in the book, Check Point Management Guide.

CVP Inspection

CVP inspection is an integral component of VPN-1/FireWall-1’s Content Security feature, and considerably reduces the vulnerability of protected hosts. CVP inspection examines all files transferred for all protocols. CVP configuration (which files to inspect, how to handle invalid files) is available for all Resource definitions. All VPN-1/FireWall-1 auditing tools are available for logging and alerting when these files are encountered.

CVP inspection is implemented by Content Vectoring Servers. The interaction between VPN-1/FireWall-1 and the Content Vectoring Server is defined by Check Point’s OPSEC (Open Platform for Secure Enterprise Connectivity) framework. This interaction is depicted in FIGURE 4-18 on page 229.

For more information about OPSEC integration within VPN-1/FireWall-1, see http://www.checkpoint.com/opsec. If you would like to download evaluation versions of OPSEC-certified products, see http://www.opsec.com.

Implementing CVP Inspection

In order to implement CVP inspection, proceed as follows:
1. Define a CVP OPSEC application.
2. Define Resource objects that specify CVP checking for the relevant protocols.
3. Define rules in the Rule Base that specify the action taken on connections that invoke each Resource.

**Defining a CVP OPSEC Application**

Content Vectoring Protocol OPSEC applications are defined in the OPSEC APPLICATION window. For information on defining a CVP OPSEC Application (see Chapter 10, “Server Objects and OPSEC Applications”) ifp servers are de

**Defining Resources**

The following CVP inspection options are available for all Resource definitions.

- **Use of CVP (Content Vectoring Protocol)** — specify whether CVP is to be used.
- **CVP Server** — if CVP is to be used, the user must then define whether or not the CVP server is allowed to modify content and whether to send HTTP headers or SMTP headers to the CVP server.
- **Reply Order field** — designates when data is to be returned to the user. You must select one of the following choices:
  - **Return data after content is approved** — Data are returned after all the data have been checked.
  - **Return data before content is approved** — Data are returned before all the data have been checked.
  - **Controlled by CVP server** — Data are returned as specified by the CVP Server.

**Defining Rules**

Rules that specify CVP inspection do not replace rules that allow FTP, HTTP, or SMTP connections. Since VPN-1/FireWall-1 examines the Rule Base sequentially, you must define rules in the appropriate order to prevent unwanted traffic from entering your network.

Resource rules which accept HTTP, SMTP, and FTP connections must be placed before other rules which accept these services. If you define a rule that allows all HTTP connections before a rule which specifies CVP inspection on a URI Resource, you may be allowing unwanted traffic.
Similarly, CVP rules must be placed after rules which reject FTP, HTTP or SMTP Resource connections. For example, a rule rejecting large e-mail messages must come before a CVP rule allowing specific SMTP connections.

**CVP Load Sharing and Chaining**

VPN-1/FireWall-1 enables a Resource to invoke any number of CVP Servers sequentially. This capability is called “chaining” and is useful when each of the CVP Servers performs a different function.

Identical CVP Servers can be configured to share the load among themselves. This capability is called “load sharing” and increases efficiency.

**Chaining**

Chaining is the process of connecting servers for the purpose of combining functionality. In the configuration shown in FIGURE 4-23, the VPN/FireWall Module invokes the CVP Servers on bigben, tower and bridge, one after the other.

**Load Sharing**

Load sharing is the process of connecting identical servers for the purpose of efficiency.

---

**Note** • You can chain load share groups but you cannot load share chaining groups.

Security Server Configuration

fwauthd.conf file

Each line in the Security Server configuration file $FWDIR/conf/fwauthd.conf corresponds to a Security Server.

```
21 fwssd in.aftpd wait 0
80 fwssd in.ahttpd wait 0
513 fwssd in.arlogind wait 0
25 fwssd in.asmtpd wait 0
23 fwssd in.atelnetd wait 0
259 fwssd in.aclientd wait 259
10081 fwssd in.lhttpd wait 0
900 fwssd in.ahclientd wait 900
0 fwssd in.pingd respawn 0
0 fwssd in.asessiond respawn 0
0 fwssd in.aufpd respawn 0
0 vpn vpnd respawn 0
0 fwssd mdq respawn 0
0 xrm xrmd respawn 0 -pr
```

FIGURE 4-24 $FWDIR/conf/fwauthd.conf – example

<table>
<thead>
<tr>
<th>field number</th>
<th>meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>standard service’s port number</td>
</tr>
<tr>
<td>2</td>
<td>executable name</td>
</tr>
<tr>
<td>3</td>
<td>Security Server served by the executable</td>
</tr>
<tr>
<td>4</td>
<td>wait flag; wait or respawn = start again)</td>
</tr>
<tr>
<td>5</td>
<td>Security Server port number (0 = dynamically assigned)</td>
</tr>
<tr>
<td>6</td>
<td>SSL encryption; es = Client to FireWall Module, ec = FireWall Module to Server, ssl= both</td>
</tr>
</tbody>
</table>
The Security Service executables are listed in TABLE 4-7.

**TABLE 4-7 Security Service binaries**

<table>
<thead>
<tr>
<th>Service</th>
<th>binary name</th>
</tr>
</thead>
<tbody>
<tr>
<td>TELNET</td>
<td>bin/in.atelnetd</td>
</tr>
<tr>
<td>FTP</td>
<td>bin/in.aftpd</td>
</tr>
<tr>
<td>HTTP</td>
<td>bin/in.ahttpd</td>
</tr>
<tr>
<td>SMTP</td>
<td>bin/in.asmtpd</td>
</tr>
<tr>
<td>RLOGIN</td>
<td>bin/in.arlogind</td>
</tr>
<tr>
<td>client authentication</td>
<td>bin/in.aclientd  (This is not a Security Server.)</td>
</tr>
<tr>
<td></td>
<td>bin/in.ahclientd  (This is not a Security Server, but the executable for when a user initiates client authentication through a Web browser.)</td>
</tr>
<tr>
<td>logical servers</td>
<td>bin/in.lhttpd  (This is not a Security Server.)</td>
</tr>
</tbody>
</table>

The wait flag is always set to wait.

The Security Server port number is one of the following:

- 0 — specifies that VPN-1/FireWall-1 will choose a random high port for the Security Server
- positive value — specifies a real port number

If this option is chosen, the standard service's port number (the first field) should be the real port number for the service secured by this Security Server. For example, for Client Authentication this would be port 259.

- negative value — indicates that FireWall-1 randomly chooses multiple ports for the Security Server.

The absolute value indicates the number of random selected ports that will be chosen. The example below specifies that FireWall-1 will randomly select four high ports for the HTTP Security Server:

```
80  bin/in.ahttpd  wait -4
```

This option is especially useful for HTTP because it enables several HTTP Security Servers to run concurrently (see the following section, “Configuring Multiple HTTP Security Servers). If the client connects again before the Authorization Timeout...
specified in the Control Properties/Security Servers window, the same port will be chosen. If the client connects again after the Authorization Timeout, another port will be chosen.

Note - Configuring a negative port value is recommended only for gateway machines with more than one CPU. Configuring this option on a gateway machine with one CPU can result in a performance degradation.

Configuring Multiple HTTP Security Servers

You can modify the Security Server configuration to enable multiple HTTP Security Servers to run concurrently. Multiple HTTP clients connecting concurrently can be handled by several HTTP Security Servers.

Note - This option is recommended for gateway machines with more than one CPU. Using this option on a gateway machine with only one CPU will result in a performance degradation.

The file $FWDIR/conf/fwauthd.conf lists the Security Server executables and their assigned port numbers. The example line below shows the HTTP Security Server assigned to a dynamically allocated port:

```
80 fwssd bin/in.ahttpd wait 0
```

The last field indicates the Security Server port number.

A negative port value indicates that VPN-1/FireWall-1 randomly chooses multiple ports for the HTTP Security Server. The absolute value indicates the number of random ports that will be chosen. The number of random ports should correspond to the number of CPUs the gateway machine has.

The example below indicates that VPN-1/FireWall-1 will randomly select four high ports for the HTTP Security Server:

```
80 bin/in.ahttpd wait -4
```

According to the above example, an HTTP client will initially connect to one of four randomly selected ports. If the same client connects again before the Authorization Timeout specified in the Security Servers page of the Global Properties window, the same port will be chosen. If the same client connects again after the Authorization Timeout, another port will be chosen.

Another concurrent HTTP client will connect to one of the remaining free ports.
Running a Security Server on Different Ports

You run a Security Server on any port. The user starts the interactive service as usual, but instead of being immediately connected to the interactive service’s server (assuming the Rule Base allows such a connection), the user is first prompted for authentication data by the TELNET Security Server. If the authentication is successful, the user is then connected to the interactive service’s server in a normal session.

To do this, add a line in $FWDIR/conf/fwauthd.conf as follows:

```
port fwsd in.ateinetd wait 0
```

where `port` is the normal port for the service you wish to authenticate using the TELNET Security Server.
ClusterXL

ClusterXL is a software-based Load Sharing and High Availability solution for Check Point VPN-1/FireWall-1 enforcement points. The High Availability capability ensures that in the event that any individual gateway becomes unreachable, all connections are re-directed to a designated backup without interruption. The Load Sharing capability distributes traffic between clusters of redundant gateways so that the total throughput of multiple machines is increased. Load Sharing also provides High Availability functionality. Both capabilities require State Synchronization between cluster members.

- State Synchronization is described on page 243.
- High Availability and Load Sharing are described on page 250.

In This Chapter

- Installing and Licensing ClusterXL page 241
- State Synchronization page 243
- Check Point High Availability and Load Sharing Solutions page 250
- Configuring High Availability and Load Sharing page 255
- High Availability and Load Sharing Commands page 278
- Cluster Status Tools page 278

Installing and Licensing ClusterXL

ClusterXL is part of the standard VPN-1/FireWall-1 installation. In order to install a policy to a Cluster you must have a license for ClusterXL, in addition to the VPN-1/FireWall-1 license. Install a Central license on the SmartCenter Server with one of the following SKUs:

- CPMP-CXL-HA-1-NG (for a single cluster)
- CPMP-CXL-HA-U-NG (for an unlimited number of clusters)
ClusterXL must only be installed in a distributed configuration, in which the SmartCenter Server and the Cluster members are on different machines.

ClusterXL is currently available for Windows NT, Windows 2000, Solaris and Linux.
State Synchronization

Different cluster members running on different machines can synchronize their states, that is, they can share this information and can mutually update each other with the different states of the connections.

In High Availability and High Availability with Load Sharing configurations, this ensures that when a machine goes down, the other machines in the cluster are familiar with the exiting connection. These connections are kept alive, and the failover goes unnoticed by users.

State Synchronization is provided even for stateless protocols such as UDP and RPC. To do this, VPN-1/FireWall-1 on the cluster member creates a virtual state for such connections, and updates this state according to the data transferred. In addition, VPN-1/FireWall-1 maintains state information for Address Translation and Encryption.

In This Section

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full and Delta Synchronization</td>
<td>243</td>
</tr>
<tr>
<td>Secured Interfaces</td>
<td>244</td>
</tr>
<tr>
<td>Implementing Synchronization</td>
<td>244</td>
</tr>
<tr>
<td>Selective Synchronization</td>
<td>245</td>
</tr>
<tr>
<td>Different Routes for Connections (Asymmetric Routing)</td>
<td>246</td>
</tr>
<tr>
<td>Timing Issues</td>
<td>247</td>
</tr>
<tr>
<td>Synchronized Cluster Restrictions</td>
<td>248</td>
</tr>
<tr>
<td>Troubleshooting State Synchronization</td>
<td>249</td>
</tr>
</tbody>
</table>

Full and Delta Synchronization

The new NG synchronization architecture works in two modes:

**Full Synchronization**—Full Synchronization transfers all state information to a cluster member that has lost its state information. This may happen when a crashed cluster member recovers and wants to rejoin the cluster, or after stopping and starting the cluster member. Full Synchronization is used to recover a very large number of connections, and is handled by the fwd daemon using a TCP connection.

**Delta Synchronization**—Delta synchronization transfers small but frequent changes in state information between cluster members. This happens whenever a new connection passes through one of the members, or when encryption keys are negotiated by one of the members. Delta Synchronization is handled by the FireWall-1 kernel, using UDP broadcasts.
Secured Interfaces

Secured interfaces are distinct NICs which are used to pass sensitive clustering information between the cluster member.

An interface is considered secured if a connection through that interface can be trusted (for example, if the interfaces on the same network are connected with a cross cable or dedicated hub). Since an intruder is unable to send packets on that connection, a secured interface can be safely used to transmit synchronization and High Availability information.

In a High Availability configuration and a High Availability with Load Sharing configuration, each machine should have at least one secured interface. Additional secured interfaces are recommended for backup purposes.

The secured interface must be on the Synchronization network. The Synchronization network is used to pass state changes between the cluster members, and to install the Security Policy. The SmartCenter Server must therefore also be on the Synchronization network.

Implementing Synchronization

Synchronization in a cluster is performed over a dedicated synchronization network. The Synchronization network is used to pass sensitive information such as encryption keys and state of connections. It is therefore very important that the Synchronization network is secure.

FIGURE 5-1 illustrates synchronization in a network cluster.

FIGURE 5-1 Synchronization in a Gateway Cluster
To implement synchronization for Check Point and for OPSEC High Availability solutions:

1. Set up the synchronization network between the cluster members. Each interface in the synchronization requires a unique IP address. It is possible to set up more than one synchronization network. If the first network fails, the next one is used. Example synchronization network diagrams are shown in
   - FIGURE 5-5: “Legacy CPHA configuration” on page 258 and
   - FIGURE 5-4: “New CPHA and Load Sharing configuration” on page 256.

2. On the cluster members, ensure SVN Foundation is installed, and turn on the synchronization feature using the Check Point Configuration Tool High Availability tab or cpconfig menu option.

3. In the Policy Editor, define the cluster object, define a synchronization network object(s) if they are not already defined, and in the cluster object Synchronization page, add the synchronization network(s) to the cluster.

**Selective Synchronization**

In a state synchronized cluster, all state changes in one cluster member are normally sent to all other cluster members. If synchronization is found to affect gateway performance or increase congestion in the network, it is possible to reduce the amount of synchronization traffic by selecting the services to be synchronized.

Selective synchronization should only be used in

- High Availability, or
- High Availability with Load Sharing, in rules that do not have asymmetric routing.

DNS (over UDP) and HTTP may be good candidates for selective synchronization as they are typically responsible most of the connections, and on the other hand frequently have very short life and inherent recoverability in the application level.

Selective synchronization is implemented via the Service definition and is available for services of type TCP, UDP and Other (User Defined). Services of other types (Compound TCP, RPC, ICMP, Group and DCE-RPC) are always synchronized (if synchronization has been configured). By default, all services are synchronized.

One way of using selective synchronization is to define a new service based on an existing service. It is then possible to have both a synchronized service and a non-synchronized definition of a service, and to use them selectively in the Rule Base.
Choosing the Services to be Synchronized

1 Edit an existing TCP, UDP and Other (User Defined) service, or define a new service based on an existing service. It is then possible to use both the Synchronized Service and a non-Synchronized definition of the service, and to use them selectively in the Rule Base.

To edit an existing service, select Manage > Services... select the service and click Edit. In the Service Properties window, click the Advanced tab to display the Advanced Services Properties window (see FIGURE 5-2 for an example).

FIGURE 5-2 Advanced Services Properties window

Select or deselect one of the following check boxes:

- **Synchronize on cluster** — In a state-synchronized High Availability or Load Sharing gateway cluster, of the services allowed by the Rule Base, only those with Synchronize on cluster will be synchronized. By default, all new and existing services are synchronized.

- **Match for 'Any'** — In a Rule with Service ANY, in it, only those services that are defined as Match for 'Any' will match that rule.

Different Routes for Connections (Asymmetric Routing)

The IP protocol supports a network configuration in which packets sent from host A to host B may be routed through gateway C, while all packets sent from host B to host A may be routed through gateway D.
Although it is possible to use State Synchronization in order to implement different routes in and out of a network, the following situation may arise (illustrated in FIGURE 5-3):

Host A initiates a connection to the Host B through Gateway C. The reply comes back through Gateway D. If the reply had come through Gateway C, it would have been allowed because the connection is in Gateway C’s connection table. However, if the reply arrives at Gateway D before Gateway D has synchronized state information with Gateway C, then Gateway D will be unaware of connection, and will not handle these packets correctly.

Applications whose state is maintained in Security Servers (User Authentication and Resources) are not supported in an asymmetric routing configuration. This is due to the fact that Security Servers state is not synchronized between cluster members.

**Timing Issues**

Synchronized cluster members update each other with their state information at least every 100 milliseconds. Under load it occurs much more frequently.

The time on the synchronized cluster members must be within seconds of each other. You should install some software that keeps the time synchronized between the two machines. Under Solaris2, you can use `xntpd`.

If one of the cluster members goes down, the other cluster member may be unaware of connections initiated by the first cluster member in the 50 milliseconds before it went down. These connections will probably be lost.

**Synchronized Cluster Restrictions**

The following restrictions apply to synchronizing cluster members:
General

1) Only cluster members running on the same platform can be synchronized. For example, it is not possible to synchronize a Windows 2000 cluster member with a Solaris 8 cluster member.

2) The cluster members must be the same software version. For example, it is not possible to synchronize a VPN/FireWall Version 4.1 Module with a VPN/FireWall NG Module.

3) The cluster members must be managed by the same SmartCenter Server.

4) The cluster members must have the same Security Policy installed. For example, suppose one cluster member accepts FTP and the other rejects FTP. If an FTP connection is opened through the first cluster member, the reply packets returning through the second cluster member will be accepted because the FTP connection is in the connections table. This behavior is inconsistent with the Security Policy on the second cluster member.

Encryption

5) For information about state synchronization of encrypted connections, see Chapter 12, “Clustering Solutions for VPN Connections” of Check Point Virtual Private Networks.

User Authentication

6) A user-authenticated connection through a cluster member will be lost if the VPN/FireWall module on the cluster member goes down. Other synchronized cluster members will be unable to resume the connection. However, a client-authenticated connection or session-authenticated connection will not be lost.

The reason for these restrictions is that VPN-1/FireWall-1 user authentication state is maintained on Security Servers, which are processes, and thus cannot be synchronized on different machines in the way that data can be synchronized. However, the state of session authentication and client authentication is stored in kernel tables, and thus can be synchronized.

Resources

7) The state of connections using resources is maintained in a Security Server, so these connections cannot be synchronized for the same reason that user-authenticated connections cannot be synchronized.
Accounting

8) Accounting information is accumulated in each cluster member and reported separately to the SmartCenter Server, where the information is aggregated. In case of a failover, accounting information that was accumulated on the failed member but not yet reported to the SmartCenter Server is lost. To minimize the problem it is possible to reduce the period in which accounting information is “flushed”. To do this, in the cluster member object’s Logs and Masters > Additional Logging page, configure the attribute Update Account Log every:

Troubleshooting State Synchronization

To check that State Synchronization is active and working, proceed as follows:

Run the command line `fwctl pstat` on any cluster member and look for the state synchronization counters and indicators in the output, which are marked with `sync` (see example). These counters and indicators are gradually incremented and updated. If they do not exist, it is an indication that state synchronization is not active.

An example of the relevant part from `fwctl pstat` in a working environment:

```
sync new ver working
sync out: on sync in: on
sync packets sent:
total: 138 retransmitted: 0 retrans reqs: 0 acks: 3
sync packets received:
total 159 of which 0 queued and 0 dropped by net
also received 0 retrans reqs and 3 acks to 0 cb requests
```
Check Point High Availability and Load Sharing Solutions

In This Section

High Availability—Overview ........................................ page 250
Load Sharing—Overview ........................................... page 250
High Availability Modes ........................................... page 251
Improvements in Load Sharing .................................... page 252
When Does a Failover Occur? ....................................... page 252
What Happens When a Gateway Recovers? ................. page 253
VLAN Support ....................................................... page 253
How a Recovered Cluster Member Obtains the Latest Security Policy ........................................ page 253
Cluster Protocols ..................................................... page 254

High Availability—Overview
The ClusterXL High Availability capability provides the mechanism for detecting the failure of a VPN-1/FireWall-1 enforcement module defined as a cluster member, and for transparent fail-over to another cluster member.

When one of the cluster members stops functioning and another one takes its place, the second cluster member has the updated state of the first cluster member's connections, so the connections are maintained in a manner that minimizes the number of lost connections.

Cluster members are given a priority. The highest priority machine serves as the gateway in normal circumstances. If this machine fails, control is passed to the next highest priority machine. If that machine fails, control is passed to the next machine, and so on. Upon gateway recovery, it is possible to maintain the current active gateway, or to switch to a highest priority gateway.

Load Sharing—Overview
The ClusterXL Load Sharing capability enables the use of High Availability standby machines in a way that reduces the load on the network gateway, increasing throughput and performance. This is achieved by distributing the traffic load coming through the gateway between a number of machines in a cluster.

All High Availability capabilities are kept when the Load Sharing feature is used, so when a cluster member fails, the other cluster members distribute its traffic between themselves.
Every member of the cluster receives all the packets sent to the cluster IP address, using a hub or a switch with a multicast configuration, and each packet is distributed to a specific machine.

High Availability Modes

High Availability New CPHA Mode

When setting up a High Availability configuration from scratch and when moving to High Availability, New CPHA (Check Point High Availability) mode is recommended.

New CPHA uses the same topology as Load Sharing and the same cluster protocols. It is essentially the same as Load Sharing, except that it has a fixed 100% to 0% load split between the active and the other cluster members.

High Availability Legacy CPHA Mode

Legacy CPHA (Check Point High Availability) was the only available High Availability mode before NG FP3.

In a Legacy CPHA topology, the cluster members share IP and MAC addresses. The active cluster member receives all the packets sent to the cluster IP address, using a hub or a switch with a shared unicast configuration.

Benefits of New CPHA over Legacy CPHA

New CPHA has the following improvements over Legacy CPHA:

1) Network topology is easier to set up because all IP and MAC addresses in the cluster are unique.

2) Switching between Load Sharing and High Availability modes is simply a matter of clicking a button in the Policy Editor Cluster object. It does not requires changes to the network topology.

3) Remote management by the SmartCenter Server of Check Point Gateways on the internet is possible.

4) In Legacy CPHA, if the cluster member defined as the Default Gateway goes down, the SmartCenter Server can no longer manage other gateways. In New CPHA this is not the case because the Default Gateway of the Management is defined as the IP address of the cluster itself, rather than one of the cluster members.
Improvements in Load Sharing

Routable IP addresses can be hard to obtain. As of NG FP3, New CPHA and Load Sharing configurations require fewer routable IP addresses. In Load Sharing prior to NG FP3, the external cluster IP address and the IP addresses of the cluster member external interface had to be on the same network, and had to be routable. From NG FP3, the external cluster IP address can be on a different network than the external member network, and need not be routable. In a two member cluster, this saves two routable IP addresses.

Another improvement is that multicasting is used in the Cluster Control Protocol between the cluster members, which significantly reduces network traffic as compared to the broadcasts used prior to NG FP3.

When Does a Failover Occur?

A “failover” describes the situation when the active cluster member is no longer active and another cluster member becomes active in its place. A failover takes place when one of the following occurs on the active cluster member:

- Any device (such as fwd) specified with the cphaprob command fails.
- An interface or cable fails.
- The machine crashes.
- The Security Policy is uninstalled.

Initiating Failover

The state of a cluster member can be manually controlled in order to take down the cluster member, and initiate failover to the next highest priority cluster member.

To manually control the status of a cluster member, in the Status Manager:

- Right click a cluster member, and select DOWN to run the cpha stop command on the machine.
- Click UP to run the cpha start command on the machine.
What Happens When a Gateway Recovers?

When the VPN-1/FireWall-1 Gateway Modules are synchronized, if one Gateway Module goes down, another Gateway becomes active and “takes over” the connections of the failed Gateway. When the failed Gateway recovers, the recovery method depends on the configured cluster setting. The options are:

- **Maintain Current Active Gateway** — If the primary machine passes on control to the secondary machine, control will be returned to the primary machine only if the secondary machine fails.

- **Switch to higher priority Gateway** — If the secondary machine has control and the primary machine is restored, then control will be returned to the primary machine.

VLAN Support

VLANs (Virtual LANs) are supported by VPN-1/FireWall-1 and ClusterXL. A packet that originates in a VLAN is tagged by the switch with a 4 byte header which specifies which switch port it came from. No packet is allowed to go from one switch port to another, apart from ports (“global” ports) that are defined so that they belongs to all the VLANs. The VPN-1/FireWall-1 cluster member machine is connected to the global port, and this logically divides a single physical VPN-1/FireWall-1 port into many VLAN ports.

How a Recovered Cluster Member Obtains the Latest Security Policy

The administrator installs the security policy on the cluster rather than separately to individual cluster members. The policy is automatically installed on all cluster members.

When a failed cluster member recovers, it will first try to take a policy from one of the other cluster members. The assumption is that the other cluster members have a more up-to-date policy. If this does not succeed, it compares its own local policy to the policy on the SmartCenter Server. If the policy on the SmartCenter Server is more up-to-date than the one on the cluster member, the policy on the SmartCenter Server will be fetched. If the cluster member does not have a local policy, it fetches one from the SmartCenter Server.

This process differs from the NG FP2 process. In NG FP2, when a gateway comes up, it does not look for a policy on other cluster members. It just compares its own local policy to the policy on the SmartCenter Server. If the policy on the SmartCenter Server is more up-to-date than the one on the cluster member, the SmartCenter Server policy will be fetched. If the cluster member does not have a local policy, it fetches one from the SmartCenter Server.
Cluster Protocols

There is constant Cluster Control protocol traffic between the cluster members. This allows members to report their own states and learn about the states of other members. This way, when a certain member reports a problem or is not responding to other members queries, a failover occurs and the traffic is handled by another member.

In Load Sharing, multicast is used between the cluster members, which significantly reduces network traffic as compared to the broadcasts used up to NG FP2.

Both New CPHA and Load Sharing use the same network topology and the same cluster protocol. This makes it very easy to switch back and forwards between these cluster modes. High Availability is essentially the same as Load Sharing with a 100% to 0% load split between cluster members.

TABLE 5-1 summarizes the protocols used by the three cluster modes. They are all Layer 2 protocols.

TABLE 5-1  Cluster Protocol Summary

<table>
<thead>
<tr>
<th>Cluster Mode</th>
<th>Cluster Control Protocol between members</th>
<th>Communication outside cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>Load Sharing</td>
<td>Multicast</td>
<td>Multicast</td>
</tr>
<tr>
<td>New CPHA</td>
<td>Multicast</td>
<td>Unicast</td>
</tr>
<tr>
<td>Legacy CPHA</td>
<td>Broadcast</td>
<td>Shared unicast</td>
</tr>
</tbody>
</table>

Within the cluster, the Cluster Control Protocol works on UDP port 8116 in all modes.
Configuring High Availability and Load Sharing

In This Section

- Example New CPHA and Load Sharing Topology
- Example Legacy CPHA Topology
- Moving from a Single Enforcement Module to Load Sharing or New CPHA
- Configuring Load Sharing or New CPHA from Scratch
- Moving Between New CPHA and Load Sharing
- Moving from Legacy CPHA to New CPHA or Load Sharing
- Configuring Legacy CPHA from Scratch
- Upgrading a Check Point High Availability Cluster
- Third Party Load Sharing Considerations
- Upgrading a Third Party cluster
- Adding Another Member to an Existing Cluster
- Moving from Load Sharing or New CPHA to Legacy CPHA
- Multicast Switch Settings for Load Sharing
- ClusterXL Advanced Settings

Example New CPHA and Load Sharing Topology

New CPHA and Load Sharing use the same network topology.

Each cluster member has an IP address for the cluster member itself, and an IP address for each interface. In addition, unique IP addresses are defined for the cluster itself and each of its interfaces.

Note: Always distinguish carefully between the cluster and the cluster members. Cluster members are defined within the cluster object, but each have their own properties.

FIGURE 5-4 shows an example network configuration for implementing Load Sharing between two enforcement modules in a cluster.
Defining the Cluster IP Addresses

The IP addresses of the cluster itself are different than the IP addresses of the cluster members. In FIGURE 5-4, the IP address of the cluster is 172.20.10.100, and this is the only legal IP address in the cluster.

The cluster has two interfaces. The external interface IP address is 172.20.10.100, and the internal interface IP address is 192.168.0.100.

A member network is a subnet on which the physical interfaces of the cluster members reside. All cluster member physical interfaces pointing in the same direction must be on the same member network.

By default, a member network of cluster member interfaces in a given direction is the same subnet on which the cluster interface resides. In this example, the cluster external interface IP address is not in the same subnet as the external member network. Because of this, the cluster interface in that direction must be explicitly associated with the cluster member network in the same direction (in the Policy Editor, Gateway Cluster Properties > Topology > Interface Properties window, General tab and Member Network tab).

Defining the Cluster Member IP addresses

The guidelines for configuring each cluster member machine are as follows:

- All machines within the cluster must have at least three interfaces:
  - an interface facing the external cluster interface, which in turn faces the internet
  - an interface facing the internal cluster interface, which in turn faces the internal network
  - an interface to use for synchronization
All interfaces pointing in a certain direction must be on the same network. For example, the interfaces facing the internet from each of the members must all be on the same network.

In this configuration, there are two cluster members, Member_A and Member_B, each with three interfaces, as follows:

- an interface with an illegal IP address facing the internet through a hub or a switch. This is the EXT interface with IP address 10.0.1.1 on Member_A and 10.0.1.2 on Member_B. This is the interface that the cluster external interface sees. Both these interfaces are on the same network.

- an interface facing the local network through a hub or a switch. This is the INT interface with IP address 192.168.0.1 on Member_A and 192.168.0.2 on Member_B. This is the interface that the local network sees. Both these interfaces are on the same network.

- an interface that is secured, for use with synchronized and protocol-sensitive information, and for installing the Security Policy. This is the SYNC interface with IP address 10.0.10.1 on Member_A and 10.0.10.2 on Member_B. This is the interface used to exchange synchronization information, and to install the Security Policy. Both these interfaces are on the same network.

Example Legacy CPHA Topology

Legacy CPHA is the High Availability Cluster mode that was available up to VPN-1/FireWall-1 NG FP2. When setting up a High Availability configuration for the first time, New CPHA is recommended.

FIGURE 5-5 shows an example network configuration for Legacy CPHA.
Defining the Cluster IP Addresses

In a Legacy CPHA configuration, the cluster IP address is the same routable non-unique IP address as the cluster IP external interface facing the internet, and is the same IP address that the cluster members share on their external interface.

The cluster internal interface IP address is the same IP address that the cluster members share on their interface addresses.

Note - Always distinguish carefully between the cluster and the cluster members. Cluster members are defined within the cluster object, but each have their own properties.

Defining the Cluster Member IP addresses

The guidelines for configuring each cluster member machine are as follows:

- All the IP addresses in the cluster may be non-routable.
- Interfaces that share the same IP address must also share the same MAC address.
- The machines must be protected; for example, anti-spoofing must be enabled on all interfaces.
- If the Legacy CPHA machines are synchronized, there must be a secure dedicated link between all the machines.
The IP address of each of the cluster members must be defined as the unique address facing the SmartCenter Server.

In this configuration, there are two cluster members: Member_A (the primary) and Member_B (the secondary) each with at least three interfaces, as follows.

- an interface with a unique IP address, facing the SmartCenter Server. This is the SYNC interface, with IP address 10.0.10.1 on Member_A and 10.0.10.2 on Member_B.

This is the interface that the SmartCenter Server sees. Because the SmartCenter Server must be able to download a Security Policy to both cluster members, the SYNC interface on each cluster member have a unique IP address so that the SmartCenter Server can “see” them both at any given time. The SYNC interface addresses must be routable, for system maintenance purposes. This IP address could be a dedicated Network Interface Card (NIC), but may also be the synchronization network interface IP address (the synchronization NIC).

The Check Point cluster members will trust critical messages coming from these networks. This means that those networks must be part of a dedicated sub-network connected by either a hub, cross-cable or a separate switch VLAN. It is possible to define more than one synchronization network for backup in case the first network fails for any reason.

- an interface with a non-unique IP address, facing the internet through a hub or switch. This is the EXT interface, with IP address 172.20.10.1 on both Member_A and Member_B.

This is the interface that the outside world sees. Because there are two interfaces (one on each cluster member) with the same IP (and MAC) address, only one of them can be active (that is, the outside world can see only one of them) at any given time. This is also the IP address defined for the cluster object.

- an interface with a different non-unique IP address, facing the local network through a hub or switch. This is the INT interface, with IP address 192.168.0.1 on both Member_A and Member_B.

This is the interface that the local network sees. Because there are two interfaces (one on each cluster member) with the same IP address, only one of them can be active (that is, the local network can see only one of them) at any given time. There can be any number of local networks, each of which is connected to both cluster members on interfaces that share the same non-unique IP address (but each local network shares a different non-unique IP address).
Moving from a Single Enforcement Module to Load Sharing or New CPHA

This procedure describes how to change from a single VPN-1/FireWall-1 enforcement module (machine ‘A’), to a Load Sharing configuration with two cluster members. Machine ‘A’ becomes cluster member ‘A”, and the new machine becomes cluster member, ‘B’. This explanation refers to the example configuration in FIGURE 5-4: “New CPHA and Load Sharing configuration” on page 256.

The procedure ensures that FireWall downtime is kept to a minimum.

The external and internal IP addresses of machine ‘A’ will become the cluster IP addresses so that the routing configuration does not change. The two cluster members will use other IP addresses.

1. Obtain and install a Central license for ClusterXL on the SmartCenter Server.

2. Configure the switches as described in “Multicast Switch Settings for Load Sharing” on page 275. Machine A should already be connected to the switches.

3. Set up machine B by assigning IP addresses for all the machine interfaces, for example the internal, external, and the synchronization interfaces (refer to FIGURE 5-4 and to the specific IP addresses of machine B). Note that these are the machine addresses, not the cluster addresses.

4. Connect the new cluster members (B) to the switches.

5. Install VPN-1/FireWall-1 on machine B. During the configuration phase, enable ClusterXL/State Synchronization. Enable ClusterXL/State Synchronization each cluster member.

6. Using the Policy Editor, define the cluster object. In the General tab of the Cluster object, check ClusterXL as a product installed on the cluster. The general IP address of the cluster is the routable external IP address of the cluster (in the example, the external routable IP address of A). The cluster can have several other IP addresses (e.g. internal and DMZ interfaces). Initialize SIC for the cluster.

7. In the Cluster Members page, add all cluster members other than A (the original FireWall machine) to the cluster (only B in the example). Cluster members exist solely inside the cluster object. For each cluster member,
   - initialize SIC (in the Cluster Members Properties > General tab),
   - define all interfaces (in the Topology tab, see FIGURE 5-6), and
   - define all Certificate properties if any (in the VPN tab).
Moving from a Single Enforcement Module to Load Sharing or New CPHA

8 In the ClusterXL page, select either Load Sharing, and define the logging method or check New CPHA specify the action Upon Gateway Recovery, and define the Failover Tracking method (FIGURE 5-7)

FIGURE 5-7 ClusterXL page
9 Define a synchronization network object(s) if they are not already defined, and in the Synchronization page, add the synchronization network(s) to the cluster (FIGURE 5-7).

If you do not use State Synchronization, existing connections will be closed when failover occurs. If you choose not to use this feature, deselect Use State Synchronization and skip to the next step.

FIGURE 5-8 Synchronization page

10 Define the cluster topology on each cluster interface. First, in the Topology >Add General tab, define the Cluster IP addresses, and in the Topology tab, define the topology and set up antispooing.

11 Next, on each cluster interface, define the member networks if necessary. You need to define member networks if the subnets on which the physical interfaces of the cluster members reside, are different than the subnets of the cluster interfaces. By default, the member networks are the subnets on which the physical interface of the cluster members reside. In the Member Networks tab, associate the cluster IP addresses in a given direction with the IP addresses of the member networks in the same direction (FIGURE 5-9).
12 Define the other pages in the cluster object as required (NAT, VPN, Remote Access, etc.)

13 Install the Security Policy on the cluster.

14 Disconnect ‘A’ from the network, to avoid IP conflicts.
In the Policy Editor, install the policy on the cluster. The policy will not be installed on machine ‘A’.
At this point, the existing connections through A will be closed and new connections will be opened through other gateways in the cluster.

On machine A, run the `cpeconfig` command to activate the configuration tool, and enable ClusterXL/State Synchronization.

Change the IP address of ‘A’ as needed. For example, assign IP addresses for the internal, external, and the synchronization interfaces.

Using the Policy Editor, delete the Gateway object for “A”, and re-create it inside the cluster, as a cluster member.

Reconnect ‘A’ to the switches from which it was removed.

Using the Policy Editor, install the policy on the entire cluster.

**Configuring Load Sharing or New CPHA from Scratch**

This procedure describes configure Load sharing or New CPHA from scratch. This explanation refers to the example configuration in FIGURE 5-4: “New CPHA and Load Sharing configuration” on page 256.

1. Obtain and install a Central license for ClusterXL on the SmartCenter Server.
2. Define IP addresses for each interfaces on all cluster members.
3. Connect the machines to the network.
4. For Load sharing configuration, Configure the switches as described in “Multicast Switch Settings for Load Sharing” on page 275
5. Install VPN-1/FireWall-1 on all cluster members. During the configuration phase, enable ClusterXL/State Synchronization.
6. Using the Policy Editor, define the cluster object. In the General tab of the Cluster object, check ClusterXL as a product installed on the cluster. The general IP address of the cluster is the routable external IP address of the cluster (in the example, the external routable IP address of A). The cluster can have several other IP addresses (e.g. internal and DMZ interfaces). Initialize SIC for the cluster.
7. In the Cluster Members page, add all cluster members to the cluster. Cluster members exist solely inside the cluster object. For each cluster member,
   - initialize SIC (in the Cluster Members Properties > General tab),
   - define all interfaces (in the Topology tab, see FIGURE 5-6), and
• define all Certificate properties if any (in the **VPN** tab).

**FIGURE 5-11** Cluster Member B Topology

8 In the **ClusterXL** page, select either **Load Sharing**, and define the logging method or check **New CPHA**, specify the action **Upon Gateway Recovery**, and define the **Failover Tracking** method (**FIGURE 5-7**).

**FIGURE 5-12** ClusterXL page

9 Define the other pages in the cluster object as required (**VPN**, **LDAP**, **Authentication**, **Log Servers**, etc.)
10 Define a synchronization network object(s) if they are not already defined, and in the **Synchronization** page, add the synchronization network(s) to the cluster (FIGURE 5-7).

If you do not use State Synchronization, existing connections will be closed when failover occurs. If you choose not to use this feature, deselect **Use State Synchronization** and skip to the next step.

**FIGURE 5-13** Synchronization page

11 Define the cluster topology on each cluster interface. First, in the **Topology > Add General** tab, define the Cluster IP addresses, and in the **Topology** tab, define the topology and set up antispoofing.

12 Next, on each cluster interface, define the member networks if necessary. You need to define member networks if the subnets on which the physical interfaces of the *cluster members* reside, are different than the subnets of the *cluster* interfaces. By default, the member networks are the subnets on which the physical interface of the cluster members reside. In the **Member Networks** tab, associate the cluster IP addresses in a given direction with the IP addresses of the member networks in the same direction (FIGURE 5-9).
13 Define the other pages in the cluster object as required (NAT, VPN, Remote Access, etc.).

14 Install the Security Policy on the cluster.

**FIGURE 5-15** Installing a Policy on a cluster
Moving Between New CPHA and Load Sharing

To move between New CPHA and Load Sharing

1. In the Policy Editor, in the ClusterXL tab of the cluster object, click
   - either **High Availability > New CPHA**, specifying the action **Upon Gateway Recovery**,
   - or **Load Sharing**.


3. If moving from Load Sharing to New CPHA — reconfigure the switches by deleting the multicast static ARP entries for the cluster IP addresses on the switch or router.
   If moving from New CPHA to Load Sharing — reconfigure the switches by adding the multicast static ARP entries for the cluster IP addresses on the switch or router (see “Multicast Switch Settings for Load Sharing” on page 275).

Moving from Legacy CPHA to New CPHA or Load Sharing

There are 2 ways to move a legacy mode CPHA cluster to a new mode HA or to a load-sharing cluster. The Minimal Effort version emphasizes a simple and relatively quick process during which the cluster will stop processing packets, while the Minimal Downtime focuses on minimal cluster downtime, though the process is more tedious.

**Minimal Effort Configuration**

This procedure describes how to move from legacy HA mode of ClusterXL to Load Sharing or to new HA mode of ClusterXL. The consideration for this is simplicity of configuration, rather than the minimal downtime.

**Configuring the Cluster Members**

1. Run `cpstop` on all members; all network connectivity will be lost.

2. Reconfigure the IP addresses on all the cluster members, so that instead of the shared /duplicate IP addresses there will be unique IP addresses.

3. Remove the shared MAC addresses by executing the command `cphaconf uninstall_macs`.

4. On window platforms — reboot the modules.

5. On UNIX/Linux platforms — execute `cpstart`
**Configuring the Management**

1. In SmartMap, open the cluster object. Under the “ClusterXL” tab, change the cluster mode from “Legacy mode” to “new mode” or to “Load sharing mode”.

2. On the cluster members tab of the cluster, for each cluster member, re-fetch the interfaces (which have changed since the IP addresses were changed). The interfaces which were previously used as “shared” interfaces should now be marked on the topology as “Cluster interfaces”.

3. On the cluster object, in the Topology tab, define the cluster IPs of the cluster. Define the cluster interfaces names. They will be bound to physical interfaces according to the IP addresses. If the new IP addresses of the cluster members on a specific interface reside on different subnet then the cluster IP in this direction, the cluster members’ network should be defined in the “members network” fields of the cluster interface.

4. Install the policy on the new cluster object (Security policy, QOS policy etc’).

**Minimal Downtime Configuration**

This procedure describes how to move from Legacy HA mode of ClusterXL to new HA mode or to Load Sharing mode. The shared internal and external interfaces will become the cluster interfaces. The cluster members will need additional IP addresses that must be prepared in advance. The procedure will move a configuration like the one in figure 3.6 to a configuration like the one in figure 3.5, while minimizing the downtime of the cluster.

If downtime of the cluster during the change is not a major issue, it is recommended to proceed according to the easier process, as mentioned above.

1. Make sure you have all the IP addresses needed for this change.

2. During the change you will need to delete and recreate the objects in the policy editor. Please backup your configuration before you start this process.

The starting point is when machine ‘A’ is active, and machine ‘B’ is standby.

3. Disconnect machine ‘B’ from all interfaces except the interface connecting it to the management (the management interface).

4. Run `cphastop` on machine ‘B’

5. Change the IP addresses of machine ‘B’ (as required by the new configuration)

6. Reset the MAC addresses on machine ‘B’ by executing `cphaconf uninstall_macs`

7. Windows machine need to be rebooted for the MAC address change to take affect.
8 In the Policy Editor, delete cluster member ‘A’ from the cluster by deleting it in the Cluster object, in the “cluster members” tab.

9 Define the topology of cluster member ‘B’ by pressing “get topology” in the cluster member object’s topology tab. Make sure to mark the appropriate interfaces as “cluster interfaces”

10 Define the new topology of the cluster (define the cluster interfaces in the cluster’s topology tab) on the cluster object.

11 In the “ClusterXL” tab, change the cluster mode from “Legacy mode” to “New mode” or to “Load Sharing” mode.

12 Verify that the other pages in the cluster object (NAT, VPN, Remote access etc.) are correct. In Legacy HA mode of ClusterXL the definitions used to be per cluster member, while now they are on the cluster itself.

13 Install the policy on the cluster (now contains only cluster member ‘B’)

14 Reconnect machine ‘B’ to the networks (from which you disconnected them in step 1).

15 If the cluster consists of more then two members, repeat steps 1-10 for each of them.

16 For Load Sharing mode, configure the switches as described in the “Multicast switch settings for Load Sharing”

17 Disconnect machine ‘A’ from the all networks accept the management network. (The cluster will now stop processing traffic)


19 On machine ‘B’ run cpstop and then cpstart (if there are more the two machines, run these commands on all machines accept ‘A’)

20 Machine ‘B’ should now become active and start processing traffic.

21 Change the IP addresses of machine ‘A’ (as required by the new configuration).

22 Reset the MAC addresses of machine ‘A’

23 Windows machine need to be rebooted for the MAC address change to take affect.

24 In the Policy Editor, recreate cluster member ‘A’ in the “cluster members” tab of the cluster object.

25 Reconnect machine ‘A’ to the networks from which it was disconnected.

26 Install the security policy on the cluster.
27 On machine ‘A’, run \texttt{cpstop} and then \texttt{cpstart}

28 The cluster should now work in the new mode.

**Configuring Legacy CPHA from Scratch**

See Figure 5-5, “Legacy CPHA configuration,” on page 258 for an example configuration.

1 Obtain and install a Central license for ClusterXL on the SmartCenter Server.

2 Define the same IP address for each machine participating in the Legacy CPHA configuration, only for the interfaces that will be shared. You must define the IP addresses before connecting the machines into the Legacy CPHA topology, because the sharing of MAC addresses requires that the shared IP addresses be configured. To avoid network conflicts, proceed as follows:

   a Make sure that each network (internal, external, Synchronization, DMZ, etc.) is connected to a separate VLAN, switch or hub. No special configuration of the switch is needed.

   b Disconnect the machines participating in the Legacy CPHA configuration from the hub/switch.

   c Define the IP addresses.

3 Install the same version (and build number) of VPN-1/FireWall-1 on each cluster member. During the configuration phase, enable ClusterXL/State Synchronization. Do NOT reboot the machines after the configuration.

4 Reconnect the machines participating in the Legacy CPHA configuration to the hub/switch. Make sure you connect the configured interfaces to the matching physical network outlet.

5 Reboot the cluster members. MAC address configuration will take place automatically.

6 Using the Policy Editor, define the cluster object. In the **General Properties** page of the Cluster object, assign the routable external IP address of the cluster as the general IP address of the cluster. Check **ClusterXL** as a product installed on the cluster.

7 In the **Cluster Members** page, add all cluster members to the cluster. Cluster members exist solely inside the cluster object. For each cluster member,

   • initialize SIC (in the **Cluster Members Properties > General** tab),
   • define all interfaces (in the **Topology** tab, see FIGURE 5-6), and
• define all Certificate properties if any (in the VPN tab).

8 In the ClusterXL tab, check Legacy CPHA, specify the action Upon Gateway Recovery, and define the Fail-over Tracking method.

9 Define a synchronization network object(s) if they are not already defined, and in the Synchronization page, add the synchronization network(s) to the cluster.

If you do not use State Synchronization, existing connections will be closed when failover occurs. If you choose not to use this feature, deselect Use State Synchronization and skip to the next step.

10 Define the other pages in the cluster object as required (NAT, VPN, Remote Access, etc.).

11 Install the Security Policy on the cluster.

12 On Windows platforms, reboot all the cluster members in order to activate the MAC address configuration.

**Automatic MAC address configuration**

Check Point High Availability solution is based on several machines using the same IP address and MAC address. The configuration of the IP addresses is a preliminary step which must be taken before configuring the High Availability (see step c on page 271). The MAC addresses of the shared interfaces are configured automatically on all platforms. The shared MAC address (which will be configured on each machine) is usually, but not necessarily, the MAC address of the first configured machine i.e. the machine that was the first to be installed or the first to be upgraded.

On Solaris and Linux the MAC address assignment is performed transparently after the policy installation.

On Windows NT and Windows 2000, every machine whose MAC address has been changed should be rebooted. To upgrade an existing cluster, proceed as follows:

1 Perform steps 1-11 of the procedure described in “Configuring Legacy CPHA from Scratch” on page 271.

2 Reboot every machine except A.

3 Finish the upgrade.

Installing a new cluster is similar to upgrading clusters (see “Configuring Legacy CPHA from Scratch” on page 271) except that the SmartCenter Server and cluster members should be installed, not updated.
Upgrading a Check Point High Availability Cluster

Assume you have a cluster of several VPN-1/FireWall-1 machines (marked A, B and C in this example) with any version from 4.1 to NGFP3.

The upgrade stage is divided into three parts:

1. Upgrade the SmartCenter Server.
2. Upgrade all but one of the cluster members.
3. Upgrade the last cluster member.

**Upgrading the SmartCenter Server**

1. Upgrade the SmartCenter Server exactly as you upgrade a normal Check Point distributed installation (see *SmartCenter User Guide*).
2. When upgrading from a 4.1 cluster, configure the synchronization network in the synchronization tab, and the cluster mode in the ClusterXL tab.

**Upgrade All But One of the Cluster Members**

1. When cluster member A is the active member, and members B and C are standby members. In Load Sharing mode – choose randomly one of the cluster members, which will be upgraded last. Upgrade cluster members B,C either directly or using SmartUpdate (see *SmartCenter User Guide*).
2. When upgrade of B, C is finished, reboot both of them.
3. When machines B,C are up again, In the SmartDashboard, change the cluster version to FP3, and re-establish SIC with the upgraded cluster members (B and C). Uncheck the “On Gateway clusters, install on all members, if it fails do not install at all” checkbox. Install the security policy on the cluster. The policy will be successfully installed on cluster members B and C, and will fail on member A.
4. The status manager should show the status of cluster member A as “Active”, and the other cluster members as “Ready”.
5. Execute “cphastop” on cluster member A. At this point machines B and/or C will start processing traffic (depending on whether this is a Load Sharing or HA configuration).

**Upgrade the Last Cluster Member**

6. Upgrade cluster member A, using SmartUpdate or directly (see *SmartCenter User Guide*).
7. Reboot cluster member A.

Chapter 5   ClusterXL   273
8 Install the policy on the entire cluster.

**Third Party Load Sharing Considerations**
When working with a third party load sharing solution that uses asymmetric
cornections between cluster members, you must edit the property
`use_limited_flushnack` on the SmartCenter Server and change it to `TRUE`. Edit the
property using the dbedit graphical database editor.

This applies in particular for VPN and NAT connections.

If the third party solution assures connection stickiness (symmetric connections), it is
recommended not to change this property, in order to gain the highest cluster
performance.

**Upgrading a Third Party Cluster**

1 Upgrade the SmartCenter Server exactly as you would have upgraded a normal
Check Point distributed installation (see *SmartCenter User Guide*).

2 When upgrading from a 4.1 cluster, configure the synchronization network in the
synchronization tab, and the cluster mode in the Availability mode tab. (either HA
or Load Sharing third party product)

3 Follow the directions specified by the third party vendor as to how to upgrade the
cluster members.

4 Install the security policy to the cluster.
The new member is now part of the cluster.

**Adding Another Member to an Existing Cluster**
In order to add an additional cluster member to an existing cluster, proceed as follows:

1 On the cluster member, enable ClusterXL using `cpconfig`.

2 Change the IPs of the new cluster member to reflect the correct topology (either
shared IPs or unique IPs, depending on the clustering solution)

3 Make sure all needed CP products are installed on the new member.

4 In the Policy Editor, on the cluster member’s tab, either create a new cluster
member (if it is a new FireWall-1 machine) with the appropriate properties, or
convert an existing Gateway to a cluster member.

5 If this is a new FireWall-1 machine, make sure SIC is initialized, and that the
topology is correctly defined.
If the cluster mode is “Load Sharing” or “New HA”, make sure the proper interfaces on the new cluster member are configured as “cluster interfaces”.

Moving from Load Sharing or New CPHA to Legacy CPHA

This procedure describes how to change from a Load Sharing or New CPHA configuration (as in FIGURE 5-4) to a Legacy CPHA configuration (as in FIGURE 5-5). The external and internal interface IP addresses of one of the cluster members will become the shared external and internal IP addresses for all cluster members.

1. Disconnect ‘B’ from the external switch/hub.
   If there are more than two members in the cluster, disconnect each from the switch/hub, so that only one machine (‘A’) is connected.

2. Configure the shared interfaces of the disconnected cluster members (‘B’) so that they have the IP addresses of the cluster.

3. In the Policy Editor, in the ClusterXL page of the Gateway Cluster Properties window of the cluster object, change the Cluster Mode to Legacy CPHA.

4. In the Cluster Members page, delete cluster member ‘A’ from the cluster.

   The Policy will not be installed on cluster member ‘A’.

6. Connect ‘B’ to the same switches as ‘A’.
   If there are more than two cluster members, each should be connected to the same switches as ‘A’.

7. Disconnect ‘A’ from the external switch/hub.

8. If moving from Load sharing to Legacy CPHA, reconfigure the switches by deleting the multicast static ARP entries for the cluster IP addresses on the switch or router.

9. Configure the interfaces of ‘A’ so that they have the IP addresses of the cluster.
   All current connections will be closed and then reopened on ‘B’.

10. Using the Policy Editor, in the cluster object Cluster Members page, recreate cluster member ‘A’ and add it to the cluster.

11. Verify that the pages of the other cluster members (NAT, VPN, Remote Access, etc.) are correct. In New CPHA and Load Sharing these definitions are per cluster, while in Legacy CPHA the definitions are per cluster member.

12. Install the Security Policy.
13 Reconnect ‘A’ to the switch/hub from which it was removed.

In Windows NT and 2000, you will be required to reboot machine ‘A’ in order to complete the MAC address configuration.

**Multicast Switch Settings for Load Sharing**

Make sure that the used switches and routers meet the ClusterXL requirements. For a list of supported hardware devices, and for their configuration instructions, see SecureKnowledge solution sk10621 (Login at http://support.checkpoint.com/login.html and enter the solution ID in the SecureKnowledge Search by Keyword(s) window).

Make sure that each network (internal, external, Synchronization, DMZ, etc.) is configured on a separate VLAN, switch or hub.

Multicast is used to pass all packets to all cluster members. Switches must be configured to forward multicast packets to the correct ports.

There are 2 recommended ways to set a switch:

1) Forward all multicast packets seen by the switch to all cluster member ports.

2) Forward only multicast packets with the destination MAC address that appears in the *Advanced* window (see FIGURE 5-17 on page 278), to the cluster member ports.

**ClusterXL Advanced Settings**

**Setting the Load Sharing Packet Distribution Method**

The Sharing Method Configuration option enables decreased packet distribution between the cluster members.

By default, packets are distributed among cluster members based on IP addresses, ports and IPSec SPIs, resulting in maximum distribution.

In some cases, however, an application may require a few connections to go through a specific cluster member. In such cases, you may wish to decrease the distribution of packets in order to increase the probability that a certain connection will pass through a single cluster member on both inbound and outbound directions. This is done by choosing a more “sticky” sharing method.

To change sharing method, in the *Gateway Cluster Properties* window, *ClusterXL* page, select *Load Sharing*, and then click *Advanced*.

The *Advanced Load Sharing Configuration* window will be displayed (FIGURE 5-16).
Select one of the following sharing configurations:

- **IPs, Ports, SPIs (default)** — This option provides the best sharing distribution, and is recommended for use. It is the least “sticky” sharing configuration.

- **IPs, Ports** — This option should be used only if problems arise when distributing IPSec packets to a few machines although they have the same source and destination IP addresses.

- **IPs** — This option should be used only if problems arise when distributing IPSec packets or different port packets to a few machines although they have the same source and destination IP addresses. It is the most “sticky” sharing configuration, in other words, it increases the probability that a certain connection will pass through a single cluster member on both inbound and outbound directions.

### Setting the Default Load Sharing Multicast MAC Address

It is possible to change the MAC address used for Multicast, and replace it with a user-defined MAC address in the event that another application on the network happens to be using the same multicast IP address.

This situation is rare, and it is not recommended to change the default MAC address for any other reason.

If you do choose to use a user defined MAC address, it must be of the form

\[01:00:5e:xx:yy:yy\]

where \(x\) is between 0 and 7 and \(y\) is between 0 and \(f\) (hex).
To change the MAC address, in the **Gateway Cluster Properties > Topology** page, select the cluster interface and click **Edit**. In the **Interface Properties** window **General** tab, click **Advanced** (FIGURE 5-17). Click **User defined**, and carefully type the new MAC address.

**FIGURE 5-17** Load Sharing Interface Properties—Advanced window

---

**Setting Disconnected Interfaces**

You can make ClusterXL ignore certain interfaces. To do so, edit the file `$FWDIR/conf/discntd.if` by adding the interfaces’ names separated by new line characters.

On Windows NT or Windows 2000, use `regedt32`, and create the value `HKLM\system\currentcontrolset\services\cpha\DisconnectedInterfaces` of type **REG_MULTI_SZ**. When more than one interface should be disconnected, write an interface per line.

---

**High Availability and Load Sharing Commands**

For high Availability and Load sharing commands, see “ClusterXL: High Availability and Load Sharing” on page 611 of the **Check Point SmartCenter Guide**.

---

**Cluster Status Tools**

**To Verify that Load Sharing Works Properly**

To verify that the Load sharing works properly. Either

- Use the Status Manager to check that all the machines are in Active state, or
- Run the `cphaprob state` command on one of the cluster members.
**Status Manager**

The Status Manager displays a snapshot of all ClusterXL modules in the enterprise, enabling real-time monitoring and alerting. Communication and traffic flow statistics are also displayed. Administrators can also use the Status Manager to specify the action to be taken if the status of a cluster member changes. For example VPN-1/FireWall-1 can issue an alert notifying system managers of any suspicious activity.

The SmartCenter Server retrieves the status information and sends the data to the GUI Client. The GUI Client displays the data and, for cluster members only, it may also issue transition notifications. For more information, see TABLE 11-2 on page 401 of *Check Point SmartCenter Guide*.

A proprietary Check Point protocol is used for communication between the Check Point product modules and the SmartCenter Server.

The ClusterXL module details in the Status Manager are explained in TABLE 5-2.

To collapse or expand ClusterXL module data, click on ![View Menu](image) in the toolbar or choose **ClusterXL Module Details** from the **View** menu.

**TABLE 5-2** ClusterXL Module Details in Status Manager

<table>
<thead>
<tr>
<th>Column</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status of the ClusterXL module installed on this object:</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Active" /> — module installed and active</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Attention" /> — This icon draws your attention to the fact that the module is active even though all the members of the cluster have some problem. Despite this, the gateway with the least problems and the next highest priority level is active and working as a backup until the highest priority level gateway can be restored.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Stand by" /> — module ready to replace an active module</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Not Active" /> — module is down or there is a problem</td>
</tr>
</tbody>
</table>
Log Viewer

Every change of a cluster member’s status is recorded according to the choice in the Fail-Over Tracking option of the cluster object’s ClusterXL page, and can be viewed using the Log Viewer.
VoIP (Voice Over IP)

In This Chapter

Overview  
H.323-Based VoIP  
SIP-Based VoIP

Overview
VoIP (Voice Over IP) enables telephone conversations to be carried over IP networks. VPN-1/FireWall-1 supports both H.323-based and SIP-based VoIP.

For information about H.323-based VoIP, see “H.323-Based VoIP” on page 281.

For information about SIP-based VoIP, see “SIP-Based VoIP” on page 288.

H.323-Based VoIP
A simple H.323-based VoIP network configuration is shown in FIGURE 6-1.
Telephones

In this configuration, there are two kinds of telephones:

- IP phones — These are defined as a network of IP devices connected to an H.323 gatekeeper. The IP devices are either IP telephones or “soft phones” (computers with the appropriate software).
- conventional telephones — These are not IP devices (and so are not defined in the FireWall-1 database) and are connected to an H.323 gateway machine, which translates between the telephony protocol and IP.

**Gatekeeper and Gateways Object Definitions**

Gatekeepers and gateways have different functionality. Both are defined in the Policy Editor as a “virtual machine” hosted on a real machine, which is defined as a host (see FIGURE 6-2) on which FireWall-1 is not installed.

**Configuring VoIP (H.323)**

To enable VoIP traffic, proceed as follows:

1. Define the network objects that will be managed by the VoIP H.323 Gatekeeper. These are:
   - a network object consisting of either IP phones or “soft phones” (computers with the appropriate software)
• the machine hosting the VoIP H.323 Gatekeeper
• the machine hosting the VoIP H.323 Gateway (optional)

2 Define the VoIP H.323 Gatekeeper.

To define the gatekeeper, define a network object of type VoIP Domain, and choose VoIP H.323 Domain Gatekeeper from the menu (FIGURE 6-3).

FIGURE 6-3 Defining a VoIP Domain

3 In the General page of the VoIP Domain Gatekeeper window (FIGURE 6-4), define the Gatekeeper's parameters.

FIGURE 6-4 VoIP Domain Gatekeeper window — General page

Name — Enter the Gatekeeper's name.

Comment — Enter a descriptive comment to be displayed when this Gatekeeper is selected in the Object list and in the Network Objects window.
**Color** — Select the color in which this gatekeeper will be displayed in the GUI.

**Related endpoints domain** — Choose the network object (defined in step 1 on page 282) that this Gatekeeper will be managing.

A Gatekeeper’s **Related endpoints domain** is one or both of the following:
- the IP phones connected to the Gatekeeper, or
- a Gateway.

**VoIP installed on** — Choose the host on which this Gatekeeper is installed.

If you have not yet defined the host, click **New** to define it.

4 In the **Routing Mode** page of the **VoIP Domain Gatekeeper** window (FIGURE 6-5), define object’s parameters.

**FIGURE 6-5 VoIP Domain Gatekeeper window — Routing Mode page**

Each conversation consists of several connections, one after the other. The first connection is between VoIP Gatekeepers.

**Allowed Routing Mode** — Specify which connections will be re-routed endpoint-to-endpoint.

**Direct** — The H.225 Q.931 connection will be re-routed endpoint-to-endpoint.

**Call Setup (Q.931)** — The H.245 connection will be re-routed endpoint-to-endpoint.
Call Setup (Q.931) and Call Control (H.245) — The RTP/RTCP connections (audio, video and their associated control connections) will be re-routed endpoint-to-endpoint.

At least one of the choices must be checked.

VoIP H.323 Gateway (Optional)

5 Define the VoIP H.323 Gateway.

To define the VoIP H.323 Gateway, define a network object of type VoIP Domain, and choose VoIP H.323 Domain Gateway from the menu (FIGURE 6-3).

6 In the General page of the VoIP Domain Gateway window (FIGURE 6-4), define the Gateway’s parameters.

FIGURE 6-6 VoIP Domain Gateway window — General page

Name — Enter the Gateway’s name.

Comment — Enter a descriptive comment to be displayed when this Gateway is selected in the Object list and in the Network Objects window.

Color — Select the color in which this Gateway will be displayed in the GUI.

Related endpoints domain — Choose the network object (defined in step 1 on page 282) that this Gateway will be managing.

If each of host’s interfaces is dedicated to carrying a different H.323 protocol, then each interface must be defined as a separate network object. The interfaces are then chained using Related endpoints domain.
For example, if the host’s interfaces are A, B and C, then the chaining is as follows:

**TABLE 6-1** protocol - interface mapping

<table>
<thead>
<tr>
<th>interface</th>
<th>protocol</th>
<th>Related endpoints domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>H.225</td>
<td>B</td>
</tr>
<tr>
<td>B</td>
<td>H.245</td>
<td>C</td>
</tr>
<tr>
<td>C</td>
<td>RTP/RTCP</td>
<td>host</td>
</tr>
</tbody>
</table>

If B is in A’s Related endpoints domain but also functions as a redirecting entity, it should be defined as a VoIP Gateway.

**VoIP installed on** — Choose the host on which this Gateway is installed.

If you have not yet defined the host, click **New** to define it.

7 In the **Routing Mode** page of the VoIP Domain Gateway window (FIGURE 6-7), define object’s parameters.

**FIGURE 6-7** VoIP Domain Gateway window — Routing Mode page

Each conversation consists of several connections, one after the other. The first connection is between VoIP Gatekeepers.

**Allowed Routing Mode** — Specify which connections will be re-routed endpoint-to-endpoint.

**Call Setup (Q.931)** — The H.245 connection will be re-routed endpoint-to-endpoint.
Call Setup (Q.931) and Call Control (H.245) — The RTP/RTCP connections (audio, video and their associated control connections) will be re-routed endpoint-to-endpoint.

At least one of the choices must be checked.

**Global Properties — H.323**

8 In the VoIP page of the Global Properties window (FIGURE 6-8), define the VoIP parameters.

**FIGURE 6-8 VoIP page — Global Properties window**

Log VoIP connection — If checked, additional log entries will be generated for every VoIP connection.

The additional log entries contain information about the phone numbers (H.323).
H.323

**Allow to redirect connections** — Allow conversations to be handed over on both sides.

**Disallow blank source phone numbers** — Do not accept connections in which the source phone number is blank.

**Enable dynamic T.120** — T.120 is application-sharing file transfer.

**Security Policy Rule Base**

9 For H.323-based VoIP, define one of the following rules in the Security Policy Rule base. Either:

**TABLE 6-2 H.323 VoIP Security Policy Rules**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP Domain</td>
<td>VoIP Domain</td>
<td>H323_ras</td>
<td>Accept</td>
</tr>
<tr>
<td>host</td>
<td>host</td>
<td>H323_ras_only</td>
<td>Accept</td>
</tr>
<tr>
<td>endpoint domain</td>
<td>endpoint domain</td>
<td>H323</td>
<td>Accept</td>
</tr>
</tbody>
</table>

Where host is the machine on which the VOIP Domain Gatekeeper is installed.

The H323_ras_only service includes only the RAS part of H.323 (without handover), so the second rule allows the conversation.

**SIP-Based VoIP**

**Configuration**

There are many possible SIP-based configurations. The most common configurations can include:

- a SIP Proxy — manages a number of IP phones (or soft phones)
- a SIP Redirect Server — performs DNS-like functions preceding a VoIP connection
- a SIP Registrar — provides a DNS-like service, mapping SIP URLs to IP addresses
Some common SIP-based VoIP network configurations are shown in FIGURE 6-9 and FIGURE 6-10.

**FIGURE 6-9** VoIP — simple SIP-based configuration (no proxy)

**FIGURE 6-10** VoIP — proxy SIP-based configuration

---

**Note**: Proxy-based configurations can include one or more proxies, located either in the internal or external networks.

### Configuring VoIP (SIP)

1. Define the network objects that will be managed by the VoIP SIP Proxy. These are:
   - a network object consisting of either IP phones or “soft phones” (computers with the appropriate software)
   - the machine hosting the VoIP SIP Domain

2. Define the VoIP SIP Domain.

To define the VoIP SIP Domain, define a network object of type **VoIP Domain**, and choose **VoIP Domain SIP** from the menu (FIGURE 6-3).
3 In the **General** page of the **VoIP Domain SIP** window (FIGURE 6-12), define the SIP Domain’s parameters.

**FIGURE 6-12** VoIP Domain SIP window — General page

- **Name** — Enter the SIP’s Domain’s name.
- **Comment** — Enter a descriptive comment to be displayed when this SIP Domain is selected in the Object list and in the **Network Objects** window.
- **Color** — Select the color in which this SIP Domain will be displayed in the GUI.
- **Related endpoints domain** — Choose the network object (defined in step 1 on page 289) that this SIP Domain will be managing.

  This network object represents the IP address(es) of the IP phone(s) and can be a network, IP range, etc.

- **VoIP installed on** — Choose the host on which this SIP Domain is installed.
If you have not yet defined the host, click **New** to define it.

**Global Properties — SIP**

4. In the **VoIP** page of the **Global Properties** window (FIGURE 6-13), define the VoIP parameters.

**FIGURE 6-13 VoIP page — Global Properties window**

---

**Log VoIP connection** — If checked, additional log entries will be generated for every VoIP connection.

The additional log entries contain information about the user (SIP URL, for example, “SIP:Mickey@Mouse.com”).
SIP

Allow to re-direct connections — Allow conversations to be handed over on both sides.

If Allow to re-direct connections is not enabled, then only peer calls (endpoint-to-endpoint) are allowed. Calls made through proxies or redirect servers are not allowed.

Allow the destination to re-invite calls — Allow the destination to make a new call to the source while a call from source to destination is in progress.

The source can make additional calls to the destination even if Allow the destination to re-invite calls is not enabled.

Maximum invitations per call — The maximum number of additional calls that can be made while the original call is in progress.

Security Policy Rule Base

For SIP-based VoIP, there are three cases:

- No proxy — define the following rules in the Security Policy Rule base:

<table>
<thead>
<tr>
<th>TABLE 6-3</th>
<th>SIP-based VoIP Security Policy Rule Base (no proxy)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Destination</td>
</tr>
<tr>
<td>network object</td>
<td>network object</td>
</tr>
</tbody>
</table>

- proxy-based — define the following rules in the Security Policy Rule base:

<table>
<thead>
<tr>
<th>TABLE 6-4</th>
<th>SIP-based VoIP Security Policy Rule Base (proxy)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Destination</td>
</tr>
<tr>
<td>VoIP Domain</td>
<td>network object, or Any</td>
</tr>
</tbody>
</table>

Note:

- To allow conversations in both directions, define two rules.
- It is not possible to define a group of SIP Domain objects.
- To allow connections to a SIP Registrar, define an explicit rule.
- Another possible configuration is when the proxy is in the internal network and the VPN/FireWall Module protects the clients only.
To allow the internal network to make calls to the internal networks (the SIP protocol is routed through the VPN/FireWall Module to the proxy, add the following rules:

**TABLE 6-5** SIP-based VoIP Security Policy Rule Base (proxy inside the internal network)

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>All internal</td>
<td>VoIP Domain</td>
<td>sip, or sip_any</td>
<td>Accept</td>
</tr>
<tr>
<td>VoIP Domain</td>
<td>All internal</td>
<td>sip, or sip_any</td>
<td>Accept</td>
</tr>
</tbody>
</table>

If VoIP Domain is in the **Source** column, then the SIP Proxy is protected by a VPN/FireWall Module (that is, the SIP Proxy is inside the local network).

If VoIP Domain is in the **Destination** column, the SIP Proxy is not behind a VPN/FireWall Module but in an external network.

If VoIP Domain is in both the **Source** and **Destination** columns, then the connection is between two SIP Proxies, one behind the VPN/FireWall Module (in the local network) and the other in an external network.

**Service**

**Service** can be either sip or sip_any. The difference between these services is described in **TABLE 6-6**.

**TABLE 6-6** sip or sip_only services

<table>
<thead>
<tr>
<th>Service</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>sip</td>
<td>If <strong>Source</strong> or <strong>Destination</strong> is Any, then the object represented by Any is not allowed to redirect the connection, unless it is a SIP Proxy.</td>
</tr>
<tr>
<td>sip_any</td>
<td>If <strong>Source</strong> or <strong>Destination</strong> is Any, then the object represented by Any is allowed to redirect the connection, even if it is not a SIP Proxy, but only if it is external to the network(s) protected by the VPN/FireWall Module.</td>
</tr>
</tbody>
</table>
CHAPTER 7

Boot Security

In This Chapter

The Need for Boot Security
Control of IP Forwarding
The Default Filter
The Initial Policy
Stopping VPN-1/FireWall-1 for Remote Maintenance
Changing Boot Security Settings
Standard Default Filter
To change the Default Filter
Boot Security FAQ

The Need for Boot Security

During the boot process, there is a short period of time (measured in seconds) between the point when VPN/FireWall Module machine becomes able to communicate and the point when the Security Policy is loaded and is enforced. During this time, VPN-1/FireWall-1 Boot Security protects both the internal networks behind the VPN/FireWall Module machine, and the machine itself. Boot Security is provided by a number of elements working together:

- Control of IP Forwarding on boot
- The Default Filter (improved in NG)
- The Initial Policy (new in NG)

In addition, the `fwstop -proc` and `cpstop -fwflag -default` commands allow the FireWall-1 processes to be stopped for maintenance while at the same time protecting the Firewalled Gateway machine and the internal network.
Control of IP Forwarding

In VPN-1/FireWall-1, networks behind the VPN/FireWall Module machine are protected by disabling IP Forwarding in the OS kernel at boot. This ensures that there will never be a time when IP Forwarding is on but a Security Policy is not being enforced, so networks behind the gateway are safe.

Disabling IP Forwarding protects networks behind the VPN/FireWall Module machine, but it does not protect the VPN/FireWall Module machine itself. For this purpose, VPN-1/FireWall-1 implements a Security Policy and an Initial Policy during the period of vulnerability.

The Default Filter

Why the Default Filter is Needed

With no Default Filter, the sequence of actions after turning on the FireWalled Gateway machine is illustrated in FIGURE 7-1.

- Machine boots up
- IP Forwarding is disabled, and Interfaces are configured.
- FireWall-1 services start.

As soon as the interfaces are configured, the machine is unprotected.

What the Default filter Does

The Default Filter ensures that both the gateway and networks behind the gateway are protected after boot.
The Default Filter that is installed by default allows
- All outgoing communications
- Incoming communications on ports through which there were previous outgoing communications (relevant where VPN-1/FireWall-1 services were stopped using `fwstop -default`. See “Stopping VPN-1/FireWall-1 for Remote Maintenance” on page 300)
- Broadcast packets

The Default Filter also provides anti-spoofing protection for the Firewalled Gateway machine. It makes sure that packets whose source (or destination) are the FireWall machine itself did (did not) come from one of its interfaces.

A Default Filter that drops all traffic is also available. See “Standard Default Filter” on page 303.

**Default Filter Operation**

With a Default Filter, the sequence of actions after turning on the FireWalled Gateway machine is illustrated in FIGURE 7-2:
- Machine boots up.
- Boot security takes effect (Default Filter loads and IP Forwarding is disabled).
- Interfaces are configured.
- FireWall-1 services start.

The machine is protected as soon as the default filter loads

**FIGURE 7-2 How a Default filter Protects the Firewalled Gateway Machine**
The Initial Policy

The Default Filter will interfere with the installation of the first policy. Until the VPN-1/FireWall-1 administrator installs the Security Policy for the first time, security is enforced by the Initial Policy. The Initial Policy adds “implied rules” to the Default Filter, to allow the communication needed for the installation of the Security Policy.

In a distributed configuration where the Primary Management and Enforcement Module are on one machine, and the FireWalled gateways are on different machines, the Initial Policy allows on the

- FireWalled Gateway— cpd and fwd communication (for Policy installation), and SIC communication (for establishment of Trust).
- Primary Management and Enforcement Module machine— CPMI communication for GUI Clients.

Where the Management and FireWalled gateway are on the same machine, the Initial Policy allows just CPMI communication for GUI Clients.

Until a Security Policy is loaded for the first time, the sequence of actions after turning on the FireWalled Gateway machine is illustrated in FIGURE 7-3.

- Machine boots up
- Default Filter loads and IP Forwarding is disabled
- Interfaces are configured.
- FireWall-1 services start.
- Initial policy is Fetched from the Local Module.
- GUI Clients connect or Trust is established, and the Security Policy is installed.
The Initial Policy is created at the end of `cpconfig` any time that no Security Policy exists on the Module. It is enforced until a Policy is installed, and is never loaded again. In subsequent boots, the regular policy is loaded immediately after the Default Filter.

In summary, the Initial Policy and the Default Filter ensure that the FireWalled machine is protected until the administrator installs a Security Policy. There is no instant of time when the machine is left unprotected.

**Note** - An Enforcement (VPN/FireWall) Module on which a user-defined Security Policy has not yet been installed, and the Initial Policy and control of IP forwarding are active, cannot function as a gateway.

For example, if a SmartCenter Server is protected by an Enforcement Module which is in this configuration state, a GUI Client that is situated behind the Module will not be able to contact the SmartCenter Server. The GUI Client will only be able to contact the SmartCenter Server once an appropriate user-defined Security Policy (with the relevant implied rules) is installed on the Enforcement Module — or if the Initial Policy is removed and control of IP forwarding is disabled.
Stopping VPN-1/FireWall-1 for Remote Maintenance

It is sometimes necessary to stop VPN-1/FireWall-1 processes for maintenance, and it is impractical to disconnect the Firewalled Gateway machine from the network. An example would be where the machine is at a remote location. The `fwstop -default` and `fwstop -proc` commands allow FireWall-1 processes to be taken down for remote maintenance without exposing the machine to attack.

**fwstop -default and fwstop -proc**

*Note -*

- Use fwstop and fwstart only for boot security reasons (see the Check Point FireWall-1 Guide). To stop and start Check Point processes, use cpstop and cpstart (see page 755).
- On Win32 platforms, use the Services applet in the Control Panel to stop and start Check Point Services.

**Usage**

```
fwstop [-default | -proc]
```
Verifying the Default Filter

### Options

<table>
<thead>
<tr>
<th>Options</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>(no parameters)</td>
<td>Kills all VPN-1/FireWall-1 processes, that is:</td>
</tr>
<tr>
<td></td>
<td>• FireWall-1 daemon (fwd)</td>
</tr>
<tr>
<td></td>
<td>• VPN-1 daemon (vpnd)</td>
</tr>
<tr>
<td></td>
<td>• the Management Server (fwm)</td>
</tr>
<tr>
<td></td>
<td>• VPN-1/FireWall-1 SNMP daemon (snmpd)</td>
</tr>
<tr>
<td></td>
<td>• the authentication daemons</td>
</tr>
<tr>
<td></td>
<td>The VPN-1/FireWall-1 Security Policy is then unloaded from the kernel.</td>
</tr>
<tr>
<td>-default</td>
<td>Kills VPN-1/FireWall-1 processes (fwd, fwm, vpnd, fwssd).</td>
</tr>
<tr>
<td></td>
<td>Logs, kernel traps, resources, and all security server connections stop working.</td>
</tr>
<tr>
<td></td>
<td>The Security Policy in the kernel is replaced with the Default Filter.</td>
</tr>
<tr>
<td>-proc</td>
<td>Kills VPN-1/FireWall-1 processes (fwd, fwm, vpnd, fwssd).</td>
</tr>
<tr>
<td></td>
<td>Logs, kernel traps, resources, and all security server connections stop working.</td>
</tr>
<tr>
<td></td>
<td>The Security Policy remains loaded in the kernel.</td>
</tr>
<tr>
<td></td>
<td>Therefore rules with generic allow/reject/drop rules, based only on service, continue working.</td>
</tr>
</tbody>
</table>

### Changing Boot Security Settings

#### Verifying the Default Filter

You can verify that the Default Filter or the Initial Policy are indeed loaded as follows:

1. Boot the system.
2. Before installing another Security Policy, type the following command:

   ```
   $FWDIR/bin/fw stat
   ```

   The command’s output should show that `defaultfilter` is installed. Both the Default Filter and the Initial Policy will show the policy loaded as “default filter”

#### control_bootsec

Enables or disables Boot Security. The command turns both the Default Filter and the Initial Policy off or on, in the correct sequence.
Changing Boot Security Settings

### Usage

```bash
$FWDIR/bin/control_bootsec [-r] [-g]
```

### Options

<table>
<thead>
<tr>
<th>Options</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-r</td>
<td>Removes boot security</td>
</tr>
<tr>
<td>-g</td>
<td>Enables boot security</td>
</tr>
</tbody>
</table>

**TABLE 7-2 options control_bootsec**

**fwboot bootconf**

Use the `fwboot bootconf` command to change IP Forwarding or Default Filter settings. This command is located in `$FWDIR/boot`

### Usage

```bash
$FWDIR/bin/fwbootconf bootconf <command> [value]
```

**commands:**

- `get_ipf`  # reports whether FireWall-1 controls IP forwarding
- `set_ipf [0/1]`  # enables or disables control of IP forwarding
- `get_def`  # prints default filter file path
- `set_def <filename>`  # sets default filter file path
- `set_def`  # turns off default filter for next boot
- `no <command>`  # turns on default filter for next boot
Options

**TABLE 7-3 options fwboot bootconf**

<table>
<thead>
<tr>
<th>Options</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| Get_ipf  | Reports whether Firewall-1 controls IP Forwarding.  
- Returns 1 if IP Forwarding is controlled on boot.  
- Returns 0 if IP Forwarding is not controlled on boot |
| Set_ipf 0| Turns off control of IP forwarding for the next boot. |
| Set_ipf 1| Turns on control of IP forwarding for the next boot. |
| Get_def | Turns off Default Filter for the next boot. |
| Set_def | Turns on Default Filter for the next boot. |
| Set_def <filename> | Will load <filename> as the Default Filter in the next boot. The only safe recommended place to put the default.bin (default name) file is $FWDIR\boot. **Note:** Do NOT move these files |

**comp_init_policy**

**Usage**

$FWDIR/bin/comp_init_policy [-u | -g]

**TABLE 7-4 options comp_init_policy**

<table>
<thead>
<tr>
<th>Options</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>comp_init_policy -u</td>
<td>Removes the current Initial Policy, and ensures that it won’t be generated in future when cpconfig is run.</td>
</tr>
<tr>
<td>comp_init_policy -g</td>
<td>Generates the Initial Policy and ensures that it will be loaded the next time a policy is fetched (at fwstart, or at next boot, or via the fw fetch localhost command). After running this command, cpconfig will add an Initial Policy when needed.</td>
</tr>
</tbody>
</table>

**Standard Default Filter**

Two Default Filters are available: defaultfilter.boot and defaultfilter.drop. They are located in $FWDIR/lib.
To change the Default Filter

defaultfilter.boot

The default filter defaultfilter.boot is installed by default. It allows:

- All outgoing communications.
- Incoming communications on ports through which there were previous outgoing communications (relevant where VPN-1/FireWall-1 services were stopped using `fwstop -default`. See “Stopping VPN-1/FireWall-1 for Remote Maintenance” on page 300).
- ICMP packets.
- Broadcast packets.

defaultfilter.drop

The default Filter defaultfilter.drop drops all communications in and out of the gateway during the period of vulnerability.

If the boot process requires that the gateway communicate with other hosts, then the drop default Security Policy should not be used.

To change the Default Filter

1. Copy over and rename the relevant desired Default Filter INSPECT file (defaultfilter.boot or defaultfilter.drop) to $FWDIR/conf/defaultfilter.pf
2. Compile the Default Filter by running the command
   
   `fw defaultgen`
   
   The output will be in $FWDIR/state/default.bin
3. Run `fwboot bootconf get_def` to print the default filter file path.
4. Copy over `default.bin` to the default filter file path.
5. If the Security Policy has not yet been installed, run `cpconfig` to regenerate the Initial Policy (open and close it.)

User-Defined Default Filter

You can define your own Default Filter as follows:


   The script may not perform any of the following functions:
   - Logging
   - Authentication
To unload a Default Filter or an Initial Policy

You must ensure that your Security Policy does not interfere with the boot process.

**To unload a Default Filter or an Initial Policy**

To unload a Default Filter or an Initial Policy from the kernel, use the same command that is used for unloading a regular policy. Do this only if you are certain that you do not need the security provided by the Default Filter or an Initial Policy.

- To unload the Default Filter locally, run the `fw unloadlocal` command.
- To unload the Default Filter remotely, run the following command on the SmartCenter Server:

  ```
  fwm unload localhost
  ```

  where `localhost` is the SIC_name of the Module.

**Boot Security FAQ**

**Question: What to do if FireWall Machine cannot complete Reboot after installation**

The Default Filter can in certain configurations prevent the Firewalled Gateway machine completing the reboot following installation.

First, examine the Default Filter and see if the Default Filter allows traffic that the machine need to boot (see “Standard Default Filter” on page 303). If it does not, remove the Default filter as follows:

1. Reboot in single user mode (for UNIX) or Safe Mode With No Networking (for Windows 2000).

2. Ensure that the Default Filter does not load in future boots. Use the command `fwbootconf bootconf Set_def`

3. Reboot.
SNMP and Network Management Tools

In This Chapter

Overview

VPN-1/FireWall-1 HP OpenView Extension

VPN-1/FireWall-1 MIB Source

Overview

VPN-1/FireWall-1 SNMP Agent (daemon)

VPN-1/FireWall-1 includes a full SNMP V2 agent with both V1 (r/w community) and V2 security features.

The VPN-1/FireWall-1 SNMP daemon (snmpd) is compatible with network management software such as HP OpenView. The VPN-1/FireWall-1 SNMP daemon also provides Check Point specific variables.

Unix

The VPN-1/FireWall-1 SNMP daemon answers directly only to Check Point MIB variables. If another SNMP daemon is present, non-Check Point OID’s are forwarded by the VPN-1/FireWall-1 SNMP daemon to that SNMP daemon.

Windows

- If the Microsoft SNMP daemon is installed, the VPN-1/FireWall-1 SNMP daemon is an extension to it.
- If the Microsoft SNMP daemon is not installed, you will not be able to use the VPN-1/FireWall-1 SNMP agent or retrieve Check Point MIB variables.
Installation

Unix — Installing the Check Point SNMP daemon is optional. The daemon is started when the `cpstart` command is executed.

Windows — If the Microsoft SNMP agent is installed, then the Check Point SNMP agent is installed automatically.

Ports to Which the VPN-1/FireWall-1 SNMP daemon binds

The VPN-1/FireWall-1 SNMP daemon is started when VPN-1/FireWall-1 is started (`cpstart`) and is stopped when VPN-1/FireWall-1 is stopped (`cpstop`).

The VPN-1/FireWall-1 SNMP daemon tries to bind to the standard SNMP port (161) and also to port 260. If it fails to bind to port 161 (presumably because another SNMP daemon is already bound to that port), then it binds only to port 260 and passes on all non-VPN-1/FireWall-1 specific SNMP queries to the SNMP daemon on port 161.

If there is no daemon bound to port 161, the VPN-1/FireWall-1 daemon binds to both ports (161 and 260). This allows all clients to use the VPN-1/FireWall-1 SNMP daemon. If another SNMP daemon attempts to bind to port 161 after the VPN-1/FireWall-1 SNMP daemon is started, the other daemon will fail to bind to the port. In the event that it is important for you to use an SNMP daemon other than the VPN-1/FireWall-1 daemon, start it before you start VPN-1/FireWall-1.

Trap alert as well as status reports can be sent to SNMP-based management software.

Under Windows NT, the VPN-1/FireWall-1 SNMP agent is an extension of the NT SNMP agent. If you have not installed the standard NT SNMP agent, you will not be able to use the VPN-1/FireWall-1 SNMP agent.

Initial Communities (“Keys”)

The initial SNMP communities (“keys”) are `public` and `private` for read and write, respectively. To change these keys, edit `$FWDIR/conf/snmp.C`, and set the values for the read and write attributes for `snmp_community`.

VPN-1/FireWall-1 MIB

The variable definitions for VPN-1/FireWall-1’s SNMP daemon are located in the files `$FWDIR/lib/snmp/chkpnt.mib`. This file can be used to incorporate the Check Point MIB into any MIB browser or network management system.

- FireWall-1’s SNMP variables are located in the subtree `1.3.6.1.4.1.2620.1.1` (also known as `enterprises.checkpoint.products.fw`).
VPN-1’s SNMP variables are located in the subtree 1.3.6.1.4.1.2620.1.2 (also known as enterprises.checkpoint.products.vpn).

Note: Previous versions of VPN-1/FireWall-1 used enterprise ID 1919 for Check Point private MIB. VPN-1/FireWall-1 version 4.0 uses 2620 — the official Check Point enterprise ID (1.3.6.1.4.1.2620), as the prefix for all Check Point specific MIB variables. SNMP traps also use the updated enterprise ID.

TABLE 8-1 lists the variables that are unique to VPN-1/FireWall-1, and unless otherwise noted, are strings of up to 256 bytes.

TABLE 8-1  VPN-1/FireWall-1 MIB Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>fwModuleState</td>
<td>the state of the Inspection Module</td>
</tr>
<tr>
<td>fwFilterName</td>
<td>the name of the currently loaded Security Policy</td>
</tr>
<tr>
<td>fwFilterDate</td>
<td>the date the Security Policy was installed</td>
</tr>
<tr>
<td>fwAccepted</td>
<td>the number of packets accepted by the Inspection Module since the last Security Policy was installed (an integer)</td>
</tr>
<tr>
<td>fwRejected</td>
<td>the number of packets rejected by the Inspection Module since the last Security Policy install (an integer)</td>
</tr>
<tr>
<td>fwDropped</td>
<td>the number of packets dropped by the Inspection Module since the last Security Policy install (an integer)</td>
</tr>
<tr>
<td>fwLogged</td>
<td>the number of packets logged by the Inspection Module since the last Security Policy was installed (an integer)</td>
</tr>
<tr>
<td>fwMajor</td>
<td>the VPN-1/FireWall-1 major release number (for example, for VPN-1/FireWall-1 Version 4.0 this is 4) — an integer</td>
</tr>
<tr>
<td>fwMinor</td>
<td>the VPN-1/FireWall-1 minor release number (for example, for VPN-1/FireWall-1 Version 4.0 this is “0”) — an integer</td>
</tr>
<tr>
<td>fwProduct</td>
<td>the VPN-1/FireWall-1 product</td>
</tr>
<tr>
<td>fwEvent</td>
<td>the last SNMP trap sent by VPN-1/FireWall-1</td>
</tr>
</tbody>
</table>

The source of the VPN-1/FireWall-1 MIB is listed in “VPN-1/FireWall-1 MIB Source” on page 314.
VPN-1/FireWall-1 HP OpenView Extension

HP OpenView Network Node Manager displays hierarchical maps of the network topology. The VPN-1/FireWall-1 extension provides information on FireWalled objects in the network. The extension enables administrators to:

- display FireWalled objects within the context of the entire network
- specify network objects and devices as FireWalled objects
- open the VPN-1/FireWall-1 Log, Security Policy and System Status views

To enable this feature, the machine running the OpenView Network Node Manager session must have a the VPN-1/FireWall-1 GUI client installed. The GUI client must be permitted by the VPN-1/FireWall-1 SmartCenter Server, and you must be one of the allowed administrators.

- display connection statistics and SNMP alert information for Check Point Modules
- access Check Point MIB data

Installing the FireWall-1 HP OpenView Extension

TABLE 8-2 lists the minimum hardware, operating system, and software requirements for installing the VPN-1/FireWall-1 Extension for HP OpenView Network Node Manager.

\begin{tabular}{|l|l|}
\hline
**Platforms** & HP PA-RISC 700/800, Sun SPARC-based systems \\
\hline
**Operating System** & HP-UX 10.x, Solaris 2.3 and higher \\
\hline
**Software** & VPN-1/FireWall-1 X/Motif GUI Client \\
& HP OpenView Network Node Manager version 4.1x \\
\hline
\end{tabular}

For hardware and software requirements of HP OpenView Network Node Manager, consult the HP documentation.

You can install the VPN-1/FireWall-1 HP OpenView Extension either directly from the CD-ROM, or you can recursively copy the installation files from the CD-ROM to a directory on your disk and install from there.

Installing the VPN-1/FireWall-1 HP OpenView Extension (Solaris2)

1. Become superuser.
2 Change to the directory in which the installation files are located (either on the CD-ROM or on the hard disk).

3 Enter the following command to install the VPN-1/FireWall-1 HP OpenView Extension:

```
hostname# pkgadd -d .
```

4 `pkgadd` presents a list of packages, and asks you to choose one to install.

Specify the VPN-1/FireWall-1 HP OpenView Extension by entering either its name or its number in the list.

**Installing the VPN-1/FireWall-1 HP OpenView Extension (HP-UX)**

If you encounter a problem with the depth of the CD-ROM directories, use the files in `hpux/TarFiles`.

1 Become superuser.

2 Copy the installation files to the `/tmp` directory.

3 If the `/tmp` directory has not been registered as an installation directory, enter the following command to register it.

```
hostname# swreg -l depot -x select_local=true /tmp
```

For information about the `swreg` command, refer to the HP-UX documentation.

4 Enter the following command to install the VPN-1/FireWall-1 HP OpenView Extension:

```
hostname# swinstall &
```

5 The SD Install - Software Selection window is displayed, and then the Specify Source window is displayed on top of it.

For information about the `swinstall` command, refer to the HP-UX documentation.

6 Click on Source Depot Path.

7 In the Depot Path window, select the directory in which the installation files are located.

8 Click on OK to close the Depot Path window.

9 Click on OK to close the Specify Source window.
10 In the SD Install - Software Selection window, select FireWall-1 HP OpenView Extension.

11 From the Actions menu, select Install (analysis).

12 When the analysis phase completes, click on OK.

13 When the installation phase completes, click on Done.

14 From the File menu, select Exit.

Uninstalling the VPN-1/FireWall-1 HP OpenView Extension

Solaris2
Use the pkgrm application to uninstall the VPN-1/FireWall-1 HP OpenView Extension.

HP-UX
1 Become superuser.
2 Type the following command:

```
hostname# swremove FWMap
```

Viewing FireWalled Objects

Network Submap
HP OpenView Windows displays a hierarchical map of all the devices, systems and Check Point Modules in the network. Check Point Modules are represented in a network submap by a FireWall icon.

FireWalls Window
The FireWalls window displays only the Check Point Modules in the network. To open the FireWalls window, double-click on the FireWalls icon in the root submap. To access the root submap, click on the Root Submap icon on the Open View toolbar.

HP OpenView identifies as FireWalled objects only those objects running the VPN-1/FireWall-1 SNMP daemon.

The FireWall discovery takes place when HP OpenView Windows (ovw) is started and whenever a new device is added to the network. If you start VPN-1/FireWall-1 after the FireWall discovery, the object will not be identified as FireWalled unless specifically queried (see “Query Selected” below).
If HP OpenView discovers a FireWalled object with the VPN-1/FireWall-1 SNMP daemon on port 260, it changes its default SNMP port for that object to 260.

**FireWall Menu**

The FireWall menu appears in the menu bar of the submap window.

<table>
<thead>
<tr>
<th>Menu Entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query Selected</td>
<td>Performs discovery on the selected objects.</td>
</tr>
<tr>
<td>Set as FireWall</td>
<td>Sets a network object as a FireWall. This option is enabled only if a VPN/FireWall Module was not detected on the selected object.</td>
</tr>
<tr>
<td>Unset as FireWall</td>
<td>Clears FireWall settings from the selected object. This option is enabled only if the object was manually set as a FireWall.</td>
</tr>
</tbody>
</table>

**FireWall-1**

This entry displays a sub-menu with the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log View</td>
<td>Opens the Log View</td>
</tr>
<tr>
<td>Security Policy</td>
<td>Opens the Security Policy</td>
</tr>
<tr>
<td>System Status</td>
<td>Opens the System Status View</td>
</tr>
<tr>
<td>Statistics</td>
<td>Displays a graph indicating the number of frames accepted, logged, dropped and rejected for the selected FireWall.</td>
</tr>
</tbody>
</table>

You can also access the above options by right-clicking on a FireWalled object.

**Note:** In order to open the Check Point GUI, the machine running the current OpenView Windows session must have a Check Point GUI client installed. In addition, the GUI client must be permitted by the VPN-1/FireWall-1 SmartCenter Server and you must be one of the allowed administrators.
VPN-1/FireWall-1 SmartCenter Servers
When you start one of the VPN-1/FireWall-1 GUI applications (Security Policy, Log Viewer or System Status), the applications runs against the FireWalled object’s SmartCenter Server, which is not necessarily the same machine as the FireWalled object. If the VPN/FireWall Module and the SmartCenter Server are on different machines, then you must configure the FireWalled object as follows:

1. Select the FireWalled object.
2. From the Edit menu, choose Describe/Modify Object.
3. In the Object Description dialog box, choose FireWall-1 Management. The FireWall-1 Management dialog box displays the host name of the SmartCenter Server.
4. Enter the name of the SmartCenter Server and click on OK.

Specify the correct host name or IP address.

VPN-1/FireWall-1 SNMP Traps
The Application Alert Events browser displays a log of SNMP traps. All VPN-1/FireWall-1 SNMP traps appear in the Application Alert Events browser.

Note: You must first direct VPN-1/FireWall-1 SNMP traps to the host running OpenView using the snmp_trap command.

Check Point MIB Data
The Check Point MIB is accessible through the Network Node Manager SNMP MIB browser.

To access the Check Point MIB, proceed as follows:

1. Choose SNMP MIB Browser from the Misc menu. The Browse MIB dialog box is displayed.
2. Navigate to the Check Point MIB, which is located under the Enterprises sub-tree.

VPN-1/FireWall-1 MIB Source
This section presents the source code for the VPN-1/FireWall-1 MIB (in $FWDIR/lib/snmp/chkpnt.mib).

CHECKPOINT-MIB DEFINITIONS:= BEGIN
    -- SUBTREE: 1.3.6.1.4.1.2620.1.1

314 Check Point FireWall-1 • September 2002
-- iso.org.dod.internet.private.enterprises.checkpoint.products.fw

IMPORTS
  enterprises
  FROM RFC1155-SMI
TRAP-TYPE
  FROM RFC-1215
OBJECT-TYPE
  FROM RFC-1212;

-- textual conventions

DisplayString ::= OCTET STRING
-- This data type is used to model textual information taken
-- from the NVT ASCII character set. By convention, objects
-- with this syntax are declared as having
--
-- SIZE (0..255)

checkpoint OBJECT IDENTIFIER ::= { enterprises 2620 }
products OBJECT IDENTIFIER ::= { checkpoint 1 }
fw OBJECT IDENTIFIER ::= { products 1 }

-- the FW group
-- Overall statistics and state
-- To be added a table of statistics by interfaces.

fwModuleState OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
ACCESS read-only
STATUS mandatory
DESCRIPTION
"The state of the fw module."
::= { fw 1 }

fwFilterName OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
ACCESS read-only
STATUS mandatory
DESCRIPTION
"The name of the loaded filter."
::= { fw 2 }

fwFilterDate OBJECT-TYPE
SYNTAX DisplayString (SIZE (0..255))
ACCESS read-only
STATUS mandatory
DESCRIPTION
"When was the filter installed (STRING!)"
::= { fw 3 }

fwAccepted OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION
  "The number of accepted packets."
 ::= {fw 4 }

fwRejected OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION
  "The number of rejected packets."
 ::= {fw 5 }

fwDropped OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION
  "The number of dropped packets."
 ::= {fw 6 }

fwLogged OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION
  "The number of logged packets."
 ::= {fw 7 }

fwMajor OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION
  "FireWall-1 Major Version."
 ::= {fw 8 }

fwMinor OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION
  "FireWall-1 Minor Version."
 ::= {fw 9 }

fwProduct OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION
  "FireWall-1 Product."
Viewing FireWalled Objects

Chapter 8  SNMP and Network Management Tools  317

::= { fw 10 }

fwEvent OBJECT-TYPE
SYNTAX  DisplayString (SIZE (0..255))
ACCESS  read-only
STATUS  mandatory
DESCRIPTION  
"A string containing the last snmp trap sent via fw"
::= { fw 11 }

Note: The following comment lines are a description of the MIB used by the SNMP traps generated by VPN-1/FireWall-1.

--fwTrap TRAP-TYPE
-- ENTERPRISE fw
-- VARIABLES { fwEvent }
-- DESCRIPTION
-- "FireWall-1 SNMP trap"
-- ::= 0

END
The Need for Server Load Balancing

The VPN-1/FireWall-1 Load Balancing feature (an optional feature) enables several servers providing the same service to share the load among themselves.

Consider the configuration depicted in FIGURE 9-1 on page 320. All the HTTP servers can provide the HTTP client with the same services (but note that not all of the HTTP servers are behind the VPN/FireWall Module). In the same way, all the FTP servers can provide the FTP client with the same services.

The system administrator wishes to ensure that the service load is balanced among the servers. The client will be unaware of the different servers. From the client's point of view, there is only one HTTP server and only one FTP server. When the service request reaches the gateway, VPN-1/FireWall-1 determines which of the servers will fulfill the request, based on the load balancing algorithm specified by the system administrator.
How Server Load Balancing Works

**Load Balancing using HTTP Logical Server**

When HTTP is chosen under **Servers Type** in the **Logical Server Properties** window, Load Balancing is performed as follows:

1. **VPN-1/FireWall-1** detects a service request for a Logical Server (see “Defining Logical Servers” on page 322).

   For example, the client starts an HTTP session on the Logical Server **HTTP_servers** (whose **Server** is defined as **HTTP_Group**, consisting of the servers Tower, Palace and BigBen, as shown in FIGURE 9-1 on page 320).

2. **VPN-1/FireWall-1** redirects the connection to the Load Balancing application (**lhttpd**).

   This is done using the translate port feature of the Address Translation mechanism.

3. The Load Balancing application determines to which particular server the session is to be redirected.

---

*Note* - The IP address returned by the DNS should be the IP address of the Logical Server, to allow the VPN/FireWall Module to perform the load balancing between the physical servers.
For example, VPN-1/FireWall-1 determines, on the basis of the load balancing algorithm defined for the Logical Server **HTTP_Servers**, that BigBen will be the server for this session.

4 The Load Balancing application notifies the client that the URL is being redirected to the chosen server.

This is done using the URL Redirection feature of HTTP to redirect the client to a specific IP address rather than the IP address of the Logical Server.

5 The rest of the session is conducted between the client and the chosen server, without the intervention of VPN-1/FireWall-1.

**Note**: When using the http method, the physical servers may be located either behind the FireWall or not, so long as they are routable both from the client and from the gateway, since the connection will ultimately be direct between client and physical server.

### Load Balancing using Non–HTTP Logical Server

When **Other** is chosen under **Servers Type** in the **Logical Server Properties** window (FIGURE 9-2 on page 323), Load Balancing for HTTP is performed using the Address Translation mechanism. Each HTTP connection is then handled separately, and connections may be redirected to different servers (if **Persistent server mode** in the **Logical Server Properties** window is not set). This may cause problems in some cases, for example, in an application where a user fills in a number of HTTP forms and a single server is expected to process all the data.

1 VPN-1/FireWall-1 detects a service request for a Logical Server (see “Defining Logical Servers” on page 322).

   For example, the client starts an FTP session on the Logical Server **FTP_servers** (whose **Server** is defined as **FTP_Group**, consisting of the servers EastEnd, Trafalgar and Whitehall, as shown in FIGURE 9-1 on page 320).

2 VPN-1/FireWall-1 determines that the session is to be redirected to a particular server.

   For example, VPN-1/FireWall-1 determines, on the basis of the load balancing algorithm defined for the Logical Server **FTP_Servers**, that Trafalgar will be the server for this session.

3 Using the Address Translation mechanism, VPN-1/FireWall-1 modifies the destination IP address of incoming packets.
If a back connection is opened (for example, in FTP), the connection is correctly established between the server and the client automatically. The source IP address of reply packets is changed back to the Logical Server’s IP address.

**Note** - When using non-http (other), the route from the physical server to the client must go through the FireWall (this usually means the server is behind the FireWall), since the connection from the client is Network Address Translated, thus requiring that every packet of the connection pass through the FireWall.

### Load Balancing Algorithms

The available load balancing algorithms are:

1) server load
   
   VPN-1/FireWall-1 queries the servers to determine which is best able to handle the new connection. There must be a load measuring agent on the server (see “Load Measuring” on page 325).

2) round trip
   
   VPN-1/FireWall-1 uses ping to determine the round-trip times between the VPN/FireWall Module and each of the servers, and chooses the server with the shortest round trip time.

   This method will not give optimum results for HTTP if some of the HTTP servers are not behind the VPN/FireWall Module, because it measures the round-trip time between the VPN/FireWall Module and the servers, and not between the client and the servers.

3) round robin
   
   VPN-1/FireWall-1 simply assigns the next server in the list.

4) random
   
   VPN-1/FireWall-1 assigns a server at random.

5) domain
   
   VPN-1/FireWall-1 assigns the “closest” server, based on domain names.

### Defining Logical Servers

To implement the VPN-1/FireWall-1 load balancing feature, proceed as follows (the example is based on the configuration depicted in FIGURE 9-1 on page 320):

1. Define a group network object consisting of all the servers that will be providing the given service.
For example, define a group network object **HTTP Group** that consists of Tower, Palace, BigBen and Louvre. There should be no other servers in the group.

2 Define a network object of type Logical Server, and define its properties.

3 Define a Logical Server as in FIGURE 9-2.

**FIGURE 9-2 Logical Server Properties window**

IP Address must be an address for which communications are routed to or through the VPN/FireWall Module. This should be either the VPN/FireWall Module’s address, or the address of a non-existing computer in the network behind the VPN/FireWall Module. This is the address that clients use to communicate with the Logical Server.

**Persistent server mode** — Specifies that once a client is connected to a physical server, the client will continue to connect to that server for the duration of the session, in one of the following ways:

**Persistence by service** — Once a client is connected to a physical server for a specified service, subsequent connections to the same Logical Server and the same service will be redirected to the same physical server for the duration of the session.
Persistency by server — Once a client is connected to a physical server, subsequent connections to the same Logical Server (for any service) will be redirected to the same physical server for the duration of the session.

Note -
- The time period during which connections are redirected is specified in the ConnectControl page of the Global Properties window (on page 287 of Check Point Management Guide).
- If a server becomes unavailable, new connections will be directed to an available server even if Persistent server mode is enabled.

Servers is HTTP_Group.

None of the network objects that belong to Servers may have the IP address listed under IP Address.

Servers Type is HTTP.

This parameter determines how the redirection is performed. For further information, see “How Server Load Balancing Works” on page 320. Note that even for a Logical Server consisting of HTTP servers, Servers Type can be Others.

Balance Method is one of the algorithms described under “Load Balancing Algorithms” on page 322.

4 Add the appropriate rules to the Rule Base, for example, the one in FIGURE 9-3.

FIGURE 9-3 Using Logical Servers in a Rule

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>HTTP_Servers</td>
<td>http</td>
<td>accept</td>
<td>Short</td>
<td>Gateways</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>HTTP_Group</td>
<td>http</td>
<td>User Auth</td>
<td>Long</td>
<td>Gateways</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>reject</td>
<td>Long</td>
<td>Gateways</td>
</tr>
</tbody>
</table>

TABLE 9-1 Explanation of Rule Base

<table>
<thead>
<tr>
<th>Rule No.</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>balances the load for connections to the Logical Server HTTP_Servers</td>
</tr>
<tr>
<td>2</td>
<td>specifies that HTTP connections to HTTP_Group be User Authenticated (could also be Accept)</td>
</tr>
<tr>
<td>3</td>
<td>rejects and logs all other communications</td>
</tr>
</tbody>
</table>
Rule Base

The VPN/FireWall Module determines the availability of a Logical Server by pinging it. You should define rules to allow the ping as follows:

- allow the echo-request service from the VPN/FireWall Module to the Logical Servers
- allow the echo-reply service from the Logical Servers to the VPN/FireWall Module

Using HTTP Logical Servers in a Rule

When an HTTP Logical Server is the Destination in a rule, the rule’s Action refers to the connection between the VPN/FireWall Module and the client (the connection that serves to redirect the client to the proper server), and must be either Accept or Encrypt. There must be a different rule that allows the connection between the client and the server. That rule can specify another action, for example, User Authentication.

The rule specifying the Logical Server as Destination must come before the rule specifying the physical servers as Destination.

In the configuration depicted in FIGURE 9-1 on page 320, HTTP connections to the HTTP servers behind the VPN/FireWall Module will be User Authenticated (in accordance with the second rule in FIGURE 9-3 on page 324), but HTTP connections to Louvre will not be User Authenticated, because they do not pass through the VPN/FireWall Module, even though they were enabled by the VPN/FireWall Module.

Using non-HTTP Logical Servers in a Rule

There are no special considerations for using non-HTTP Logical Servers in a rule. One rule, with the Logical Server as Destination, is sufficient.

Load Measuring

Check Point provides a sample load measuring agent application for installation on servers on which VPN-1/FireWall-1 is not installed, as well as a protocol for users who wish to write their own agents.

The load measuring agent is a service running on the port number specified in the Load agents port property (in the Connect Control page of the Global Properties window) and returns information about the server’s load to VPN-1/FireWall-1. All the load measuring agents in a configuration must use the same port number.

Note: The load agent uses UDP port 18212 by default.
The load measuring agent measures the load at the interval specified by the Load measurement Interval property, also defined in the Connect Control page of the Global Properties window.

For example, in the configuration depicted in FIGURE 9-1 on page 320, the server Louvre is not FireWalled, so the only way for VPN-1/FireWall-1 on London to know what Louvre's load is (and to what extent Louvre is able to handle additional clients), is for Louvre's system administrator to install a VPN-1/FireWall-1 compatible load measuring agent on Louvre.
FAQ (Frequently Asked Questions)

In This Chapter

Defining Objects and Services  page 327
Daemons  page 332
Security Servers  page 333
Logging  page 337
Security  page 338
VPN-1/FireWall-1/n (VPN-1/FireWall-1/25, VPN-1/FireWall-1/50, etc.) Issues  page 339
Supported Protocols and Interfaces  page 341
Inspecting  page 342
Administrative Issues  page 343
Performance  page 344

Defining Objects and Services

Question: Which Network Objects Are on My Network?

Refer to the files /etc/hosts and /etc/networks. For Unix systems, see the manual pages for hosts and networks.

If NIS/YP (Network Information Service, formerly Sun Yellow Pages) is running on your system, use the commands ypcat hosts and ypcat networks to access network information. For Unix systems, see the manual pages for ypcat.

Question: How Do I Define the “Internet” or “Others”?
You might wish to define rules that apply to the “Internet” or to “all other hosts and networks but mine”. To do that, you should first define a group network object that includes all network objects that are “mine”: all your hosts, networks, domains, groups, etc.

Add the “mine” network object to the source or the destination of the rule you are defining and select it. Then use the menu options **Negate**. This will put a cross over the “mine” network object, which indicates: any network object that **Negate** mine (that is, not in “mine” group).

**Question: What's the difference between hosts, gateways and interfaces?**

In defining network objects, it is important to keep in mind the distinction between hosts, gateways, and interfaces.

A host is a computer, typically with only one interface. A gateway is a computer with more than one interface, but the gateway itself is a single object and should be defined as such. Each of its interfaces is defined individually in the **Topology** page of the gateway’s **Properties** window.
A host's name is the string returned by the `hostname` command. The IP address is the one corresponding to the host's name, as given in `/etc/hosts`, NIS/YP (Yellow Pages) or DNS.

**Question: Which Services and Protocols Are on My Network?**

Refer to the files `/etc/services`, `/etc/rpc`, and `/etc/protocols`. For Unix systems, see the manual pages for `services`, `rpcinfo`, and `protocols`.

If NIS/YP (Network Information Service, formerly Sun Yellow Pages) is running on your system, use the commands `ypcat services` and `ypcat protocols` to access network information. For Unix systems, see the manual pages for `ypcat`.

**Question: Which Services Have More Than One Type?**
Some services are available under more than one protocol; that is, they have more than one type. For instance, *time* and *domain* are available under both UDP and TCP; *nfs* is a TCP service, a UDP service and an RPC program.

### TABLE 10-1 Services available under both TCP and UDP

<table>
<thead>
<tr>
<th>service name</th>
<th>port number</th>
<th>service name</th>
<th>port number</th>
</tr>
</thead>
<tbody>
<tr>
<td>chargen</td>
<td>19</td>
<td>echo</td>
<td>7</td>
</tr>
<tr>
<td>daytime</td>
<td>13</td>
<td>sunrpc</td>
<td>111</td>
</tr>
<tr>
<td>discard</td>
<td>9</td>
<td>time</td>
<td>37</td>
</tr>
<tr>
<td>domain</td>
<td>53</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### TABLE 10-2 Services available both as RPC and TCP or UDP

<table>
<thead>
<tr>
<th>RPC name</th>
<th>RPC program number</th>
<th>TCP/UDP name</th>
<th>TCP/UDP number</th>
</tr>
</thead>
<tbody>
<tr>
<td>portmapper</td>
<td>100000</td>
<td>sunrpc</td>
<td>UDP/TCP port 111</td>
</tr>
<tr>
<td>nfs</td>
<td>100003</td>
<td>nfs</td>
<td>UDP port 2049</td>
</tr>
</tbody>
</table>

**Question: Which Services Are Dependent on Other Services?**

Common services that require other services to function correctly are listed in TABLE 10-3 on page 331. Some services are available in several types (for instance, *nfs* could be UDP or RPC). Each type may have different dependencies.

**Note** - VPN-1/FireWall-1 is supplied with predefined service groups that ensure that access is allowed to all other services required for a service to function properly.
Chapter 10 FAQ (Frequently Asked Questions)

Question: Dual DNS (Internal and External)

In a configuration that includes two Domain Name Servers (DNS) — an internal DNS for resolving internal names and an external DNS for resolving external names — the internal names can be hidden from external users by the following strategy:

• the external DNS has primary entries to a limited number of internal hosts
• the external DNS cannot issue inquiries to the internal DNS
• the internal DNS can issue inquiries to the external DNS

In this way, the internal DNS is restricted to resolving internal names for internal users while external users can gain no knowledge of internal names.

VPN-1/FireWall-1 can be used to enforce this strategy. The external DNS can reside on the VPN/FireWall Module.

Question: How Many Rules Are Supported?

Theoretically, the Policy Editor can support a large number of rules, and Rule Bases of more than 150 rules are not uncommon. In practice, even very complex policies are normally defined in about 15 rules. Since the rules can contain group objects, a small number of rules is usually sufficient to define the Security Policy.

Question: Is it necessary to define each of a gateway's interfaces as a separate network object? If yes, are they all gateways, or should the other interfaces be defined as hosts? Why doesn't VPN-1/FireWall-1 treat a gateway and all its interfaces as a single object?

The interface is not a separate network object, but rather part of another network object (gateway, router, etc.). You should not define interfaces as network objects. Instead, define interfaces as part of the network object's definition in the Interfaces tab of its Properties window.

Question: Is there a way to allow only specific ports to communicate with a system?

<table>
<thead>
<tr>
<th>Service</th>
<th>Type</th>
<th>Number</th>
<th>Required</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>ypserv</td>
<td>RPC</td>
<td>100004</td>
<td>ybind yppasswd yppasswd ypxfrd</td>
<td></td>
</tr>
<tr>
<td>nfs</td>
<td>RPC</td>
<td>100003</td>
<td>mountd nlockmgr</td>
<td>ypserv</td>
</tr>
<tr>
<td>nfds</td>
<td>UDP</td>
<td>2049</td>
<td>mountd</td>
<td></td>
</tr>
<tr>
<td>r* (rcp, rsh but not rlogin)</td>
<td>command s</td>
<td></td>
<td>shell (TCP)</td>
<td></td>
</tr>
</tbody>
</table>
To limit source port number from 2000 to 3000, proceed as follows:

1. In the Services Manager, create a new service of type TCP or UDP.
2. In **Source Port Range**, enter the range 2000 - 3000.
3. Then use the newly created service in your Rule Base.

**Question: How can I control FTP from HTTP?**

There is no difference, from VPN-1/FireWall-1’s point of view, between an FTP session that originated as such (for example, a user typing `ftp elvis.com`) and an FTP session created when a user downloads a file by clicking on its name in a Web page. A rule that applies to one applies to the other.

If you wish to enable your users to use FTP from their Web browsers, you must define a rule allowing them to use FTP in general, without reference to HTTP. In addition, you must also:

- *not* define an FTP proxy to the browser
- set the **Enable PASV FTP Connections** property (required by some HTTP servers)

**Question: How can I restrict ping information to allow a set of machines to ping freely without restrictions, while preventing other hosts from pinging through the firewall?**

Create two rules, one to allow the set of machines to send echo-requests and another to allow that same set of machines to receive echo-replies.

You can combine the two rules, either by putting both services in the same rule or by specifying “echo” (a pre-defined group which includes echo-request and echo-reply) as the service.

Because ping is an ICMP service and therefore has no port numbers, it is treated differently from other services, such as FTP and TELNET, which are automatically allowed to return information. The ping information is checked when it leaves and when it comes back, preventing a single rule from allowing a set of machines unrestricted pings, as the returns from the remote machines are dropped by VPN-1/FireWall-1.

**Daemons**

**Question: `inetd.conf` and the VPN-1/FireWall-1 TELNET Daemon**

**Question:** If I am running VPN-1/FireWall-1 with User Authentication, can I still allow a standard TELNET to the FireWalled host itself? In other words, will making a rule that allows TELNET (without User Authentication) re-install the standard `in.telnetd` in `inetd.conf`?
Answer: The answer to the second question is no. Once you install the VPN-1/FireWall-1 Security Servers, VPN-1/FireWall-1 modifies `inetd.conf` and comments out the standard TELNET and FTP daemons.

**Security Servers**

**Question: How can I hide that the fact that VPN-1/FireWall-1 is running from users of authenticated TELNET and FTP services?**

If you want users to see only the user defined message file, and not the “VPN-1/FireWall-1 authenticated telnet gw...” message, then add the following line to `objects.c`, under “:props”:

```
:undo_msg (true)
```

**Warning**: The `objects.c` file should not be edited directly. Instead, use `dbedit` (see “dbedit” on page 589 of *Check Point Management Guide*) to edit the `objects_5_0.C` file on the SmartCenter Server.

**Question: How can I define an Authentication rule for individual users rather than for groups?**

The short answer is that it’s not possible, but you can achieve the effect by defining a group for every user. Then you might have a user Alice and a group GrpAlice (with only Alice as a member), a user Bob and a group GrpBob (with only Bob as a member), and so on for each of your users.

The long answer is that it’s not clear what the benefit of this would be, since you can define restrictions at the user level that are enforced for each user in a group. For example, suppose you have a rule like this:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>DayUsers@localnet</td>
<td>Any</td>
<td>Any</td>
<td>UserAuth</td>
<td>Log</td>
<td>Gateways</td>
</tr>
</tbody>
</table>

The rule does not apply equally to all the users in the group *DayUsers*. It allows each user access only in accordance with his or her access privileges, as defined in each user’s *User Properties* window. (This is true if you have chosen the default value, *Intersect with User Database*, in the rule’s *User Authentication Action Properties* window.)
Suppose you want to allow Alice access only in the morning, and Bob access only in the afternoon. Just set their access privileges accordingly in their User Properties windows. Then, no matter which groups they belong to, they will be allowed access during those times only.

You can also set each user’s Allowed Sources to his or her own PC. Then Alice and Bob will each be allowed access only during their defined times and only from their own PCs.

On the other hand, suppose you want to restrict Alice to using only FTP and Bob to using only TELNET. Then you really do have to define separate groups, for example, GrpFTP and GrpTELNET, and define Alice as a member (perhaps the only member) of the first group and Bob as a member (perhaps the only member) of the second group, and write two rules:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>GrpFTP@localnet</td>
<td>Any</td>
<td>ftp</td>
<td>UserAuth</td>
<td>Log</td>
<td>Gateways</td>
</tr>
<tr>
<td>GrpTELNET@localnet</td>
<td>Any</td>
<td>telent</td>
<td>UserAuth</td>
<td>Log</td>
<td>Gateways</td>
</tr>
</tbody>
</table>

If these are the only rules in the Rule Base which apply to the members of these groups, then they will be restricted to using the given services, because the default rule will deny them access to all other services.

The interplay between the group’s access privileges (as defined in the rule) and the users’ access privileges (as defined in the User Properties window) gives you considerable flexibility.

**Question: Is it possible to authenticate FTP through a Web browser? For example, when the user tries to download a file through the Web browser, he or she should have to enter a name and password. But, when we try this, we get an error message from the browser.**

When using a browser without defining a proxy in the browser, all HTTP requests use the HTTP protocol and all FTP requests use the FTP protocol. Only part of the FTP protocol is supported in this mode; only anonymous ftp requests can be performed.

When using a browser with a proxy defined for FTP (this is defined in the browser), the defined proxy should be an HTTP proxy and not an FTP proxy. There is no way of using an FTP proxy for FTP connections when the client is a Web browser — this is a limitation of the Web browser and not of VPN-1/FireWall-1.

When using this configuration, the connection between the browser and the proxy uses the HTTP protocol. It is up to the proxy to convert the request from the HTTP protocol of the FTP protocol:
The VPN-1/FireWall-1 HTTP Security Server does not support this kind of protocol conversion. So, if you wish to use the VPN-1/FireWall-1 to authenticate FTP requests from a Web browser, a second proxy which does support this kind of protocol conversion should be installed, and defined to VPN-1/FireWall-1 as the next HTTP proxy. This configuration is shown in FIGURE 10-4.

If you do not define a next proxy to VPN-1/FireWall-1, then you will get an error message “scheme ftp not supported” when you attempt to authenticate an FTP request.

For additional information, see “The HTTP Security Server in Proxy Mode” on page 147.

**Question: How can I go across two or more FireWalls for authenticated services?**

**TELNET**

This is easy enough to do with TELNET — just TELNET to one FireWall after the other in sequence, authenticating yourself each time, until you get to your final destination.

**HTTP**

For HTTP outbound connections, just define the VPN-1/FireWall-1 HTTP Authenticating Server as your proxy in the browser and you will get the authentication prompts, one after the other.

If you are using a Netscape browser or Internet Explorer 3.0, then the authentication for outbound HTTP (when VPN-1/FireWall-1 is defined as a proxy to the browser) and inbound HTTP is done separately, that is, the user is prompted for each authentication separately, as he or she moves outward from the client.

For HTTP inbound connections, enter the list of passwords and users in reverse order. Since a password or user name can include a @ character, the passwords in the list are separated in an unusual way:

Suppose you have $n$ FireWalls, as in FIGURE 10-5:
FIGURE 10-5n HTTP Authenticating FireWalls

After the \( n \)th user enters 2\(^{n-2} \) characters, followed by the \( n-1 \)th user and 2\(^{n-3} \) characters, etc.

\[
\text{HttpUser}(2^{n-2}) \text{HttpServerIP@FW}_n \text{User}(2^{n-2}) \text{FW}_n \text{IP}@FW_{n-1} \text{User}(2^{n-3}) \text{FW}_{n-1} \text{IP} ... @FW_2 \text{User}@FW_2 \text{IP}
\]

SMTP

Question: When the VPN-1/FireWall-1 SMTP Security Server detects an error, I expect that it will notify the sender of the mail message (assuming the Notify Sender on Error field is checked in the SMTP Resource definition). Instead, I get a “connection to original-MTA failed” error message in the log.

This situation arises when there is no SMTP server between the sender and the VPN/FireWall Module. To understand what is happening, consider the networks in FIGURE 10-6.

FIGURE 10-6 “connection to original-MTA failed”

Suppose a message sent from localnet is rejected by the VPN-1/FireWall-1 SMTP Security Server. If Notify Sender on Error is checked, then the Security Server will attempt to send a mail message to the original source. If that source is running Windows, there will usually not be a mail server listening on port 25, and the result will be the “connection to original-MTA failed” message in the log. Unix workstations usually do have mail servers installed on port 25.
On the other hand, if the original mail message arrives at the VPN-1/FireWall-1 SMTP Security Server from the Internet, then there will be a mail server on the return path and the notification will be successful.

In practice, this is rarely a problem, since nearly all mail messages will have passed through a mail server before arriving at the VPN-1/FireWall-1 SMTP Security Server.

**Logging**

**Question: How Can I Do a Statistical Analysis of My Log File?**

There are several ways to do this:

- Check Point offers a Reporting Module product, which enables you to generate sophisticated reports analyzing your log data.
- Use the command `fw log` and redirect its output to a file. You can then parse the file with standard Unix tools like `perl`, `sort`, `awk`, or `sed`. Alternatively, the file can be used as input to database or spreadsheet programs.

You can also export the Log File by choosing **Export** in the **File** menu, or with the `fw logexport` command (see “fwm logexport” on page 600 of *Check Point SmartCenter Guide*).

- You can access log data using the OPSEC LEA API.

**Question: Some Log entries refer to rule zero (or to rules with negative numbers!), but there are no such rules in the Rule Base.**

**Rule Zero**

Rule zero is the rule VPN-1/FireWall-1 adds before the rules in Rule Base to implement Anti-Spoofing, dropping of packets with IP options, and some aspects of authentication. Anti-spoofing is implemented before any rules are applied, so anti-spoof track logging shows rule zero as the relevant rule.

For example, if a user fails to log in to an authentication server, then the log shows rule zero because at the time of the failure, the relevant rule (that is, the rule under which the user would have been granted or denied access had the login been successful) is unknown, since the requested service is unknown.

**Rules with Negative Numbers**

These are rules added by VPN-1/FireWall-1 to implement certain features. For example, a log entry generated as a result of an `fw sam` command (see “fwm sam” on page 572 of *Check Point SmartCenter Guide*) carries a negative rule number.

**Question: Is there any way I can choose to not log certain services? My Log File is filling up with recurring traffic through certain ports, and I don’t know what these services are.**
If you do not know what a service is, then it is probably best (from a security point of view) to block it. You should not be allowing communications unless you know what they are, so your first priority should be to identify the nature of the unknown traffic.

If you want to accept a service, but you do not want it to be logged, then define a rule (early in the Rule Base) that accepts the service without logging the connection.

**Question:** In my Log Viewer, I see some entries where my internal router is the Source and the protocol is ICMP. I have no idea what these entries are, or whether I should be concerned about them.

Some routers send ICMP packets from time to time, and you need not be concerned about it. You can remove the Log entries by adding a rule to the Rule Base that accepts ICMP packets from the internal router but does not log them.

**Question:** How can I switch my Log File on a periodic basis?

Extensive Log File management capabilities are configurable in the **Logging Policy** page of the network object’s **Properties** window (see Chapter 5, “Network Objects of Check Point SmartCenter Guide”).

**Security**

**Question:** Does Packet Reassembly Pose a Security Risk?

VPN-1/FireWall-1 performs virtual packet reassembly, and does not send a packet until all its fragments have been collected and inspected. The algorithm used is stricter than the standard packet reassembly algorithm, and does not permit overlays.

*Note*: Since IP specifications forbid a router from reassembling IP fragments, VPN-1/FireWall-1 does not send the reassembled packet but rather the fragments as VPN-1/FireWall-1 received them. This is the meaning of the term “Virtual Defragmentation.”

**Question:** Do Aliased (or Virtual) Interfaces Pose a Security Risk?

VPN-1/FireWall-1 ignores virtual interfaces, so that inspection and anti-spoofing is performed on the physical interface.

If you want to use virtual interfaces with anti-spoofing, you must define two network objects, one for each subnet, and then create a network group which consists of the two network objects. Then you can put the group in the physical interface’s anti-spoofing entry, just as you would if there were another physical network connected to the interface.

**Question:** How does VPN-1/FireWall-1 prevent session hijacking?
VPN-1/FireWall-1’s Encryption feature is the best solution, if you are concerned about this problem. Encryption would prevent hijacking by anyone who does not have the key.

**Question: How does VPN-1/FireWall-1 prevent attacks based on TCP sequence number prediction?**

Here too, VPN-1/FireWall-1’s Encryption feature is the best solution. Even if the attacker knows the sequence number, he or she would be unable to interfere with the encrypted connection.

It is recommended that you:
- Configure anti-spoofing properly.
- Enable SYN Relay, which causes the VPN/FireWall Module to assign sequence numbers using a cryptographic function — this solves the problem of the original server assigning vulnerable sequence numbers.

**Question: How does VPN-1/FireWall-1 Deal with IP Options?**

VPN-1/FireWall-1 drops packets with IP options, because they are considered to pose a serious security risk.

**Question: Is a FireWalled Host Not Secured When It Re-boots?**

If IP Forwarding is correctly set in the operating system, then there is no time during the re-boot process during which a protected network is not secured. For further information, see “Control of IP Forwarding” on page 296.

For information about protecting the FireWalled host itself during the re-boot process, see Chapter 7, “Boot Security”.

**Question: Can VPN-1/FireWall-1 secure modem connections?**

VPN-1/FireWall-1 can secure modem connections provided that:
- the modem is “in front” of the VPN/FireWall Module, and
- the dial-up lines provide PPP or SLIP connections

If both these conditions are true, then VPN-1/FireWall-1 treats connections via the modems the same way it treats connections via Ethernet, token ring, etc.

**VPN-1/FireWall-1/n (VPN-1/FireWall-1/25, VPN-1/FireWall-1/50, etc.) Issues**

**Question: How are these products restricted?**
VPN-1/FireWall-1 products enforce restrictions based on the number of protected hosts. If these restrictions are exceeded, VPN-1/FireWall-1 will issue an error message. These restrictions are:

- **number of internal hosts**

  Up to \( n \) nodes behind the gateway are allowed, where \( n \) is the number in the product name. For example, VPN-1/FireWall-1/50 is restricted to 50 nodes, VPN-1/FireWall-1/250 is restricted to 250 nodes, etc.

  A node is defined as a computing device with an IP address. A multi-user computer with one IP address is counted as one node.

  This restriction relates to the number of protected hosts. Every host behind VPN-1/FireWall-1 is protected by VPN-1/FireWall-1, even if no connections to the outside are initiated from that host.

  Every node protected by VPN-1/FireWall-1 is counted against the limit, even if its IP address is hidden from VPN-1/FireWall-1 by a proxy or by other means.

- **number of external interfaces**

  For all VPN-1/FireWall-1/n products, multiple external interfaces may be connected to the FireWalled machine, but IP forwarding will not be allowed between external interfaces.

  There is no restriction on the number of internal interfaces on the FireWalled machine.

- **no external Modules**

  An additional restriction for these products is that they cannot manage external VPN/FireWall or FloodGate Modules, that is, the Management Server (on which the Check Point database and files reside) and the VPN/FireWall and FloodGate Module must both be on the same machine. However, the GUI Client can be installed on a different machine from the Management Server. This configuration is sometimes referred to as a Client/Server configuration.

  **Note** - If you exceed the restriction on the number of protected hosts, VPN-1/FireWall-1 will display warning messages on the system console notifying you that you have violated the terms of the VPN-1/FireWall-1 license. You should immediately upgrade to the appropriate product in order to be in compliance with the terms of the VPN-1/FireWall-1 license. In the meantime, your security is not compromised and VPN-1/FireWall-1 will continue to protect your network.
**Supported Protocols and Interfaces**

**Question: Does VPN-1/FireWall-1 inspect non-IP packets, for example IPX packets?**

VPN-1/FireWall-1 provides security (access control) only for IP packets, and not for packets of other protocols (see TABLE 10-4 below for details).

**TABLE 10-4 non-IP protocols**

<table>
<thead>
<tr>
<th>On these platforms ...</th>
<th>VPN-1/FireWall-1 ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris</td>
<td>... passes only IP or ARP packets, and drops all other packets.</td>
</tr>
<tr>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>Windows 2000</td>
<td></td>
</tr>
<tr>
<td>Nokia</td>
<td>... passes all packets to the appropriate stack (without enforcing any access control).</td>
</tr>
<tr>
<td>Windows NT 4.0</td>
<td></td>
</tr>
<tr>
<td>AIX</td>
<td></td>
</tr>
</tbody>
</table>

**Question: Does VPN-1/FireWall-1 support the Talk protocol?**

VPN-1/FireWall-1 does not currently support the Talk protocol.

**Question: Does VPN-1/FireWall-1 support PPP, PPPoE, SLIP and X.25?**

VPN-1/FireWall-1 supports PPP, PPPoE, SLIP and X.25, but these interfaces must be installed before VPN-1/FireWall-1 starts.

**Question: Does VPN-1/FireWall-1 support Kerberos?**

VPN-1/FireWall-1 supports the Kerberos service, but the Kerberos authentication scheme is not supported.

**Question: Are there any special considerations for ISDN interfaces?**

If you are implementing a default Security Policy (see “Control of IP Forwarding” on page 296 for additional information) on a gateway with ISDN interfaces, VPN-1/FireWall-1 will not recognize the ISDN interfaces. The reason is that during the boot process, the ISDN interfaces are loaded just after the default Security Policy. When the real Security Policy is loaded, VPN-1/FireWall-1 “knows” that it has been loaded before, so it does not scan for new interfaces. There are several possible solutions to this problem:

- Disable the default Security Policy, at the cost of leaving the gateway exposed during the boot process.
- Deploy the default Security Policy only after the ISDN interfaces have been configured, exposing the gateway until that point.
Since the gateway is only connected to the Internet after the ISDN interfaces are configured, this solution entails a relatively short period of vulnerability.

- Leave the default Security Policy in its normal place and configure the ISDN interfaces after the real Security Policy is loaded.

In Unix systems, you will get an error message when you add the ISDN interfaces, and you must then uninstall the VPN-1/FireWall-1 kernel and install it, as follows:

```
fw ctl uninstall
fw ctl install
fw fetch localhost
```

**Question: How Can I Handle Multicast?**

Firewall–1 does not treat multicast as a special case, so for VPN-1/FireWall-1, a multicast packet is simply an IP packet with a class D (224.0.0.0 — 239.255.255.255) destination address.

If you wish to specify a rule which will apply to all multicast packets, define a network object (of type network) whose IP address is 224.0.0.0 and whose netmask is 240.0.0.0. This network will encompass all legal multicast destination addresses.

To use multicast with Anti-Spoofing, add the multicast network to all the interfaces to which multicast packets might be sent. You must do this because Anti-Spoofing checks both the destination and source IP addresses.

**Inspecting**

**Question: How is a Security Policy enforced on a host's different interfaces?**

The Security Policy (the Rule Base and the properties defined in the Global Properties window) is enforced for both incoming and outgoing packets, on all interfaces.

In previous versions of VPN-1/FireWall-1, the **Apply Gateway Rules to Interface Direction** property controlled how the Rule Base and Properties were enforced on gateways for incoming and outgoing packets. This property no longer exists, and Rule Base is enforced on all incoming and outgoing packets, on all interfaces.

**Question: How can I protect my internal hosts from each other?**

Consider the following configuration:
Assume that the Security Policy installed on the gateway does not allow TELNETs to the hosts in localnet. What happens when 194.0.0.2 TELNETs to 194.0.67.14?

The answer is that this TELNET is allowed, because the connection does not pass through the FireWall. 194.0.67.14 responds to 194.0.0.2’s ARP request, and 194.0.0.2 routes the connection directly to 194.0.67.14. VPN-1/FireWall-1 on the gateway does not see the connection and does not inspect it.

**Question: When is a Modified Security Policy Implemented?**

Changes are implemented when the Security Policy is installed. The only time it is necessary to stop VPN-1/FireWall-1 and restart it is after a FireWalled host’s physical interfaces have changed.

**Question: How should VPN-1/FireWall-1 be stopped?**

The correct way to stop VPN-1/FireWall-1 is with the `cpstop` command. If you kill the VPN-1/FireWall-1 daemon, the VPN/FireWall Module continues to operate, but there is no logging or authorization, and no new encryption sessions can be started.

Note that when you stop VPN-1/FireWall-1, your network is completely exposed. Disabling IP forwarding will protect the networks behind the gateway, but the gateway itself will still be exposed. The only way to protect the gateway in this case is to physically disconnect the network cables.

**Administrative Issues**

**Question: Are there any security hazards the administrator should be aware of when using VPN-1/FireWall-1?**
VPN-1/FireWall-1 provides transparent connectivity to all Internet resources.

Some client-server implementations may pose security hazards, e.g., older versions of sendmail. The administrator should ensure that any application is safe to use before authorizing its use through a firewall. Since VPN-1/FireWall-1 enables the administrator to authorize any application, he or she has to carefully examine each one and assess the risk of allowing the use of that particular application (client or server).

**Question: Unregistered IP Addresses**

VPN-1/FireWall-1 enables using a large number of unregistered or concealed internal IP addresses by presenting on external traffic only a small number of registered IP addresses.

VPN-1/FireWall-1’s Address Translation feature enables a network to use unregistered Internet addresses or to hide the internal IP addresses. For additional information, see Chapter 2, “Network Address Translation (NAT).”

**Question: How Does VPN-1/FireWall-1 Address Vulnerable Applications?**

To address vulnerable applications, VPN-1/FireWall-1 can be set up to allow inbound connections of a particular service only to a specific server that has been enhanced to handle possible failures. For example, all inbound SMTP traffic can be directed to a server running an enhanced version of sendmail. By providing such an open solution, the administrator can always acquire the latest and best application for any desired platform.

**Performance**

**Question: Does VPN-1/FireWall-1 Introduce Performance Degradation?**

The VPN-1/FireWall-1 Kernel Module itself introduces practically no performance degradation, but encryption, Accounting and Live Connection features do have a measurable impact on performance.

**Question: What are the Guidelines for Improving VPN-1/FireWall-1 Performance?**

**General Performance Guidelines**

Multiple CPUs will improve performance for certain configurations (for example, Security Servers and encryption).

Hardware acceleration is available for encryption.

Check Point load sharing solutions can distribute loads across multiple Modules.
Installing a Security Policy on a remote VPN/FireWall Module can often be speeded up by listing both machines in the `hosts` (Unix) or `lmhosts` (Windows) files.

VPN/FireWall Module

VPN-1/FireWall-1 performance depends on the hardware, the Security Policy, and the characteristics of the network traffic. While the Firewall is inspecting packets, the time of handling a packet spends in the kernel increases. The conclusion is that VPN-1/FireWall-1 has a greater impact on latency (connection latency or transaction latency) and less on the bandwidth.

Benchmarks have shown that, while there is usually little throughput degradation, the latency may well be significantly degraded in some cases. This degradation can as a rule, be successfully addressed. Acquiring faster hardware is always helpful. In addition, the following suggestions should improve performance as well:

Keep the Rule Base simple.

Performance degrades when there is a very large number of rules, or when the rules are complex.

Position the most frequently applied rules first in the Rule Base.

For example, if most connections are HTTP packets, the rule which accepts HTTP should be the first rule in the Rule Base. Be sure to keep this rule as simple as possible.

Properties

- Decrypt on accept

This property should be disabled if you are not using Encryption or SecuRemote.

Overhead

Logging, Accounting, Encryption, Network Address Translation and Security Servers all degrade performance to some extent.

Logging, Accounting and Security Servers add I/O overhead and context switches. The degradation in performance might be significant if they are used in frequently applied rules.

Question: How can I estimate VPN-1/FireWall-1’s memory usage?

You can find out how much memory is available by using the following command:

```
fw ctl pstat
```
Each session requires about 120 bytes of memory, more if the session is authenticated or if Network Address Translation is applied.

In addition, there is some static overhead as well.

The VPN/FireWall Module does not release the memory used by a session until about 50 seconds after the session ends, so if there are many sessions significantly shorter than a minute, the VPN/FireWall Module needs more memory than the number of active sessions would indicate.

For HTTP, each URL access is a separate session.

The general formula is:

\[
\text{MemoryUsage} = \frac{(\text{ConcurrentConnections})}{(\text{AverageLifetime})}\times(\text{AverageLifetime} + 50 \text{ seconds})\times120
\]

**Question: To What Extent is VPN-1/FireWall-1 Fault Tolerant?**

The VPN/FireWall Modules will continue inspecting and reporting logs, alerts, and status even if the Master is not active for any reason (host went down, application exited, etc.). Users can define multiple default Masters to which the VPN/FireWall Modules will report logs, alerts, and status in the event that the first Master is unavailable. The status and statistics of VPN/FireWall Modules can be monitored constantly by a number of SmartCenter Servers or SNMP platforms. If the VPN/FireWall Module host is rebooted, the VPN/FireWall Module can be loaded automatically and brought up with the latest Security Policy installed. The VPN/FireWall Module can also be configured to fetch its Security Policy from various SmartCenter Servers every time it boots.

A Check Point Module can log locally if its Log Server is unavailable, and then automatically resume sending logs when the Log Server becomes available again. Logs can also be sent to multiple Log Servers simultaneously.

High Availability can be configured for:

- VPN/FireWall Modules — see Chapter 5, “ClusterXL” of *Check Point FireWall-1*.
- SmartCenter Servers — see Chapter 17, “Management High Availability” of *Check Point SmartCenter Guide*.
- Encryption — see Chapter 12, “Clustering Solutions for VPN Connections” of *Check Point Virtual Private Networks*.

The SNMP daemon is used to report status and even if it dies, the only thing that would happen is that in Firewall/VPN’s Status Window or on the SNMP platform, the user would see that it is no longer possible to communicate with the daemon.
The Firewall/VPN daemon (\texttt{fwd}) is used to control the VPN/FireWall Module. If it dies, the user would not be able to control it, but the VPN/FireWall Module would continue to enforce the Security Policy that was last loaded.

As long as a gateway is up and routing, all packets are subject to VPN/FireWall Module inspection. If the gateway reboots, the VPN/FireWall Module is immediately loaded into the kernel and the latest Security Policy is loaded into it and enforced. VPN-1/FireWall-1 can be configured so that IP Forwarding is enabled only when the Security Policy is being enforced (see “Control of IP Forwarding” on page 296 for additional information).

The VPN/FireWall Module keeps a local copy of the latest Security Policy, so that even if the SmartCenter Server is down when the gateway reboots, the VPN/FireWall Module will still load the latest Security Policy.

With respect to logging, the VPN/FireWall Module can be configured to send logs and alerts to a certain host (the Master). If the Master is not available, the VPN/FireWall Module can be configured to attempt logging to another host, and another and another. Even if logging fails, the VPN/FireWall Module will still continue to function.
Index

A
access  limiting to specific ports 331
accounting  and synchronized FireWalls 249
aliased interfaces 338
anti-spoofing  virtual interfaces 338
Apply Gateway Rules to Interface Direction property 342
ARP configuration  special considerations for NAT 82
ARP requests 79
authenticated services  going across two or more FireWalls 335
authentication  authentication methods 124
authentication schemes 125
comparison of different types 125
High Availability 248
transparent authentication 126
when to use each type 125
Authentication methods 124
authentication scheme  number per user 126
automatic ARP configuration  two gateways responding for same NATed address 82
AXENT Pathways Defender 126, 149

B
boot security  default filter 295
fwstop -proc 295
fwstop-default 295
Initial Policy 295
IP Forwarding 295

C
cable failure 252
Chaining 133
Check Point SNMP daemon 307
Client Authentication 135
authorizing services 177, 183
configuring 177
configuring support for HTTPS 201
defining on a per-user rather than a per-group basis 333
High Availability 248
logging, example of 189
overview 173
sign on methods 174
signing on through a Web browser 197
Single Sign On System Extension 190
timeouts 184
tracking 184
Client Authentication Sign On Methods
agent automatic sign on 176
fully automatic sign on 175
manual sign on 174
manual sign on through a Web browser 197
manual sign on using TELNET 193
partially automatic sign on 175
single sign on 176
using agent automatic sign on 199
using fully automatic sign on 198
using partially automatic sign on 197
Cluster control protocol 244
ClusterXL commands 278
color 284, 285, 290
configuration  Security Servers 237
ConnectControl
server load balancing 319
connection to original-MTA failed error message 336
Content Security 205
Content Vectoring Server, see CVP Server
cphaprob command 252
cpstop  and killing the fw daemon, difference between 343
cpstop-default 295
cross cable 244
CVP Inspection
step by step procedure 234
CVP Server  how it is invoked 229
returning data 235
step by step procedure for using 235
dedicated hub 244
Default Filter 295
default route 79
default Security Policy verifying that it is loaded 301
Denial of Service attack 18
DHCP 191
DNS  over TCP 33
DNS verification 33
DNS, dual 331
domain load balancing algorithm 322
Domain Controller 191
echo-reply 332
Logical Servers 325
Wait Mode 188
echo-request 332
Logical Servers 325
Wait Mode 188
eitherbound 342
encryption
and synchronized FireWalls 248
using with NAT on the same system 118
enterprise ID 309
er 137
error message
"connection to original-MTA failed" 336
external FireWall Module not managed by FireWall-1/ n 340
external interface hiding IP address 71
external interfaces restricted number of 340

gateway hiding IP address of external interface 71
gateways defining interfaces as separate objects 331
guidelines performance 344

failover
definition 252
when does it occur 252
fault tolerance 346
FireWall synchronization implementation 244
overview 243
FireWall-1 HP OpenView Extension installing 311
FTP 125
authenticating through the HTTP Security Server 334
file names logged for authenticated sessions 207
from HTTP 332
get and put logged for User Authenticated FTP 207
User Authentication 125
FTP daemon 333
FTP proxy defining to browser 332, 334
FTP resource matching 211
FTP resources command matching 212
file name matching 212
matching 211
FTP Security Server 36
fw-1 spool directory 217
FW1_chntauth 203
fwauthd.conf 203
fwstop -proc 295

G

GATEWAY

httpd.conf 203

H

H.225 284
H.245 284, 286
H.323 281, 282
H.323 Gatekeeper 283
H.323 Gateway 283
H323_ras_only 288
hardware acceleration 344
high availability
and Log Viewer 280
avoiding network conflicts 271
commands 278
different Management Modules 248
different Security Policies 248
encrypting connections between synchronized FireWalls 248
from Load Sharing configuration 274
overview 250
protecting the machines 258
resources 249
secured interfaces 244
Security Servers 249
SIC 258
switches and hubs 271
synchronizing different version VPN/FireWall Modules 248
synchronizing VPN/FireWall Modules on different platforms 248
user authenticated connections 248
using non-routable IP addresses 258
hijacking sessions 338
hostname command 329
hosts file 345
Hosts, Gateways and Interfaces distinction between 328
HP
FireWall-1 HP OpenView extension 310
HP OpenView Extension installing 310
specifying the Management Server for FireWalled objects 314
HP OpenView, see FireWall-1 HP OpenView extension
HTTP
allowing FTP sessions from 332
restraining inbound 146
restraining outbound 146
User Authentication 125
using a Server for Null Requests 160
using reauthentication options 145
HTTP Security Server 44
as proxy 217
configuring multiple ports 152
defining as a Security Proxy 149
defining as an HTTP proxy 148
error messages 152
overview 143
putting a proxy behind 132, 143
support for FTP 217
support for HTTPS 219, 221
HTTP Servers defining 144
HTTPS
authenticating outbound 149
using URI Resource rules with 220
with non-transparent authentication 155

I

IANA 86
ICMP
in.telnetd 332
inetd.conf 332
Initial Policy 295
Install On field
NAT tab 88
Insufficient Information
problem 208
interface
secured 244
interface failure 252
Interfaces 244
interfaces
aliased 338
defining a gateway's interfaces as separate objects 331
defining as an object 331
how Security Policy is enforced on different 342
virtual 338
interfaces, external restricted in FireWall-1/50 and FireWall-1/250 340
internal hosts
license restriction exceeded 340
number restricted in FireWall-1/n 340
too many 340
internal interfaces
number not restricted 340
Internet
defining to FireWall-1 327
intrusion attempts
detecting 52
IP address
configuration of 272
multiple machines with identical IP address 83
non-unique 259
unique 259
IP addresses
hiding 344
unregistered 344
IP Forwarding 295
IP Options 339
IPX packets
inspecting 341
ISDN interfaces 341

Legacy CPHA
example network
configuration 257
lmhosts file 345
Load agents port property 326
load balancing
servers 319
step by step instructions 322
load balancing algorithms 322
Load measurement Interval property 326
load measuring 325
Load Sharing 83
adding cluster members 274
commands 278
configuring sharing method 276
every example network
configuration 255
from a High Availability configuration 268
from a single gateway machine 260
switch settings 275
load sharing 344
local.arp file 82
log
rule number zero 337
rule with negative number 337
Log File
analysis of 337
periodically switching 338
statistical analysis of 337
log viewer
and High Availability 244
Logical Server 322
echo-request, echo-reply 325
persistent server mode 321, 323, 324
using HTTP Logical Servers in rule 325
Logical Servers
step by step instructions on using 322

MAC address 258
automatic configuration of 272
on Solaris and Linux 272
on Windows 272
format 82
High Availability 259
in local.arp file 82
NAT 79
shared 272
MEP 133
MIB 308, 309
chkpnt.mib file 308
chkpnt.mib file source code 314
Microsoft SNMP daemon 307
modem connections
securing 339
multicast 342
multiple CPUs 344

N
NAT
and encryption 118
and Tunnel mode 120
automatic ARP configuration 82
communications between hosts in different internal networks 110, 111
compound conditions 92
defining rules automatically 87
FTP port command 87
gateway with three interfaces 106
gateway with two interfaces 102
Hide mode 70, 71
Hide Mode limitations 72
Hiding Behind 0.0.0.0 75
hiding the gateway's internal address 117
internal host with illegal IP address tries to communicate with external host with same IP address 120
multiple translation 93
need for 67
reply packets 79
restrictions on sqlnet2 service 86
routing considerations 78
Rule Base 112
Static Destination mode 77
Static Source mode 75
translating both source and destination 93

K
Kerberos 341

L
LEA 337

M
MAC address 258
automatic configuration of 272
on Solaris and Linux 272
on Windows 272
format 82
High Availability 259
in local.arp file 82
NAT 79
shared 272
MEP 133
MIB 308, 309
chkpnt.mib file 308
chkpnt.mib file source code 314
Microsoft SNMP daemon 307
modem connections
securing 339
multicast 342
multiple CPUs 344

N
NAT
and encryption 118
and Tunnel mode 120
automatic ARP configuration 82
communications between hosts in different internal networks 110, 111
compound conditions 92
defining rules automatically 87
FTP port command 87
gateway with three interfaces 106
gateway with two interfaces 102
Hide mode 70, 71
Hide Mode limitations 72
Hiding Behind 0.0.0.0 75
hiding the gateway's internal address 117
internal host with illegal IP address tries to communicate with external host with same IP address 120
multiple translation 93
need for 67
reply packets 79
restrictions on sqlnet2 service 86
routing considerations 78
Rule Base 112
Static Destination mode 77
Static Source mode 75
translating both source and destination 93
valid external address for Hide Mode 74
NAT Hide total number of connections 72
NAT rules advantages of generating automatically 70
network object on network 327
network objects which are on my network? 327
node definition of 340
number restricted in VPN-1/FireWall-1/n 340
non-ARP packets 341
non-IP packets 341
non-IP protocols support for 341
Non-Transparent Authentication and HTTP 154
Non-transparent Authentication prompt_for_destination parameter 141
non-unique IP address 259
Notify Sender on Error field 336
NT configuring NAT on 82

Perform destination translation on the client side 84
performance improving 344
performance guidelines 344
period of vulnerability 342
persistency Logical Servers 323
physical address 79
ping allowing unrestricted 332
ping of death 21
Policy Server 135
port 161
failure to bind to 308
ports limiting access to specific ports 331
PPP 341
PPPoE 341
prompt_for_destination User Authentication 141
protocol which available on network? 329
proxy putting behind VPN-1/FireWall-1 HTTP Authenticating Server 132, 143
proxy ARP method 81

RFC 1631 compliant NAT 68
RFC 1918 86
RFC 791 21
RLOGIN User Authentication 125
round robin load balancing algorithm 322
round trip load balancing algorithm 322
RTP/RTCP 265, 287
Rule Base adding a new rule 94
deleting rule from 101
direction of enforcement 342
number of rules supported 331
sequential application of rules, exception to 208
using ping in 332
rule zero in Log Viewer, meaning of 337
rules adding to Rule Base 94
deleting from Rule Base 101
rules, see also Security Policy

S

S/Key 125
SecureClient 135
secured interfaces
High Availability 244
SecuRemote Client 134
SecuRemote Server 134
SecurID 125
Security Policy and ISDN interfaces 341
modified, when implemented 343
Security Servers 205
configuration file 237
FTP resource matching 211
incoming connections 211
interaction with OPSEC products 222
outgoing connections 211
using to authenticate other services 240
server load load balancing algorithm 322
server load balancing 319
how it works 320
services dependence on other services 330

O

objects_5_0.C file 141, 142, 169, 263, 333
Open Platform for Secure Enterprise Connectivity, see OPSEC
OpenView, see FireWall-1 HP
OpenView extension OPSEC 229, 234
OPSEC-certified products obtaining evaluation copies 234

P

packet reassembly 338
security risks associated with 338
Passive SYN Gateway deployment guidelines 64
description of 63
passwords number per user 126

Q

Q.931 284

R

RADIUS 125
random load balancing algorithm 322
RAS 288
Redirect queries to other UA gateway 134
Redirect queries over VPN tunnel 133
Redirect queries to backup gateways 133
Reporting Module 337
resources
High Availability 249
RFC 1035 33
RFC 1631 87

RFC 1631 compliant NAT 68
RFC 1918 86
RFC 791 21
RLOGIN User Authentication 125
round robin load balancing algorithm 322
round trip load balancing algorithm 322
RTP/RTCP 265, 287
Rule Base adding a new rule 94
deleting rule from 101
direction of enforcement 342
number of rules supported 331
sequential application of rules, exception to 208
using ping in 332
rule zero in Log Viewer, meaning of 337
rules adding to Rule Base 94
deleting from Rule Base 101
rules, see also Security Policy
which available on network? 329
which have more than one type 330
Session Authentication configuring overview 162
Session Authentication Agent required for Session Authentication 125
Session Authentication agent configuring 165
pre-configuring 168
session hijacking 338
preventing 338
Single Sign On System Extension 190
SIP 281, 289
SIP Domain 289
SIP Proxy 288
SIP Redirect Server 288
SIP Registrar 288, 292
SLIP 341
SMTP Security Server 48, 213, 336
configuration file 215
supported protocols 215
SNMP daemon
Check Point 307
initial keys 308
initial communities 308
Microsoft 307
optional 308
read and write communities (keys) 308
SNMP traps 309
snmp.C file 308
Specific Sign On 183
sqlnet2 and NAT 86
SSL encryption 237
Standard Sign On 183
Static Destination mode 77
Static Source mode 75
Stealth Authentication 137
subnet
more than one VPN/FireWall Module on the same 83
suspicious events
detecting 52
switches
setting for Load Sharing 276
SYN Attacks 58
SYN Gateway
description of 61
SYN Relay
description of 63
TCP sequence number 339
synchronization
timing issues 247
synchronized FireWall Modules restrictions on implementation 248
synchronized FireWalls restrictions 248
synchronizing VPN/FireWall Modules on different platforms 248
SYNDefender 58
deployment guidelines 64
maximum number of protected sessions 30
SYNRelay
deployment guidelines 65
T 241
T.120 288
TACACS 126
Talk protocol 341
TCP
NAT Hide mode 71
TCP sequence number prediction 339
TCP Zone Transfer 33
TELNET
User Authentication 125
VPN-1/FireWall-1 daemon 332
TELNET daemon 333
timing issues
tsynchronization 247
too many internal hosts 340
Transparent Authentication 126
trusted interfaces
High Availability 244
Tunnel Mode and NAT 120
two or more FireWalls going across for authenticated services 335
UDP
NAT Hide mode 71
UDP port 18212 326
UFP Server
step by step procedure for using 231
unique IP address 259
Unix
configuring NAT on 81
URL Filtering 231
URL filtering
step by step procedure 231
user
number of authentication schemes 126
number of passwords 126
User Authentication defining on a per-user rather than a per-group basis 333
deployment 127
entering user name and password 138
High Availability 248, 249
overview 127
tracking and timeout parameters 130
UserAuthority Gateway 133
V 338
virtual interfaces 338
virtual packet reassembly 338
Voice over IP, see VoIP
VoIP 281
VPN/FireWall Modules restrictions on synchronization 248
VPN-1/FireWall-1 administrative issues 343
killing the daemon and for stop, difference between 343
stopping 343
VPN-1/FireWall-1 daemon stopping 301
VPN-1/FireWall-1 HP OpenView extension
default SNMP port for FireWall objects 313
FireWall discovery 312
VPN-1/FireWall-1 password advantage over OS password 125
VPN-1/FireWall-1 SNMP daemon 307
VPN-1/FireWall-1 SNMP daemon 307
W

Wait Mode
  echo-request, echo-reply  188
www.opsec.com  222

X

X.25  341