FireWall-1 and SmartDefense

Express CI (R57)

IMPORTANT
Check Point recommends that customers stay up-to-date with the latest service packs and versions of security products, as they contain security enhancements and protection against new and changing attacks.

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

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

See the latest version of this document in the User Center at:

http://www.checkpoint.com/support/technical/documents

April 2005
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 222-277-103 and FAR 52.227-19.

TRADEMARKS:
Check Point, the Check Point logo, ClusterXL, ConnectControl, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FireWall-1 SmallOffice, FireWall-1 VX, FireWall-1 XL, FloodGate-1, INSPECT, INSPECT XL, IQ Engine, MultiGate, Open Security Extension, OPSEC, Provider-1, SecureKnowledge, SecurePlatform, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, SmartDashboard, SmartDefense, SmartSLM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SmartConsole, TurboCard, Application Intelligence, SVN, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Net, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 SmallOffice and VPN-1 VX are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other trademark 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. 6,496,935, 5,606,668, 5,699,434 and 5,835,726 and may be protected by other U.S. Patents, foreign patents, or pending applications.

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 management from Entrust.

Verisign is a trademark of Verisign Inc.

The following statements refer to those portions of the software copyrighted by the OpenSSL Project which are not based on works of the U.S. Government.

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 appear in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name of the OpenSSL Project not be used in advertising or publicity pertaining to distribution of the software without specific, written permission. This software is provided as is without express or implied warranty. Copyright 1996, 1997, 1998, 1999, 2000, and 2001 by Eric Young.

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

The OpenSSH software is a fork of the original SSH software. The OpenSSH software is provided by the openssh 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 series of authors, contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage. The following statements refer to those portions of the software copyrighted by the OpenSSL Project which are not based on works of the U.S. Government.

The following statements refer to those portions of the software copyrighted by the OpenSSL Project which are not based on works of the U.S. Government.

The following statements refer to those portions of the software copyrighted by the OpenSSL Project which are not based on works of the U.S. Government.
# Table Of Contents

## Chapter 1  Summary Of Contents

Structure of the Book 11  
Section 1: Network Access 11  
Section 2: Connectivity 11  
Section 3: SmartDefense 12  
Section 4: Application Intelligence 12  
Section 5: Web Security 12  
Appendices 13

## Chapter 2  FireWall-1 Access Control

The Need for Access Control 17  
FireWall-1 Solution for Secure Access Control 17  
Access Control at the Network Boundary 18  
The Security Rule Base 19  
Example Access Control Rule 19  
Rule Base Elements 20  
Implied Rules 20  
Preventing IP Spoofing 21  
New Services 23  
Considerations for Access Control 25  
Spoof Protection 26  
Simplicity 26  
Basic Rules 26  
Rule Order 27  
Topology Considerations: DMZ 27  
The X11 Service 27  
When to Edit Implied Rules 27  
Configuring Access Control 28  
Defining access Control Rules 28  
Defining a Basic Policy 28  
Configuring Anti-spoofing 30  
Configuration of Visitor Mode Blocking 31

## Chapter 3  Authentication

The Need for Authentication 33  
VPN-1 Pro Solution for Authentication 33  
Introduction to VPN-1 Pro Authentication 34  
Authentication Schemes 34  
Authentication Methods 36  
Choosing an Authentication Method 47  
Configuring Authentication 48
Creating Users and Groups  48
Configuring User Authentication  49
Configuring Session Authentication  50
Configuring Client Authentication  54
Configuring Authentication Tracking  55
Configuring a VPN-1 Pro Gateway to use RADIUS  56
Configuring a VPN-1 Pro Gateway to use SecureID  57
Configuring a VPN-1 Pro Gateway to use TACACS+  58

Chapter 4  Network Address Translation (NAT)
The Need to Conceal IP Addresses 63
Check Point Solution for Network Address Translation 64
  Public and Private IP addresses  64
  NAT in FireWall-1  65
  Static NAT  65
  Hide NAT  66
  Automatic and Manual NAT Rules  68
  Address Translation Rule Base  68
  Bidirectional NAT  69
  Understanding Automatically Generated Rules  69
  Port Translation  71
  NAT and Anti-Spoofing  72
  Routing Issues  72
  IP Pool NAT  74
  Disabling NAT in a VPN Tunnel  75
Planning Considerations for NAT 75
  Hide Versus Static  75
  Automatic Versus Manual Rules  75
  Choosing the Hide Address in Hide NAT  76
Configuring NAT 76
  General Steps for Configuring NAT  76
  Basic Configuration - Network Node with Hide NAT  77
  Sample Configuration - Static and Hide NAT  78
  Sample Configuration - Using Manual Rules for Port Translation  80
Advanced NAT Configuration 81
  Allowing Connections Between Translated Objects on Different Gateway Interfaces  81
  Enabling Communication for Internal Networks with Overlapping IP addresses  81
  SmartCenter Behind NAT  84

Chapter 5  ISP Redundancy
Need for ISP Link Redundancy 89
Solution for ISP Link Redundancy 90
  ISP Redundancy Overview  90
  ISP Redundancy Operational Modes  91
  Monitoring the ISP Links  92
  How ISP Redundancy Works  92
  The ISP Redundancy Script  94
  Manually Changing the Link Status (fw isp_link)  94
Chapter 9  Securing Voice Over IP (VoIP)

The Need to Secure Voice Over IP 155
Check Point Solution for Secure VoIP 156
  Introduction to the Check Point Solution for Secure VoIP 156
  Control Signalling and Media Protocols 157
  VoIP Handover 157
  VoIP Application Intelligence 159
  VoIP Logging 160
  Protocol-Specific Security: SIP, H.323, MGCP and SCCP 161
  Securing SIP Based VoIP 161
  Securing H.323-Based VoIP 167
  Securing MGCP Based VoIP 173
  Securing SCCP Based VoIP 178
Considerations for Secure VoIP 180
  Enforcing Handover 180
  Know Your Network Topology 180
Configuring VoIP 181
  Configuring SIP-Based VoIP 181
  Configuring H.323-Based VoIP 185
  Configuring MGCP-Based VoIP 191
  Configuring SCCP-Based VoIP 196
Troubleshooting SIP 201

Chapter 10  Securing Instant Messaging Applications

The Need to Secure SIP-based Instant Messenger Applications 203
Check Point Solution for Securing Instant Messengers 204
  Introduction to Instant Messenger Security 204
  Understanding Instant Messengers Security 204
  Logging Instant Messenger Applications 205
  NAT Support for MSN Messenger over SIP 205
Configuring SIP-based Instant Messengers 207
  Defining the Rule Allowing SIP-based Instant Messengers 207
  Configuring the SmartDefense Instant Messengers options 208
Chapter 11  Microsoft Networking Services (CIFS) Security
Securing Microsoft Networking Services (CIFS) 209
Restricting Access to Servers and Shares (CIFS Resource) 210

Chapter 12  FTP Security
Introduction to FTP Content Security 211
FTP Enforcement by the FireWall-1 kernel 211
FTP Enforcement by the FTP Security Server 212
  Control the Allowed Protocol Commands  212
  Maintaining Integrity of Other Protected Services  212
  Avoiding Vulnerabilities in FTP Applications  212
  Content Security  212
Configuring Restricted Access to Specific Directories 213

Chapter 13  CVP and UFP Content Security
The Need for Content Security 215
Check Point Solution for Content Security 216
  Introduction to Content Security  216
  Security Servers  217
  Deploying OPSEC Servers  218
  CVP Servers for Anti-Virus and Malicious Content Protection  220
  Using URL Filtering (UFP) to Limit Web Surfers  223
  The TCP Security Server  226
Configuring Content Security 226
  Resources: What They Are and How to Use Them  226
  Creating a Resource and Using it in the Rule Base  227
  Configuring Anti-Virus Checking for Incoming Email  228
  Configuring CVP Checking for Web Traffic with Improved Performance  230
  Performing CVP or UFP Inspection on any TCP Service  233
Advanced CVP Configuration: CVP Chaining and Load Sharing 234
  Introduction to CVP Chaining and Load Sharing  234
  CVP Chaining  234
  CVP Load Sharing  235
  Combining CVP Chaining and Load Sharing  236
  Configuring CVP Chaining and Load Sharing  237

Chapter 14  Web Intelligence
The Need for Web Attack Protection 241
The Web Intelligence Solution for Web Attack Protection 242
Web Intelligence Technologies 243
Web Intelligence Online Updates 243
Web Intelligence Security and Usability 244
  Web Server Focused Security  244
  Enforcement Granularity  244
  Configuration Flexibility  244
  Variable Security Levels  245
Chapter 15  Web Content Protection

Introduction to Web Content Protection 255
Web Content Security via the Security Rule Base 256
  What is a URI Resource? 256
  Filtering URLs, Schemes and Methods by Source and Destination 256
  Basic URL Filtering 257
  URL Logging 257
  Java and ActiveX Security 257
Securing XML Web Services (SOAP) 258
Understanding HTTP Sessions, Connections and URLs 259
  HTTP Request Example 259
  HTTP Response Example 260
  HTTP Connections 260
  Understanding URLs 261
Connectivity Versus Security Considerations for Web Surfers 261
  Allowing or Restricting Content 261
  Content Compression 262
Factors that Affect HTTP Security Server Performance 262
  The Number of Simultaneous Security Server Connections 263
  How To Run Multiple Instances of the HTTP Security Server 263
Configuring Web Content Protection 264
  Blocking URL-based Attacks using a URI Resource 264
  Configuring URL Logging 265
  Configuring Basic URL Filtering 265

Appendix A  Security Before
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>VPN-1 Pro Activation</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Achieving Security Before VPN-1 Pro Activation</td>
<td>269</td>
</tr>
<tr>
<td></td>
<td>Boot Security</td>
<td>269</td>
</tr>
<tr>
<td></td>
<td>Control of IP Forwarding on Boot</td>
<td>270</td>
</tr>
<tr>
<td></td>
<td>The Default Filter</td>
<td>270</td>
</tr>
<tr>
<td></td>
<td>The Initial Policy</td>
<td>271</td>
</tr>
<tr>
<td></td>
<td>Default Filter and Initial Policy Configuration</td>
<td>273</td>
</tr>
<tr>
<td></td>
<td>Verifying the Default Filter or Initial Policy is Loaded</td>
<td>273</td>
</tr>
<tr>
<td></td>
<td>Change the Default Filter to a Drop Filter</td>
<td>273</td>
</tr>
<tr>
<td></td>
<td>User-Defined Default Filter</td>
<td>274</td>
</tr>
<tr>
<td></td>
<td>Using the Default Filter for Maintenance</td>
<td>274</td>
</tr>
<tr>
<td></td>
<td>To Unload a Default Filter or an Initial Policy</td>
<td>275</td>
</tr>
<tr>
<td></td>
<td>If You Cannot Complete Reboot After Installation</td>
<td>275</td>
</tr>
<tr>
<td></td>
<td>Command Line Reference for Default Filter and Initial Policy</td>
<td>275</td>
</tr>
<tr>
<td></td>
<td><strong>Appendix B</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>FireWall-1 Command Line Interface</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Index</strong></td>
<td>281</td>
</tr>
</tbody>
</table>
CHAPTER 1

Summary Of Contents

Structure of the Book
This Guide is divided into a number of sections and chapters.
- Chapter 1, “Summary Of Contents” is this chapter.

Section 1: Network Access
This section describes how FireWall-1 controls and secures network access for users and resources.
- Chapter 2, “FireWall-1 Access Control” explains how to set up a security policy that fits the organizational requirements.
- Chapter 3, “Authentication” explains the available FireWall-1 authentication schemes (for username and password management), and authentication methods (how users can authenticate themselves).

Section 2: Connectivity
This section describes how network connectivity is established using FireWall-1.
- Chapter 4, “Network Address Translation (NAT)” describes the translation of IP addresses, most commonly for the purpose of providing Internet access to internal hosts with private IP addresses. Also described are some advanced NAT capabilities, such as enabling communication between internal networks with overlapping IP addresses, and working with a NATed SmartCenter Server.
- Chapter 5, “ISP Redundancy” describes how to assure reliable Internet connectivity by allowing a single or clustered FireWall-1 gateway to connect to the Internet via redundant Internet Service Provider (ISP) links.
- Chapter 6, “ConnectControl - Server Load Balancing” describes how to distribute network traffic among a number of servers, in order to reduce the load on a single machine, improve network response time, and provide high availability.
Section 3: SmartDefense

- Chapter 7, “SmartDefense” gives a conceptual overview of SmartDefense, which enables customers to configure, enforce and update network and application attack defenses. The integration with the DShield Storm Center is described in detail. For information about specific protections, see the SmartDefense HTML pages and the online configuration help.

Section 4: Application Intelligence

Some of the most serious threats in today's Internet environment come from attacks that attempt to exploit application vulnerabilities. Check Point Application Intelligence is a set of advanced capabilities, integrated into FireWall-1 and SmartDefense, which detect and prevent these application-level attacks. The chapters in this section explain how to protect against application-level attacks.

Note - Information about specific protections can be found in the SmartDefense HTML pages and the online configuration help.

- Chapter 9, “Securing Voice Over IP (VoIP)” explains how to secure VoIP traffic in H.323, SIP, MGCP and SCCP environments.
- Chapter 10, “Securing Instant Messaging Applications” explains how to secure SIP-based Instant Messengers. MSN Messenger in its SIP mode of operation, can be secured with an extra level of granularity.
- Chapter 11, “Microsoft Networking Services (CIFS) Security” explains how to secure Microsoft Networking Services by means of a CIFS resource, while meeting the high performance requirements of LAN security.
- Chapter 12, “FTP Security” explains how to configure FTP security through the Rule Base.
- Chapter 13, “CVP and UFP Content Security” explains how to use Content Vectoring Protocol (CVP) applications for anti-virus protection, and URL Filtering (UFP) applications for limiting access to web sites.

Section 5: Web Security

- Chapter 14, “Web Intelligence” describes the add-on for VPN-1 Pro that provides high performance attack protection for web servers and applications. It provides proactive attack protection by looking for malicious code and ensuring adherence to protocols and security best practice.
• Chapter 15, “Web Content Protection” describes the integrated web security capabilities that are configured via the Security Rule Base, and the ability to secure XML Web Services (SOAP) on Web Servers.

Appendices

• Chapter A, “Security Before VPN-1 Pro Activation” describes how the FireWall-1 enforcement point protects itself and the networks behind it before a security policy is installed.

• Chapter B, “FireWall-1 Command Line Interface” is a short summary of the available console commands.
Structure of the Book
Section 1: Network Access

This section describes how to secure the networks behind the FireWall-1 enforcement point by allowing only permitted users and resources to access protected networks.
CHAPTER 2

FireWall-1 Access Control

In This Chapter

The Need for Access Control  page 17
FireWall-1 Solution for Secure Access Control  page 17
Considerations for Access Control  page 25
Configuring Access Control  page 28

The Need for Access Control

As a network administrator you need the means to securely control access to resources such as networks, hosts, network services and protocols. Determining what resources can be accessed, and how, is the job of authorization, or Access Control. Determining “who” can access these resources is the job of user authentication, described in Chapter 3, “Authentication”.

FireWall-1 Solution for Secure Access Control

In This Section

Access Control at the Network Boundary  page 18
The Security Rule Base  page 19
Example Access Control Rule  page 19
Rule Base Elements  page 20
Access Control at the Network Boundary

A FireWall-1 Gateway (a “firewall”) at a network boundary acts as an enforcement point that inspects and provides access control for all traffic passing through the gateway (FIGURE 2-1). Traffic that does not pass through the enforcement point is not controlled.

FIGURE 2-1 A FireWall-1 enforcement point inspects all traffic that crosses it

The FireWall-1 administrator is responsible for implementing the company Security Policy. FireWall-1 allows the company Security Policy to be consistently enforced across multiple firewalls. To achieve this, an enterprise-wide Security Policy Rule Base is defined at the SmartCenter Server central SmartCenter console. The SmartDashboard SmartConsole Client is used to install the Policy, and distribute it to the FireWall-1 Gateways. Granular control of the Policy is possible by having specific rules apply only on specific enforcement points.

FireWall-1 provides secure access control through its granular understanding of all underlying services and applications traveling on the network. Stateful Inspection technology provides full application-layer awareness, and comprehensive access control for more than 150 pre-defined applications, services and protocols as well as the ability to specify and define custom services.
Stateful Inspection extracts state-related information required for security decisions from all application layers and maintains this information in dynamic state tables for evaluating subsequent connection attempts. For complete technical information about Stateful Inspection, see the Check Point Tech. Note at http://www.checkpoint.com/products/downloads/firewall-1_statefulinspection.pdf

The Security Rule Base

The Security Policy is implemented by defining an ordered set of rules in the Security Rule Base. A well-defined Security Policy is essential in order for FireWall-1 to be an effective security solution.

The fundamental concepts of the Security Rule Base is “That which is not explicitly permitted is prohibited”.

The Rule Base specifies what communication will be allowed to pass and what will be blocked. It specifies the source and destination of the communication, what services can be used, at what times, whether to log the connection and the logging level. Reviewing SmartView Tracker traffic logs is a very important aspect of security management, and should get careful attention.

FireWall-1 works by inspecting packets in a sequential manner. When FireWall-1 receives a packet belonging to a connection, it compares it against the first rule in the Security Rule Base, then the second, then the third, and so on. When it finds a rule that matches, it stops checking and applies that rule. If the packet goes through all the rules without finding a match, then that packet is denied. It is important to understand that the first rule that matches is applied to the packet, not the rule that best matches.

Example Access Control Rule

FIGURE 2-2 shows a typical Access Control rule. It says that HTTP connections that originate in one of Alaska_LAN group of hosts, to any destination, will be accepted, and logged.

<table>
<thead>
<tr>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>VPN</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRASH</th>
<th>INSTALL</th>
<th>TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alaska_LAN</td>
<td>Any</td>
<td>Any Traffic</td>
<td>HTTP</td>
<td>accept</td>
<td>Log</td>
<td>Policy Targets</td>
<td>Any</td>
</tr>
</tbody>
</table>
Rule Base Elements

A rule is made up of a number of Rule Base elements. Not all fields are always relevant in a given rule.

<table>
<thead>
<tr>
<th>TABLE 2-1</th>
<th>Rule Base elements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source and Destination</td>
<td>The source and destination is with respect to the originator of the connection. For applications that work in the client server model, the source is the client. Once the connection is accepted, packets in the connection are allowed in both directions. Source and destination can also be negated. You may for example find it convenient to specify that the source is NOT in a given network.</td>
</tr>
<tr>
<td>VPN</td>
<td>Configure whether the rule applies to any connection, either encrypted or clear, or only to VPN connections. To limit this rule to VPN connections, right-click and select Replace...</td>
</tr>
<tr>
<td>Service</td>
<td>The service column allows predefined applications to be specified. It is also possible to define new services.</td>
</tr>
<tr>
<td>Action</td>
<td>A packet can either be Accepted, Rejected, or Dropped. The other possible Actions relate to authentication (see Chapter 3, “Authentication” on page 109). If a connection is Rejected, the firewall sends a RST packet to the originating end of the connection and the connection is closed. If a packet is Dropped then no response is sent and the connection will eventually time out.</td>
</tr>
<tr>
<td>Track</td>
<td>Various logging options are available. See the SmartCenter guide.</td>
</tr>
<tr>
<td>Install-On</td>
<td>Specifies the FireWall-1 Gateways on which the rule is to be installed. There may be no need to enforce a particular rule at every FireWall-1 Gateway. For example, a rule may allow certain network services to cross one particular gateway. If these services are not to be allowed to networks behind other FireWall-1 Gateways, the rule need not be installed on other gateways. For further information, see the SmartCenter guide.</td>
</tr>
<tr>
<td>Time</td>
<td>Specify the days and time of day at which this rule should be enforced.</td>
</tr>
</tbody>
</table>

Implied Rules

The Security Policy is made up of rules. Apart from the rules defined by the administrator, FireWall-1 also creates Implied Rules, which are derived from the Policy Global Properties. Implied rules are defined by FireWall-1 to allow certain connections to and from the firewall with a variety of different services. Examples of two important implied rules are ones that enable

- FireWall-1 Control Connections
- Outgoing Packets originating from the FireWall-1 Gateway
There are also implied rules for other possible connection scenarios.

FireWall-1 creates a group of implied rules from the Policy Global Properties, that it places first, last, or before last in the Security Rule Base defined by the administrator. Implied rules can be logged. The rules are therefore processed in the following order:

1. Implied Rules defined as first. If an implied rule is first, the implied rule cannot be modified or overwritten in the Security Rule Base, because the first rule that matches is always applied to packet, and no rules can be placed before it.

2. Explicit, administrator-defined rules 1 through n-1 in the Rule Base (assuming n rules).

3. Implied Rules listed as Before Last. Setting a property to Before Last makes it possible to define more detailed rules that will be enforced before this property.

4. Last explicitly defined rule (Rule n).

5. Implied Rules listed as Last. If a property is Last, it is enforced after the last rule in the Security Rule Base, which usually rejects all packets, and it will typically have no effect.

6. Implicit Drop Rule (no logging occurs).

**Preventing IP Spoofing**

Spoofing is a technique where an intruder attempts to gain unauthorized access by altering a packet's IP address to make it appear as though the packet originated in a part of the network with higher access privileges. It is important to make sure that the communication does in fact originate from the apparent source.

Anti-spoofing verifies that packets are coming from, and going to, the correct interfaces on the gateway. It confirms that packets claiming to be from an internal network are actually coming from the internal network interface. It also verifies that, once a packet is routed, it is going through the proper interface.

A packet coming from an external interface, even if it has a spoofed internal IP address, will be blocked because the FireWall-1 anti-spoofing feature detects that the packet arrived from the wrong interface.

**FIGURE 2-3** illustrates what anti-spoofing does.

On Alaska_GW, FireWall-1 checks that

- All incoming packets to interface IF1 come from the Internet.
- All incoming packets to interface IF2 come from Alaska_LAN or Alaska_RND_LAN or Florida_LAN.
On Alaska_RND_GW, FireWall-1 checks that:

- All incoming packets to interface IF3 come from Alaska_LAN or Florida_LAN or the Internet.
- All incoming packets to interface IF4 come from Alaska_RND_LAN.

When configuring anti-spoofing, you also need to specify (in the interface topology definitions) whether the interfaces lead to the Internet, in which case they must be defined as External, or whether they lead to an internal network, in which case they are defined as Internal. FIGURE 2-3 illustrates whether the gateway interfaces are Internal or External.

**FIGURE 2-3 Illustrating Anti-Spoofing**

What are the Legal Addresses

Legal addresses are those that are allowed to enter a FireWall-1 interface. Legal addresses are determined by the topology of the network. When configuring Anti-Spoofing protection, the administrator must tell FireWall-1 what are the legal IP addresses behind the interface. This can be done automatically using the Get Interfaces with Topology option which automatically defines the interface with its topology, and creates network objects. FireWall-1 obtains this information by reading routing table entries.

More information about Anti-spoofing Protection

- For planning considerations, see “Spoof Protection” on page 26.
- For configuration details, see “Configuring Anti-spoofing” on page 30.
New Services

In This Section

**DCE-RPC**  page 23
**SSLv3 Service**  page 23
**SSHv2 Service**  page 23
**FTP_BASIC Protocol Type**  page 24
**Domain_UDP Service**  page 24
**Blocking Visitor Mode**  page 24

**DCE-RPC**

DCE-RPC (Distributed Computing Environment- remote procedure call) is a technology used for calling a procedure on a remote machine.

Unlike other services that are associated with a specific TCP or UDP port, DCE-RPC uses dynamically assigned port numbers assigned by the Endpoint Mapper.

DCE-RPC uses the Endpoint Mapper mechanism, for the purpose of dynamically assigning a port number to specific applications. A client that wishes to connect to a DCE-RPC application typically connects to TCP135 (default RPC Endpoint Mapper port) and provides the Endpoint Mapper with a UUID number interface. In return, the Endpoint Mapper provides the client a port to which the client can connect.

SmartView Tracker logs UUID interfaces, which makes it possible to identify non-common UUID interfaces. UUID interfaces can be used to enforce security rules.

**SSLv3 Service**

It is possible to verify that SSL client connections are using version 3 or higher of the SSL protocol in order to prevent security problems known with earlier versions of SSL. SSLv3 enforcement is enabled using the `ssl_v3` service.

If the `ssl_v3` service is used in a rule, and an SSLv2 connection is attempted, the connection is rejected.

Many internet browsers use SSLv2. To allow their connections to pass through FireWall-1, use the HTTPS service in the Rule Base.

**SSHv2 Service**

It is possible to verify that SSH connections are using version 2 or higher of the protocol in order to prevent security problems known with earlier versions of SSH. SSHv2 enforcement is enabled using the `ssh_version_2` service.
If the SSHv2 service is used in a rule, SSHv1 connections are dropped.

**FTP_BASIC Protocol Type**

FTP_BASIC is a new protocol type. This protocol type enforces a reduced set of the FTP security checks done by the regular FTP protocol type. Using FTP_BASIC eliminates known connectivity problems with FTP implementations that are not fully RFC compliant. The following checks are NOT enforced by FTP_BASIC, and are enforced by the FTP protocol type:

- That every packet is terminated with a newline character, so that the PORT command is not split across packets. This protects against the FTP Bounce attack.
- Data connections to or from well-known ports are not allowed, to prevent the FTP data connection being used to access some other service.
- Bidirectional traffic on the data connection is not allowed, as it can be used improperly.

**Domain_UDP Service**

The Domain_UDP service provides access control for DNS.

- DNS performance when using this service has been improved. Many DNS connections are for queries which comprise one request and one reply packet. FireWall-1 normally maintains virtual DNS connections for the period of the UDP timeout. DNS verification speed can be improved by telling FireWall-1 to delete the connection as soon as it receives the reply packet. To do this, change the property delete_on_reply (false) to true using the Database Tool.
- DNS logs are more informative. For example, the domain of the device making a DNS query is now shown in the Information column.
- DNS verification of EDNS queries is supported. This allows use of BIND. EDNS headers are allowed if they contain all zeros, other than the field that controls the packet length (maximum payload size).

**Blocking Visitor Mode**

**Introduction to TCPT**

Visitor Mode and the TCP tunneling protocol (TCPT) were developed by Check Point to allow SecureClient connections from behind any gateway device with a restrictive outgoing Security Policy. An example of such as Security Policy is one that allows only HTTP and HTTPS (SSL) outgoing traffic, and prevents the various protocols (such as IKE) required for the secure connections.
Why Block Visitor Mode and Outgoing TCPT?

The VPN-1 Pro administrator can decide to block Visitor Mode by implementing a very restrictive outgoing Security Policy that allows ordinary HTTPS connections and disallows TCPT connections passing on the same port.

Visitor Mode and Incoming TCPT are allowed via the Gateway object. See the Advanced Configuration chapter of the VPN-1 Pro guide for details.

How VPN-1 Pro identifies TCPT

VPN-1 Pro performs content inspection in order to identify TCPT packets and reject them if necessary. It does not merely check the port.

The default port used by TCPT is 443, which is the same port used by SSL. This can be changed. (See “How to change the port used to block outgoing TCPT” on page 31.)

When to Block Outgoing TCPT

Only block TCPT if there is a rule that allows the port used by TCPT, for example, port 443. If there is no rule that allows the port used by TCPT, then it will be implicitly blocked, and there is no need explicitly block it.

There are a number of services that perform content inspection, rather than merely checking port numbers. If you block outgoing TCPT, and there is a rule that allows a service that uses the same port as TCPT, and that service performs content inspection, then both TCPT and that service will be blocked. The exception is the SSLv3 service. A rule that allows SSLv3, permits only SSL version 3 connections, and rejects TCPT.

Services that do content inspection are those that have a defined Protocol Type in the TCP Service Properties>Advanced window.

For configuration instructions, see “How to Block Visitor Mode (Blocking Outgoing TCPT)” on page 31.

Considerations for Access Control

In This Section

Spoof Protection page 26
Simplicity page 26
Basic Rules page 26
Rule Order page 27
Considerations for Access Control

**Spoof Protection**
If you don’t protect your network against address spoofing, all your carefully crafted access control rules will be ineffective. It is easy enough for a malicious user to attempt to gain access by changing the source address of the packet. Make sure you configure anti-spoofing protection on every interface of the FireWall-1 Gateway, including internal interfaces. For configuration details, see “Configuring Anti-spoofing” on page 30.

**Simplicity**
The key to a secure firewall is a simple Rule Base. The biggest danger to the security of your organization can be simple misconfiguration. Why should a malicious user try to sneak spoofed, fragmented packets past your firewall when you have inadvertently allowed unrestricted messaging protocols? To keep your Rule Base simple, keep it short. The more rules you have, the more likely you will make a mistake. The fewer rules your Rule Base has, the easier it is to understand and maintain.

**Basic Rules**
Be careful to allow only the traffic that you want. Consider both traffic crossing the firewall that is initiated on the unprotected side of the firewall, and traffic initiated on the protected side of the firewall.

The following basic Access Control rules are recommended in every Security Rule Base:

- A Stealth Rule to prevent any direct access to the FireWall-1 Gateway.
- A Cleanup Rule to drop all traffic that is not permitted by the previous rules.

There is an implied rule that does this, but the Cleanup Rule allows you to log any access attempts.

Remember the fundamental concept of a Rule Base: “That which is not explicitly permitted is prohibited”.

---

Topologies Considerations: DMZ  
The X11 Service  
When to Edit Implied Rules
Rule Order

Rule order is critical. Having the same rules, but placing them in a different order, can radically alter how your firewall works. It is therefore best to place the more specific rules first, the more general rules last. This prevents a general rule being matched before a more specific rule, and protects your firewall from misconfigurations.

Topology Considerations: DMZ

If you have servers that are externally accessible from the internet, you should create a demilitarized zone (DMZ). Servers in the DMZ are accessible from any network, and all externally accessible servers should be in the DMZ. The purpose of the DMZ is to isolate all servers that are accessible from untrusted sources, like the Internet, so that if someone compromises one of those servers, the intruder will have only limited access to externally accessible servers. Servers in the DMZ should be as secure as possible. Do not allow the DMZ to initiate connections into the internal network, other than for specific applications such as UserAuthority.

The X11 Service

The X11 (X Window System Version 11) graphics display system is the de-facto graphics system in the Unix world. To allow X11, you must create a specific rule using the X11 service. When selecting Any as the Source or Destination, the X11 service is not included. This is because of the unusual nature of X11, by which the GUI application actually acts as the server, rather than the client.

When to Edit Implied Rules

Implied rules are controlled from the Global Properties window FireWall-1 Implied Rules page. In general, there is no need to change them. Some are best left unselected so that the property can be controlled with greater granularity via the Rule Base. For example, you may wish to allow ICMP pings across certain gateways only. The following are the recommended settings:

<table>
<thead>
<tr>
<th>Implied Rule</th>
<th>Recommended Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept VPN-1 &amp; FireWall-1 Control Connections</td>
<td>First</td>
</tr>
<tr>
<td>Accept outgoing packets originating from gateway</td>
<td>Unselected</td>
</tr>
<tr>
<td>Accept RIP</td>
<td>Unselected</td>
</tr>
<tr>
<td>Accept Domain Name Over UDP (Queries)</td>
<td>Unselected</td>
</tr>
<tr>
<td>Accept Domain Name over TCP (Zone transfer)</td>
<td>Unselected</td>
</tr>
</tbody>
</table>

TABLE 2-2 FireWall-1 Implied Rules recommended settings
Configuring Access Control

In This Section

- Defining access Control Rules  page 28
- Defining a Basic Policy  page 28
- Configuring Anti-spoofing  page 30
- Configuration of Visitor Mode Blocking  page 31

Defining access Control Rules

An example Access control Rule is shown in FIGURE 2-2 on page 19. To define a rule:

1. Define the network objects for each network and host (for details, see SmartCenter guide).
2. From the menu, select Rules > Add Rule and choose one of Bottom, Top, Below, Above.
3. In the Source and Destination columns, right click and select Add..., choose a network object and click OK.
4. In the Service column, right click, select Add..., choose a service or a service group, and click OK.
5. In the Action column, right click and select Accept, Drop, or Reject.
6. In the Track column, right click, select Add... and choose one of the tracking options.

Defining a Basic Policy

FIGURE 2-4 shows a network requiring an Access Control policy.

<table>
<thead>
<tr>
<th>TABLE 2-2 FireWall-1 Implied Rules recommended settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept ICMP requests</td>
</tr>
<tr>
<td>Accept CPRID connections (SmartUpdate)</td>
</tr>
<tr>
<td>Accept dynamic address Modules' DHCP traffic</td>
</tr>
</tbody>
</table>

Configuring Access Control
The Access Control Policy is required to:

1. Allow internal users access to the World Wide Web.
2. Allow all users access to the servers on the DMZ network.
3. Protect the network from outsiders.

The Policy also requires two basic rules: a Stealth Rule and a Cleanup Rule.

To create the Policy, add rules in the SmartDashboard using the **Rules > Add Rules...** menu items, as detailed in “Defining a Basic Policy” on page 28. FIGURE 2-5 shows the resulting Access Control Security Rule Base.

**FIGURE 2-5** Typical Access Control Security Rule Base

<table>
<thead>
<tr>
<th>NO</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>VPN</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
<th>INSTALL ON</th>
<th>TIME</th>
<th>COMMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>Alaska_GW</td>
<td>Any</td>
<td>Any</td>
<td>drop</td>
<td>Log</td>
<td>Any</td>
<td>Any</td>
<td>Stealth Rule</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Alaska_DMZ_LAN</td>
<td>Any</td>
<td>FTP</td>
<td>accept</td>
<td>Log</td>
<td>Policy Target</td>
<td>Any</td>
<td>DMZ Access Rule</td>
</tr>
<tr>
<td>3</td>
<td>Alaska_LAN</td>
<td>Any</td>
<td>Any</td>
<td>FTP</td>
<td>accept</td>
<td>Log</td>
<td>Policy Target</td>
<td>Any</td>
<td>Web Traffic Rule</td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>drop</td>
<td>Log</td>
<td>Policy Target</td>
<td>Any</td>
<td>Cleanup Rule</td>
</tr>
</tbody>
</table>
Configuring Anti-spoofing

Make sure you configure anti-spoofing protection on every interface of every FireWall-1 Gateway, including internal interfaces. This basic configuration example shows how to set up anti-spoofing parameters on an external interface and the internal interface.

Define a Valid Address for the External Interface

1. In SmartDashboard, select Manage > Network Objects.
2. Select the Check Point Gateway and right click Edit.
3. In the Properties list, click Topology.
4. Click Get > Interfaces to read the interface information on the gateway machine.
5. Select the interface that faces the Internet and click Edit.
6. In the Interface Properties window, click Topology, and select External (leads out to the internet).
7. Check Perform Anti-Spoofing based on interface topology, under Spoof Tracking select Log, and click OK.

Define a Valid Address for Internal Interfaces

8. Under the name column, select the internal interface, click Edit.
9. In the Interface Properties window, click Topology, and click Internal (leads to the local network).
10. Under IP Addresses behind this interface:
    • If there is only one network behind the interface, choose Network defined by the interface IP and Net Mask.
    • If there is more than one network behind the interface, define a Group Network object that comprises all the networks behind the interface, choose Specific and select the group.
11. Check Perform Anti-Spoofing based on interface topology, under Spoof Tracking select Log, and click OK.
12. Repeat step 8 to step 11 for all internal interfaces.
13. Install the Security Policy.
Configuration of Visitor Mode Blocking

For background information about TCPT blocking, see “Blocking Visitor Mode” on page 24.

How to Block Visitor Mode (Blocking Outgoing TCPT)

To block outgoing TCPT, use the Database Tool on the SmartCenter Server, and locate, and change the following property for every FireWall-1 enforcement module for which you wish to block outgoing TCPT:

```
disable_outgoing_tcpt (false)
```

Change the value of the property to `true`.

How to change the port used to block outgoing TCPT

To change the port used to block TCPT, use the Database Tool and locate the following global property on the SmartCenter Server:

```
tcpt_outgoing_port (443)
```

Change the value of the property to the required port number.
Configuring Access Control
Authentication

In This Chapter

- The Need for Authentication  page 33
- VPN-1 Pro Solution for Authentication  page 33
- Configuring Authentication  page 48

The Need for Authentication

People in different departments and with different levels of responsibility must be given
different access permissions to different parts of the network. It is therefore necessary to
allow access only to valid users. Determining who is a valid user is the job of
Authentication.

VPN-1 Pro Solution for Authentication

In This Section

- Introduction to VPN-1 Pro Authentication  page 34
- Authentication Schemes  page 34
- Authentication Methods  page 36
- Choosing an Authentication Method  page 47
Introduction to VPN-1 Pro Authentication

VPN-1 Pro authenticates individual users via the use of credentials. VPN-1 Pro can manage credentials using a number of different Authentication Schemes. All Authentication Schemes in VPN-1 Pro rely on some sort of username and password. Some of these schemes involve storing the passwords on the VPN-1 Pro enforcement module. In other schemes, passwords are stored on external servers.

There are three ways in which users can authenticate themselves to VPN-1 Pro. The available Authentication Methods are: User Authentication, Session Authentication, and Client Authentication.

Authentication ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Authentication Schemes

Authentication Schemes employ usernames and passwords to identify users. Some of these schemes are maintained locally, storing the usernames and passwords on the VPN-1 Pro enforcement module. Others store the user database externally, and authentication requests are directed to an external authentication server. Some schemes, such as SecurID, are based on a one-time password. All the schemes can be used with users defined on an LDAP server. For information on configuring VPN-1 Pro to integrate LDAP, see SmartDirectory (LDAP) and User Management in the SmartCenter book.

VPN-1 Pro Password

VPN-1 Pro can store a static password in its local user database for each user configured in SmartCenter Server. No additional software is needed.

OS Password

VPN-1 Pro can use the user and password information that is stored in the operating system of the machine on which VPN-1 Pro is installed. It is also possible to use passwords that are stored in a Windows domain. No additional software is needed.

RADIUS

Originally developed by Livingston Enterprises (now part of Lucent Technologies) in 1992, Remote Authentication Dial-In User Service (RADIUS) is an external authentication scheme that provides security and scalability by separating the authentication function from the access server. RADIUS was submitted to the Internet Engineering Task Force (IETF) as a proposed standard protocol in 1996. RFC 2865 is the latest update to the proposed standard, and can be found at URL: www.ietf.org/rfc/rfc2865.txt.
When employing RADIUS as an authentication scheme, VPN-1 Pro forwards authentication requests by remote users to the RADIUS server. The RADIUS server, which stores user account information, authenticates the users.

The RADIUS protocol uses UDP for communications with the gateway. RADIUS Servers and RADIUS Server Group objects are defined in SmartDashboard. For more on configuring RADIUS, see “Configuring a VPN-1 Pro Gateway to use RADIUS” on page 56.

SecurID
Developed by RSA Security, SecurID requires users to both possess a token authenticator and to supply a PIN or password. Token authenticators generate one-time passwords that are synchronized to an RSA ACE/Server, and may come in the form of hardware or software. Hardware tokens are key-ring or credit card-sized devices, while software tokens reside on the PC or device from which the user wants to authenticate. All tokens generate a random, one-time-use access code that changes every minute or so. When a user attempts to authenticate to a protected resource, that one-time-use code must be validated by the ACE/Server.

When employing SecurID as an authentication scheme, VPN-1 Pro forwards authentication requests by remote users to the ACE/Server. ACE manages the database of RSA users and their assigned hard or soft tokens. The VPN-1 Pro enforcement module acts as an ACE/Agent 5.0, which means that it directs all access requests to the RSA ACE/Server for authentication. For agent configuration see ACE/Server documentation.

There are no scheme-specific parameters for the SecurID authentication scheme. For more on configuring SecurID, see “Configuring a VPN-1 Pro Gateway to use SecureID” on page 57.

TACACS
Terminal Access Controller Access Control System (TACACS) provides access control for routers, network access servers and other networked devices via one or more centralized servers. TACACS was originally developed by the U.S. Department of Defense and BBN Planet Corp. and then further developed by Cisco. A newer version of the protocol called TACACS+ provides enhancements to the original protocol, including the use of TCP instead of UDP.

TACACS is an external authentication scheme that provides verification services. When employing TACACS as an authentication scheme, VPN-1 Pro forwards authentication requests by remote users to the TACACS server. The TACACS server, which stores user account information, authenticates users. The system supports physical card key...
devices or token cards, and supports Kerberos secret-key authentication. TACACS encrpts the username, password, authentication services and accounting information of all authentication requests for more secure communications.

For information on configuring TACACS see “Configuring a VPN-1 Pro Gateway to use TACACS+” on page 58.

**Undefined**

The authentication scheme for a user can be specified as undefined. If a user with an undefined authentication scheme is matched to a Security Rule with some form of authentication, he or she is always denied access.

**Authentication Methods**

In This Section

- *Introduction to Authentication Methods* page 36
- *User Authentication* page 37
- *Session Authentication* page 39
- *Client Authentication* page 40

**Introduction to Authentication Methods**

Instead of creating a security rule that simply allows or denies connections, the firewall administrator can compel clients to authenticate when they try to access specific network resources. There are three such Authentication Methods:

- User Authentication.
- Session Authentication.
- Client Authentication.

These three Authentication Methods differ in services provided, logon mechanism, and user experience. All can be configured to connect and authenticate clients initially to the VPN-1 Pro Gateway before passing the connection to the desired resource, a process known as non-transparent authentication. Alternatively, they can be configured to connect clients directly to the target server, a process known as transparent authentication.

This section describes how the user authenticates using each of these methods, and how they work. For details on setting up the different authentication methods, see “Configuring Authentication” on page 48.
User Authentication

User Authentication provides authentication for five services: Telnet, FTP, HTTP, HTTPS, and rlogin. By default, User Authentication is transparent. The user does not explicitly connect to the VPN-1 Pro Gateway, but initiates a connection directly to the target server.

The following example demonstrates a Telnet session to 10.11.12.13, with User Authentication and the OS Password authentication scheme (Rlogin works in almost exactly the same way):

```
# telnet 10.11.12.13
Trying 10.11.12.13...
Connected to 10.11.12.13.
Escape character is '^)'.
Check Point FireWall-1 authenticated Telnet server running on tower
User: fbloggs
FireWall-1 password: *******
User fbloggs authenticated by FireWall-1 authentication
Connected to 10.11.12.13
...
login:
```

User Authentication works as follows:

1. VPN-1 Pro intercepts the communication between the client and server.
2. VPN-1 Pro prompts for a username and password.
3. If the user successfully authenticates, VPN-1 Pro passes the connection on to the remote host. If the correct authentication information is not supplied by the user within the allowed number of connection attempts, the connection is dropped.
4. The remote host prompts for its own username and password.

**Note** - When configuring user objects, you can set the locations that they are allowed to access. This can lead to conflicts with security rules that require a form of authentication. See "Resolving Access Conflicts" on page 46 for more information.

The following example demonstrates an FTP session to 10.11.12.13, with User Authentication and the OS Password authentication scheme.

```
# ftp 10.11.12.13
Connected to 10.11.12.13.
220 london Check Point FireWall-1 Secure FTP server running on tower
Name (10.11.12.13:fbloggs):
```
Now the username must be entered in the following format:

```
FireWall-1 User@Destination Host
```

This format is demonstrated as follows:

```
fbloggs@10.11.12.13
331-aftpd: FireWall-1 password: you can use FW-1-password
```

Now enter the FireWall-1 password:

```
Password: xyz987
230-aftpd: User fbloggs authenticated by FireWall-1 authentication.
230-aftpd: Connected to 10.11.12.13. Logging in...
230-aftpd: 220 bigben ftp server (UNIX(r) System V Release 4.0) ready.
ftp>
```

At this point you will be connected to the remote FTP server. Log in using the user command:

```
ftp> user anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password: fbloggs@checkpoint.com
230 Anonymous user logged in.
ftp>
```

**Timeout Considerations for User Authentication of HTTP**

In HTTP, the Web browser automatically supplies the password to the server for each connection. This creates special security considerations when using User Authentication for HTTP 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 **User Authentication session timeout** in the **Authentication** page of the **Check Point Gateway** window. Users of one-time passwords do not have to reauthenticate for each request during this time period.

To enhance security, you may want to compel users to reauthenticate for certain types of requests. 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. To set reauthentication parameters, adjust the **Reauthentication** options in the **HTTP Server** definition of the **Global Properties > FireWall-1 > Security Server** page.
For information on configuring User Authentication, see “Configuring User Authentication” on page 49.

**Session Authentication**

Session Authentication can be used for any service, but to retrieve a user’s identity it requires a Session Authentication agent. The Session Authentication agent is normally installed on the authenticating client, in which case the person who initiates the connection to the destination host supplies the authentication credentials. Like User Authentication, it requires an authentication procedure for each connection. However, the Session Authentication agent can also be installed on the destination machine, or on some other machine in the network. In that case, the person at the machine on which the Agent is installed is asked to supply the username and password.

**FIGURE 3-1** shows the Session Authentication login prompt. After typing his or her username, another prompt asks the user to supply a password.

**FIGURE 3-1** Session Authentication login prompt

The Session Authentication agent works as follows:

1. The user initiates a connection directly to the server.
2. VPN-1 Pro intercepts the connection.
3. The Session Authentication agent challenges the user for authentication data and returns this information to VPN-1 Pro.
4. If the authentication is successful, VPN-1 Pro allows the connection to pass through the gateway and continue on to the target server.
For information on configuring Session Authentication and the Session Authentication agent, see “Configuring Session Authentication” on page 50.

**Note** - When configuring user objects, you can set the locations that they are allowed to access. This can lead to conflicts with security rules that require a form of authentication. See “Resolving Access Conflicts” on page 46 for more information.

### Client Authentication

Client Authentication can be used to authenticate any service. It allows access from a specific IP address for an unlimited number of connections. The user working on a client performs the authentication by successfully meeting an authentication challenge, but it is the client machine that is granted access. Client Authentication is less secure than User Authentication, as it allows multiple users and connections from authorized IP addresses or hosts. The authorization is per machine for services that do not have an initial login procedure. The advantage of Client Authentication is that it can be used for any number of connections, for any service, and authentication is valid for any length of time.

**Note** - When configuring user objects, you can set the locations that they are allowed to access. This can lead to conflicts with security rules that require a form of authentication. See “Resolving Access Conflicts” on page 46 for more information.

Client Authentication can be used with any one of five different sign on methods. These sign on methods provide a choice of Authentication Methods for authenticated and other services, as summarized in TABLE 3-1. For all sign on methods other than Manual Client Authentication, the VPN-1 Pro Gateway is transparent to the user. This means that the user authenticates directly to the destination host.

<table>
<thead>
<tr>
<th><strong>TABLE 3-1  Client Authentication Sign On Methods</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Authentication Sign On Method</strong></td>
</tr>
<tr>
<td>Manual</td>
</tr>
<tr>
<td>Partially automatic</td>
</tr>
<tr>
<td>Fully automatic</td>
</tr>
<tr>
<td>Agent automatic</td>
</tr>
<tr>
<td>Single Sign On</td>
</tr>
</tbody>
</table>

There are two Client Authentication Sign On options:
Authentication Methods

- Standard Sign On
- Specific Sign On

Standard Sign On allows the user to use all the services permitted by the rule, without having to perform authentication for each service.

Specific Sign On allows the user to access only the services they specify when they authenticate, even if the rule allows more than one service. If the user wishes to use another service, he or she needs to reauthenticate for that specific service.

At the end of the session, the user can sign off. When a user signs off, he or she is signed off from all services, and the connection is closed by the remote host.

An explanation follows of each of the Client Authentication sign on methods summarized in TABLE 3-1:

**Manual Sign On**

Manual Sign On is available for any service, as long as it is specified in the Client Authentication rule.

In Manual Sign On, the user must first connect to the Gateway in order to authenticate (in other words, the authentication is not transparent). The user must authenticate in one of two ways:

1. A Telnet session to the Gateway on port 259

2. An HTTP connection to the gateway on port 900, through a Web browser. The requested URL must include the gateway name and the port number, such as http://Gateway:900.
The following example shows what Client Authentication with Standard, Manual Sign On looks like to a user. Before opening a connection to the destination host, user *fbloggs* first authenticates to *london*, the VPN-1 Pro Gateway:

```
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:  *fbloggs*  
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.
```
The following example shows what Client Authenticating with Specific, Manual Sign On looks like to a user. In the example, two services are specified: `rstat` and `finger`, each one to a different host.

```
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.
```

**Wait Mode for Client Authentication**

Wait Mode is a Client Authentication capability for the VPN-1 Pro Gateway that applies to Manual Sign On when the user initiates a Client Authenticated connection with a Telnet session to port 259 on the Gateway.

Wait Mode makes it unnecessary to open a new Telnet session in order to Sign Off and withdraw Client Authentication privileges. In Wait mode, the initial Telnet session remains open, and Client Authentication privileges remain valid so long as the connection is open. The privileges are withdrawn when the Telnet session is closed.

VPN-1 Pro keeps the Telnet session open by pinging the authenticating client. If for some reason the client machine stops running, VPN-1 Pro closes the Telnet session and Client Authentication privileges from this IP address are withdrawn.

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.
**Partially Automatic Sign On**

Partially Automatic Sign On is available for the authenticated services Telnet, FTP, HTTP, HTTPS, and RLOGIN services, as long as they are specified in the Client Authentication rule. No other services can be authenticated with Partially Automatic Client authentication.

If the user attempts a connection to a remote host using one of the authenticated services, he or she is asked to authenticate by means of User Authentication.

**Fully Automatic Sign On**

Fully Automatic Sign On is available for any service, as long as the required service is specified in the Client Authentication rule.

If the user attempts a connection to a remote host using an authenticated service (Telnet, FTP, HTTP, HTTPS, and RLOGIN), he or she is asked to authenticate by means of User Authentication.

If the user attempts a connection to a remote host using any other service, he or she is asked to authenticate by means of the Session Authentication agent, which must be properly installed.

**Agent Automatic Sign On**

Agent Automatic Sign On is available for any service, as long as the required service is specified in the Client Authentication rule, and as long as the Session Authentication agent is properly installed.

If the user attempts a connection to a remote host using any service, he or she is asked to authenticate by means of the Session Authentication agent.

**Single Sign On**

Single Sign On is available for any service, as long as the required service is specified in the Client Authentication rule. UserAuthority must be installed.

Single Sign On is the Check Point address management feature that provides transparent network access. In this method, VPN-1 Pro consults the user IP address records to determine which user is logged on at a given IP address. When a connection matches a Single Sign On enabled rule, VPN-1 Pro queries UserAuthority with the packet's source IP. UserAuthority returns the name of the user who is registered to the IP. If the user's name is authenticated, the packet is accepted; if not, it is dropped.
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 Pro 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 Pro knows which user is at the client, and additional authentication is not necessary.

To authorize all relevant Standard Sign On Rules after successful Partially or Fully Automatic authentication, use the GUIdbedit Database Tool to change a setting in VPN-1 Pro’s database. You can find the GUIdbedit Database Tool in the same directory on your local drive where SmartConsole is installed.

1. Launch GUIdbedit.
2. Search for the field name `automatically_open_ca_rules`.
3. Set the value 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 Client Authentication, proceed as follows:

1. Stop VPN-1 Pro (`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 Pro services provided as part of the Client Authentication feature.

3. Use a simple text editor to edit the file `$FWDIR/conf/fwauthd.conf`, an example of which is depicted in FIGURE 3-2. 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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Command</th>
<th>Wait</th>
<th>Restart</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>fwssd</td>
<td>in.aftpd</td>
<td>wait</td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>fwssd</td>
<td>in.ahttpd</td>
<td>wait</td>
<td></td>
</tr>
<tr>
<td>513</td>
<td>fwssd</td>
<td>in.arlogind</td>
<td>wait</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>fwssd</td>
<td>in.asmtpd</td>
<td>wait</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>fwssd</td>
<td>in.atelnetd</td>
<td>wait</td>
<td></td>
</tr>
<tr>
<td>259</td>
<td>fwssd</td>
<td>in.aclientd</td>
<td>wait</td>
<td>259</td>
</tr>
<tr>
<td>10081</td>
<td>fwssd</td>
<td>in.lhttpd</td>
<td>wait</td>
<td></td>
</tr>
<tr>
<td>900</td>
<td>fwssd</td>
<td>in.ahclientd</td>
<td>wait</td>
<td>900</td>
</tr>
<tr>
<td>0</td>
<td>fwssd</td>
<td>in.pingd</td>
<td>respawn</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>fwssd</td>
<td>in.asessiond</td>
<td>respawn</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>fwssd</td>
<td>in.aupfd</td>
<td>respawn</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>vpn</td>
<td>vpnd</td>
<td>respawn</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>fwssd</td>
<td>mdq</td>
<td>respawn</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>xrm</td>
<td>xrmd</td>
<td>respawn</td>
<td>0 -pr</td>
</tr>
</tbody>
</table>

FIGURE 3-2 $FWDIR/conf/fwauthd.conf file

Warning - Do not change anything else in the line.

4 Make sure that there is no rule that blocks the connection to the new port.

5 Restart VPN-1 Pro (`cpstart`).

Not all of the parameters shown in the sample file of FIGURE 3-2 will necessarily be present in your file.

For information on configuring Client Authentication, see “Configuring Client Authentication” on page 54.

Resolving Access Conflicts

When configuring users, you can set locations to which they are allowed to access. In doing so, however, you are disallowing all locations not specified. This can lead to a conflict with any security rule requiring authentication. For example, if a rule grants authenticated access to users from Mktg_net to Finance_net, yet the Location tab of user Susan allows connections only within Mktg_net, VPN-1 Pro does not know whether to allow the authentication request when Susan tries to connect to Finance_net.

You can specify how to resolve this conflict by editing the Authentication Action Property of the rule in question. Right click on the Action field of a rule using some form of authentication and select Edit Properties.
• If you want to apply the more restrictive access privileges specified in the rule and in the Location tab of each user’s User Properties window, choose Intersect with User Database.
• If you want to allow access according to the location specified in the rule, choose Ignore User Database.

You can set this property for both the Source and Destination of the rule.

Choosing an Authentication Method

With User Authentication, the administrator can allow the user who is away from his or her desk, to work on the local network without extending access to all users on the same host. However, User Authentication is available only for the services Telnet, FTP, HTTP, HTTPS, and RLOGIN.

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. 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 can be set to be valid for a specific length of time.

Session Authentication supplies an authentication mechanism for any service, and requires users to supply their credentials per session. A Session Authentication agent must be installed on every authenticating client. It is therefore not suitable for authenticating HTTP, which opens multiple connections per session. Like Client Authentication, use it only on single-user machines, where only one user can come from a given IP at any one time.
Configuring Authentication

In This Section

Creating Users and Groups .................................................. page 48
Configuring User Authentication .............................................. page 49
Configuring Session Authentication ........................................ page 50
Configuring Client Authentication ......................................... page 54
Configuring Authentication Tracking ..................................... page 55
Configuring a VPN-1 Pro Gateway to use RADIUS .................. page 56
Configuring a VPN-1 Pro Gateway to use SecureID ................. page 57
Configuring a VPN-1 Pro Gateway to use TACACS+ ............... page 58

Creating Users and Groups

Authentication Rules are defined in terms of user groups, rather than in terms of individual users. You must therefore define users and add them to groups. You can define users using the VPN-1 Pro proprietary user database, or using an LDAP server. For details on incorporating LDAP, see SmartDirectory (LDAP) and User Management in the SmartCenter book.

This simple example shows how to create a group, create VPN-1 Pro users from a template, add the users to the group, and install the user information in the database. For more details on creating users and groups, see SmartCenter Overview in the SmartCenter book.

Creating a User Group

1 Select the User Groups from the Users and Administrators tab of the Objects tree. Right Click, and select New Group... The Group Properties window opens. Give the group a Name. You will populate the group later, when creating the users.

Creating a User Template

2 Select the Users from the Users and Administrators tab of the Objects tree. In the Templates branch right click and select New Template.... The User Template Properties window is displayed.
3 Give the template a name. In the **Groups** tab, add this user template to all the groups to which users based on this template need to belong. In the **Authentication** tab, choose the appropriate authentication scheme for the user. In the remaining tabs, enter the other properties of the user template.

Once you have created a template, any user you create based on the template will inherit all of the template’s properties, including membership in groups. If you modify a template’s properties, the change will affect all users created from the template in the future. Users already created from the template will not be affected.

### Creating Users

4 In the **Users** branch of the objects tree, right click and choose the template on which the new user’s properties will be based. The **User Properties** window is displayed.

5 Enter the data for the user. For any user, you can freely change the properties that user inherited from the template, but they will be changed for the user only. The template remains unchanged.

### Install the User Information in the Database

6 Users and groups can be installed separately from the Rule Base. This means you can update users and groups without re-installing the Rule Base. To install the User Database, select **Policy > Install Database...** from the SmartDashboard menu.

### Configuring User Authentication

1 Configure the Users and Groups that are needed for authentication, and install the User Database (see “Creating Users and Groups” on page 48).

2 Define a User Authentication access rule.

   A In the **Source** column, right click to select **Add User Access...**, and choose the group.

   B If you would like to restrict the location of authenticating users: In the **Location** section of the same window, check **Restrict To** and choose the host, group of hosts, network or group of networks from which users can access.

   C In the **Service** field choose the services you would like to authenticate.
Configuring Authentication

In the Action column, choose User Auth.

TABLE 3-2 shows an HTTP User Authentication Rule.

<table>
<thead>
<tr>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>VPN</th>
<th>SERVICE</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alaska_Users@Any</td>
<td>Alaska_LAN</td>
<td>Any Traffic</td>
<td>HTTP</td>
<td>User Auth</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FTP</td>
<td></td>
</tr>
</tbody>
</table>

3 Double click the Action column to edit the User Authentication Action Properties.

4 If you wish, adjust the User Authentication session timeout in the Authentication page of the VPN-1 Pro Gateway object.

5 Install the Security Policy.

The Importance of Rule Order for User Authentication

When defining one or more User Authentication rule for the services Telnet, FTP, HTTP, HTTPS, and RLOGIN, and there are other non-authentication rules that use these services, make sure the User Authentication rule is placed last among these rules.

Configuring Session Authentication

1 If using the Session Authentication agent, install and configure it for all the machines desktops that are to allow Session Authentication (see “Installing and Configuring the Session Authentication Agent” on page 51).

2 Configure the Users and Groups that are needed for authentication, and install the User Database (see “Creating Users and Groups” on page 48).

3 Edit the Check Point Gateway object representing the VPN-1 Pro Gateway, and in the Authentication page, enable the required authentication schemes. The gateway must support all the authentication schemes defined for the users. For example, if some users use VPN-1 Pro Password, and others use RADIUS Authentication, check both these schemes.

4 Define a Session Authentication access rule.

A In the Source column, right click to select Add User Access..., and choose the group. Don’t close the window yet.

B If you would like to restrict the location of users: In the Location section of the same window, check Restrict To and choose the host, group of hosts, network or group of networks from which users can access.
In the **Service** field choose the services you would like to authenticate.

**D** In the **Action** column, choose **Session Auth.**

**TABLE 3-3** shows a typical Session Authentication Rule.

**TABLE 3-3** Session User Authentication Rule for HTTP and FTP

<table>
<thead>
<tr>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>VPN</th>
<th>SERVICE</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aaska_Users@Any</td>
<td>Alaska_LAN</td>
<td>Any</td>
<td>Traffic</td>
<td>HTTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>FTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Session Auth</td>
</tr>
</tbody>
</table>

5 Double click the **Action** column to edit the **User Authentication Action Properties**.

6 If you wish, adjust the **Failed Authentication Attempts** settings for Session Authentication in the **Authentication** page of the **Global Properties**.

7 Install the Security Policy.

**Installing and Configuring the Session Authentication Agent**

1 Install the Session Authentication agent from the CD-ROM. The Session Authentication agent is normally installed on the authenticating client, in which case the person who wants to the connection to the destination host supplies the authentication credentials. However, the Session Authentication agent can also be installed on the destination machine, or on some other machine in the network. In that case, the person at the machine on which the Agent is installed is asked to supply the username and a password.

2 Open the Session Authentication agent. On Windows machines, double-click its icon in the system tray. The *FireWall-1 Session Authentication* window (FIGURE 3-3) is displayed.

**FIGURE 3-3** FireWall-1 Session Authentication window
3. Click **Configure**. The **Configuration** window (FIGURE 3-4) is displayed. The **Configuration** window has three tabs, explained below.

**Passwords Tab**

**FIGURE 3-4**  Configuration window — 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 VPN-1 Pro 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 Pro Tab

FIGURE 3-5 Configuration window — Allowed FireWall-1 tab

The **Allowed FireWall-1** tab of the **Configuration** window enables you to specify the VPN-1 Pro Gateways for which this Session Authentication agent may provide authentication services.

**Any IP Address** — This Session Authentication agent may provide authentication services for any VPN-1 Pro Gateway.

**IP Address** — This Session Authentication agent may provide authentication services only for a VPN-1 Pro Gateway running on the specified IP address. You can specify up to three IP addresses.

Options Tab

FIGURE 3-6 Configuration window — Options tab

The **Options** tab of the **Configuration** window (FIGURE 3-6) enables you to specify whether to allow clear passwords and resolve addresses.
Configuring Authentication

Starting the Session Authentication Agent

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-1 Pro Gateway.

Configuring Client Authentication

1. Configure the Users and Groups that are needed for authentication, and install the User Database (see “Creating Users and Groups” on page 48).

2. Edit the Check Point Gateway object representing the VPN-1 Pro Gateway, and in the Authentication page, enable the required authentication schemes. The gateway must support all the authentication schemes defined for the users. For example, if some users use VPN-1 Pro Password, and others use RADIUS Authentication, check both these schemes.

3. Define a Client Authentication access rule.

   A In the Source column, right click to select Add User Access..., and choose the group.

   B If you would like to restrict the location of authenticating users: In the Location section of the same window, check Restrict To and choose the host, group of hosts, network or group of networks from which users can access.

   C In the Service field choose the services you would like to authenticate.

   D In the Action column, choose Client Auth.

   TABLE 3-4 shows a typical Client Authentication Rule.

<table>
<thead>
<tr>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>VPN</th>
<th>SERVICE</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aaska_Users@Any</td>
<td>Alaska_LAN</td>
<td>Any Traffic</td>
<td>HTTP</td>
<td>Client Auth</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FTP</td>
<td></td>
</tr>
</tbody>
</table>

4. Double click the Action column to edit the Client Authentication Action Properties. The settings for Requires Sign On and for Sign On Method are described in “Client Authentication” on page 40.
5 Make sure all Client Authentication Rules are placed above the Rule that prevents direct connections to the VPN-1 Pro Gateway (the “Stealth Rule”), so that they have access to the VPN-1 Pro Gateway.

6 If you wish, adjust the Failed Authentication Attempts settings for Client Authentication in the Authentication page of the Global Properties.

7 Install the Security Policy.

**Allowing Client Authentication Wait Mode**

When using Manual Sign On, and the user authenticates with a Telnet session to port 259 on the Gateway, Wait Mode makes it unnecessary to open a new Telnet session in order to Sign Off and withdraw Client Authentication privileges.

To enable Wait Mode, edit the Check Point Gateway object, and in the Authentication page, check Enable Wait Mode for Client Authentication.

In Client Authentication Wait Mode, VPN-1 Pro monitors the Telnet connection to port 259 of the Gateway by pinging the user’s host. You should define rules to allow the ping as follows:

1. Allow the echo-request service from the VPN-1 Pro Gateway to the user’s host.
2. Allow the echo-reply service from the user’s host to the VPN-1 Pro Gateway.

**Configuring Authentication Tracking**

Successful and unsuccessful authentication attempts can be monitored in SmartView Tracker or via other tracking options, such as email, alerts, etc. Authentication tracking is configured in the following ways:

1. Failed authentication attempts can be tracked for all forms of Authentication. On the Authentication page of a Gateway Object, the Authentication Failure Track property sets the tracking option when authentication failures occur. The selection that you make here sets the tracking policy for all failed authentication attempts that take place through this gateway.

2. Successful authentication attempts can be tracked for Client Authentication. In the Client Authentication Action Properties window, the Successful Authentication Tracking property sets the tracking option for all successful Client Authentication attempts. Right click in the Action column of the Client Authentication rule to set this option. The default setting is Log.

3. You can track all Authentication attempts, whether successful or unsuccessful, by selecting an option in the Track column of any rule using a form of authentication. The tracking option set by rule can only add to the tracking policy set in the
Configuring Authentication

Gateway Object. For example, if the Gateway Object is set to Log all failed authentication attempts, setting a rule to None will have no effect - failed authentication attempts will still be logged in SmartView Tracker. However, setting the rule to Alert will cause an Alert to be sent for each failed authentication attempt.

**Note** - Authentication failure tracking for Check Point firewalls prior to version NG is set by the Authentication Failure Track property on the Authentication page of Global Properties.

**Configuring a VPN-1 Pro Gateway to use RADIUS**

1. In SmartDashboard, create a RADIUS Host object by choosing Manage > Network Objects > New > Node > Host... Name it and assign it an IP address.

2. Create a RADIUS Server object by choosing Manage > Server and OPSEC Applications > New... > RADIUS...

   A. Name the RADIUS Server object.

   B. Associate the RADIUS Server object with the RADIUS Host object you created in step 1.

   C. Assign the Service - choose between RADIUS on port 1645 service or NEW-RADIUS on port 1812. (The default setting is RADIUS, however the RADIUS standards group recommends using NEW-RADIUS, as 1645 can conflict with the datametrics service running on the same port.)

   D. Assign the same Shared Secret that you configured on the actual RADIUS server.

   E. Choose whether you want RADIUS Ver. 1.0 Compatible, which is RFC 2138 compliant, or RADIUS Ver. 2.0 Compatible, which is RFC 2865 compliant.

   F. Assign the RADIUS server’s Priority if you are employing more than one RADIUS Authentication Server.

   G. Click OK.

3. Right click on your gateway object and choose Edit > Authentication page. Enable RADIUS authentication.

4. Define a user group by choosing Manage > Users & Administrators > New > User Group (e.g. RADIUS_Users).

5. Enable RADIUS authentication for VPN-1 Pro users by choosing Manage > Users and Administrators > New > User by Template > Default.
6 Enable RADIUS authentication for users without VPN-1 Pro user accounts by creating an External User Profile. Choose Manage > Users and Administrators > New > External User Profile > Match all users... or Match by domain.... If you are supporting more than one external authentication scheme, make sure to set up your External User Profiles with the setting Match By Domain.

7 For all User Profiles and Templates:
   A On the General tab, enter the default login name for the RADIUS Server. (When configuring Match all users as an External User Profile, the name “generic*” is automatically assigned).
   B On the Personal tab, adjust the Expiration Date.
   C On the Authentication tab, choose RADIUS from the drop down list.
   D On the Groups tab, add the User Profile to the RADIUS group.

8 Make sure that you enable traffic between the SmartCenter Server and the RADIUS Authentication Server.

9 Verify that communications between the firewall and the RADIUS Server are not NATed in the Address Translation Rule Base.

10 Save, verify, and install the policy.

**Configuring a VPN-1 Pro Gateway to use SecureID**

1 Generate and copy the sdconf.rec file from the ACE/Server to:
   - on UNIX, Linux or IPSO - /var/ace/sdconf.rec;
   - on Windows NT - %SystemRoot%\System32\sdconf.rec.

2 In SmartDashboard, right click on your gateway object and choose Edit > Authentication page. Enable SecurID authentication.

3 Define a user group by choosing Manage > Users & Administrators > New > User Group (e.g. SecurID_Users).

4 Enable SecurID authentication for VPN-1 Pro users by choosing Manage > Users and Administrators > New > User by Template > Default.

5 Enable SecurID authentication for users without VPN-1 Pro user accounts by creating an External User Profile. Choose Manage > Users and Administrators > New > External User Profile > Match all users... or Match by domain.... If you are supporting more than one external authentication scheme, make sure to set up your External User Profiles with the setting Match By Domain.
Configuring Authentication

6 For all User Profiles and Templates:

A On the **General** tab, enter the default login name for the ACE/Server. (When configuring **Match all users** as an External User Profile, the name “**generic**” is automatically assigned).

B On the **Personal** tab, adjust the **Expiration Date**.

C On the **Authentication** tab, choose **SecurID** from the drop down list.

D On the **Groups** tab, add the User Profile to the SecurID group.

7 Make sure that you enable traffic between the SmartCenter Server and the ACE/Server.

8 Verify that communications between the firewall and the ACE/Server are not NATed in the Address Translation Rule Base.

9 Save, verify, and install the policy.

**Configuring a VPN-1 Pro Gateway to use TACACS+**

1 In SmartDashboard, create a TACACS Host object by choosing **Manage > Network Objects > New > Node > Host...** Name it and assign it an IP address.

2 Create a TACACS server by choosing **Manage > Server and OPSEC Applications > New...> TACACS...**

   A **Name** the TACACS Server object.

   B Associate the TACACS Server object with the TACACS **Host** object you created in step 1.

   C Choose the **Type** of TACACS you want to run. (The default is **TACACS**, but **TACACS+** is recommended).

   D Assign the **Service** - match the TACACS service (UDP or TCP) to the **Type** you chose in step C.

3 Right click on your gateway object and choose **Edit > Authentication page**. Enable **TACACS** authentication.

4 Define a user group by choosing **Manage > Users & Administrators > New > User Group** (e.g. TACACS_Users).

5 Enable TACACS authentication for VPN-1 Pro users by choosing **Manage > Users and Administrators > New > User by Template > Default**.
6 Enable TACACS authentication for users without VPN-1 Pro user accounts by creating an External User Profile. Choose Manage > Users and Administrators > New > External User Profile > Match all users... or Match by domain.... If you are supporting more than one external authentication scheme, make sure to set up your External User Profiles with the setting Match By Domain.

7 For all User Profiles and Templates:
   A On the General tab, enter the default login name for the TACACS Server. (When configuring Match all users as an External User Profile, the name “generic*” is automatically assigned).
   B On the Personal tab, adjust the Expiration Date.
   C On the Authentication tab, choose TACACS from the drop down list.
   D On the Groups tab, add the User Profile to the TACACS group.

8 Make sure that you enable traffic between the SmartCenter Server and the TACACS Authentication Server.

9 Verify that communications between the firewall and the TACACS Server are not NATed in the Address Translation Rule Base.

10 Save, verify, and install the policy.
Configuring Authentication
Section 2: Connectivity

This section describes how to give internal users and resources unrestricted yet secure connectivity across the enforcement point.
Network Address Translation (NAT)

In This Chapter

The Need to Conceal IP Addresses  page 63
Check Point Solution for Network Address Translation  page 64
Planning Considerations for NAT  page 75
Configuring NAT  page 76
Advanced NAT Configuration  page 81

The Need to Conceal IP Addresses

In an IP network, each computer is assigned a unique IP address that defines both the host and the network. Many computers in an organization have private, non-routable IP addresses, but nevertheless require access to the Internet. In most cases it is impossible to simply give them Internet-routable IP addresses, due to the lack of available public IP addresses, and administrative constraints.

IPv4 (the current version of IP) provides only 32 bits of address space, so available IP addresses are becoming scarce, most having already been assigned. Internet Service Providers will usually allocate only one or a few addresses at a time. Larger companies may purchase several addresses for use, but purchasing addresses for every computer on the network is usually impossible.

Even if public IP addresses become available, changing the addresses of every machine in a large network can be an administrative nightmare, being both labor intensive and time consuming.
Whether computers have a routable or a non-routable addresses, the administrator may wish to conceal their real addresses for security reasons. The administrator may wish to ensure that addresses cannot be seen from outside the organization, or even from other parts of the same organization. Making a network’s internal addresses public knowledge can reveal the topology of the network. Hiding this information can only enhance security.

Check Point Solution for Network Address Translation

In This Section

Public and Private IP addresses  page 64
NAT in FireWall-1  page 65
Static NAT  page 65
Hide NAT  page 66
Automatic and Manual NAT Rules  page 68
Address Translation Rule Base  page 68
Bidirectional NAT  page 69
Understanding Automatically Generated Rules  page 69
Port Translation  page 71
NAT and Anti-Spoofing  page 72
Routing Issues  page 72
IP Pool NAT  page 74
Disabling NAT in a VPN Tunnel  page 75

Public and Private IP addresses

Public IP addresses are those that are routable on the Internet. RFC 1918 documents private address spaces can be used on internal networks that will not have hosts directly connected to the Internet. The Internet assigned Numbers authority (IANA) has set aside the following three blocks of IP addresses for internal (private) network use:

- Class A network numbers: 10.0.0.0–10.255.255.255
- Class B network numbers: 172.16.0.0–172.31.255.255
- Class C network numbers: 192.168.0.0–192.168.255.255

In an intranet that uses private addresses, a FireWall-1 NAT gateway is put in place to connect the intranet to the Internet. The FireWall-1 Global Properties > NAT page specifies the address ranges that FireWall-1 considers private (non-unique).
NAT in FireWall-1

Network Address Translation (NAT) involves replacing one IP address with another. NAT can change both the source and destination address inside the packet. This means that a packet that is sent from the internal (protected) to the external (unprotected) side of the firewall appears to the destination as if it came from a different address, and packet that is sent from the external to the internal side of the firewall will arrive at the correct address.

FireWall-1 supports two kinds of NAT:

- **Static NAT**, where each private address is translated to a corresponding public address. In a typical Static NAT scenario with a number of machines in an internal network, the address of each machine is translated to a different public IP address. It is a many-to-many translation. Static NAT allows machines on both sides of the FireWall-1 Gateway to initiate connections, so that, for example, internal servers can be made available externally.

- **Hide NAT**, where a single public address is used to represent multiple computers on the internal network with private addresses. Hide NAT is a many-to-one translation. Hide NAT allows connections to be initiated only from the protected side of the FireWall-1 Gateway.

NAT can be performed on Check Points, Nodes, Networks, Address Ranges, and Dynamic objects.

NAT can be defined either automatically, via the network object, which automatically adds rules to the Address Translation Rule Base, or manually, by defining rules in the Address Translation Rule Base.

Manually creating NAT Rules adds extra flexibility. For example, as well as translating IP addresses, it is possible to translate the Service, in other words the destination port numbers. *Port number translation* is a type of Static NAT, in which one port number is translated to another port number.

**Static NAT**

Static NAT translates each private address to a corresponding public address.

- Static NAT on a node translates the private address of the node to a public address.
- Static NAT on a network or address range translates each IP address in the network or range to a corresponding public IP address, starting from the defined Static IP address.

In FIGURE 4-1, an address range (10.1.1.2 to 10.1.1.10) is hidden behind IP address a NAT range (192.168.0.2-192.168.0.11). A connection is shown originating at 10.1.1.3, and the source and destination translation for the original and reply packet.
Hide NAT

With a NAT gateway, it is possible to share a single public address with multiple computers on your intranet that have private addresses. The Internet is unaware of the division you have created between the Internet and your intranet, and sees your multiple computer connection as simply a single connection.

Hide NAT allows only connections that originate on the internal network. This lets an internal host initiate a connection to both inside and outside the intranet, but a host outside the network cannot initiate a connection to an internal host.

The Hide Address is the address behind which the internal network, address range or node is hidden. You can choose to hide the internal address(es)

- behind a virtual IP address, which is a public (routable) IP address that does not belong to any real machine, or
- behind the IP address of the FireWall-1 interface through which the packet is routed out (what used to be known as “Hiding behind IP address 0.0.0.0”).

In FIGURE 4-2, an address range (10.1.1.2 to 10.1.1.10) is hidden behind the address of the external FireWall-1 interface (192.168.0.1). A connection is shown originating at 10.1.1.3, and the source and destination translation for the original and reply packet.
FIGURE 4-2  Hide NAT on An Address Range

How Hide NAT Works

In Hide Mode, the source port numbers of the packets are modified. When return packets enter a firewall, FireWall-1 determines by port number to which internal machines the packets are destined. Port numbers are dynamically assigned from two pools of numbers:

- from 600 to 1023
- from 10,000 to 60,000

Port numbers are almost always assigned from the second pool. The first pool is used for only three services: rlogin (destination port 512), rshell (destination port 513) and rexec (destination port 514). If the service of the connection is one of these three, and the original source port is less than 1024, then a port number is assigned from the first pool. This behavior is configurable.

FireWall-1 keeps track of the port numbers assigned, so that the original port number is correctly restored for return packets. A port number currently in use is not assigned again to a new connection.

Hide NAT has a capacity of 50,000 connections per server. This means that the Hide NAT capacity limit is only reached if more than 50,000 connections from Hide NATed internal clients are simultaneously directed at a single server on the unprotected side of the FireWall-1 Gateway—a webcast of a wildly popular basketball game, perhaps?
### Automatic and Manual NAT Rules

NAT can be defined *automatically* via the network object (Node, Network or Address Range). When you define NAT via the network object, rules are automatically added to the Address Translation Rule Base.

You can *manually* specify NAT rules, by adding or editing NAT rules to the Address Translation Rule Base. FireWall-1 validates manual NAT rules, helping to avoid mistakes in the setup process. Creating manual NAT Rules gives maximum control over the way NAT will function. You can specify the source, destination and service separately for the original and the translated packet.

When creating Manual NAT Rules, you must explicitly define the translated network objects in addition to the original objects. With Automatic rules this is not necessary. Automatic NAT rules cannot be edited in the Address Translation Rule Base.

### Address Translation Rule Base

The Address Translation Rule Base is shown in **FIGURE 4-3**.

**FIGURE 4-3  Address Translation Rule Base**

<table>
<thead>
<tr>
<th>NO.</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>INSTALL ON</th>
<th>COMMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alaska_web</td>
<td>Any</td>
<td>Any</td>
<td>Original</td>
<td>Original</td>
<td>All</td>
<td>Automatic rule uses the network object data</td>
<td></td>
</tr>
</tbody>
</table>

Each rule specifies what happens to the first packet of a connection. Reply packets travel in the opposite direction to the original packet, but are matched to the same rule.

The Address Translation Rule Base is divided into two sections, the Original Packet section, and the Translated Packet section. The Original Packet section specifies the conditions when the rule is applied. The Translated Packet section specifies the action taken when the rule is applied.

Each section in the Address Translation Rule Base Editor is divided into Source, Destination, and Service. 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
Rule Match Order

Rule matching in the Address Translation Rule Base follows the same principle as in the Security Rule Base (see “The Security Rule Base” on page 19). When FireWall-1 receives a packet belonging to a connection, it compares it against the first rule in the Rule Base, then the second, then the third, and so on. When it finds a rule that matches, it stops checking and applies that rule.

The exception to this is when two automatic rules can match a connection, and Bidirectional NAT is turned on.

Bidirectional NAT

Bidirectional NAT applies to automatic NAT rules in the Address Translation Rule Base, and allows two automatic NAT rules to match a connection. Without Bidirectional NAT, only one automatic NAT rule can match a connection.

When NAT is defined for a network object, an automatic NAT rule is generated which performs the required translation. If there are two such objects and one is the source of a connection and the other the destination, then without Bidirectional NAT, only one of these objects will be translated, because only one of the automatically generated NAT rules will be applied, and so a connection between the two objects will only be allowed in one direction. With Bidirectional NAT, both automatic NAT rules are applied, and both objects will be translated, so connections between the two objects will be allowed in both directions.

The detailed logic of Bidirectional NAT is as follows:

- If the first match on a connection is on a Manual NAT rule, no further checking of NAT Rule Base is done.
- If the first match on a connection is on an Automatic NAT rule, then the rest of the NAT Rule Base is checked, one rule at a time, to see if another Automatic NAT Rule matches the connection. If it does, both rules are matched, and no further checking is performed.

The operation of Bidirectional NAT can be tracked using the SmartView Tracker, using the fields NAT Rule Number and NAT Additional Rule Number. The “additional rule” is the rule that matches the automatic translation performed on the second object in Bidirectional NAT.

Understanding Automatically Generated Rules

NAT can be defined automatically via the network object (Node, Network or Address range). When you define NAT via the network object, rules are automatically added to the Address Translation Rule Base.
Hide NAT on a Node adds one rule to the Address Translation Rule Base. It specifies that the source address of the packet is translated for connections that originate in the Node in the internal network. This is called a Source Hide Rule.

Static NAT on a Node adds two rules to the Address Translation Rule Base. In addition to the Source Hide rule, another rule specifies that for connections that originate in the external network, the Destination address of the packet is translated. This is called a Destination Static Rule.

If NAT (Hide or Static) is performed on a Network or an address range, an extra rule is added. The extra rule specifies that communication within the network or address range is not translated, that is, a packet sent from one machine to another in the same network is not changed.

**Example of Automatically Generated Rule — Hide NAT**

For the scenario in FIGURE 4-2 on page 67, automatically defined Hide NAT on the address range Node adds two rules to the NAT Rule Base, as shown in FIGURE 4-5.

**FIGURE 4-4  Automatically Generated NAT Rules for Hide NAT on an Address Range**

<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>Range_Hide</td>
<td>Range_Hide</td>
<td>Any</td>
<td>Original</td>
</tr>
<tr>
<td>2</td>
<td>Range_Hide</td>
<td>Any</td>
<td>Any</td>
<td></td>
</tr>
</tbody>
</table>

Rule 1 says that for connections within the internal (unprotected) side of the firewall, no NAT takes place.

Rule 2 says that for connections initiated on the internal (protected) side of the firewall, the source address of the packets is translated to the public Hide NAT address.

In automatic Hide NAT rules, the translated address is known as the Hiding Address, and this is the address that is known and used on the unprotected side of the FireWall-1 Gateway. The “real” addresses are the private addresses that are used on the protected side of the FireWall-1 Gateway.

**Example of Automatically Generated Rules — Static NAT**

For the scenario in FIGURE 4-1 on page 66, automatically defined Static NAT on the Node adds two rules to the NAT Rule Base, as shown in FIGURE 4-5.
FIGURE 4-5  Automatically Generated NAT Rules for Static NAT on an Address Range

<table>
<thead>
<tr>
<th>NO.</th>
<th>ORIGINAL PACKET</th>
<th>TRANSLATED PACKET</th>
<th>INSTALL</th>
<th>COMMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Range_static</td>
<td>Any</td>
<td>Original</td>
<td>Automatic rule (see the network object data)</td>
</tr>
<tr>
<td>2</td>
<td>Range_static</td>
<td>Any</td>
<td>Original</td>
<td>Automatic rule (see the network object data)</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Range_static</td>
<td>Original</td>
<td>Automatic rule (see the network object data)</td>
</tr>
</tbody>
</table>

Rule 1 says that for connections within the internal (unprotected) side of the firewall, no NAT takes place. A packet sent from one machine to another in the same network is not changed.

Rule 2 says that for packets originating on the internal (protected) side of the firewall, source addresses are translated to valid (public) static NAT addresses.

Rule 3 says that for packets originating on the external (unprotected) side of the firewall, valid (public) destination addresses are translated to static NAT addresses.

In automatic Static NAT rules, statically translated public addresses are called *Valid Addresses*, and these are the addresses that are known and used on the unprotected side of the FireWall-1 Gateway. The “real” addresses are the private addresses that are used on the protected side of the FireWall-1 Gateway.

**Precedence In Automatic Rules**

Automatic Rules are placed in the Address Translation Rule Base as follows:

1. Static NAT rules before Hide NAT rules.
2. NAT on a node before NAT on a network or an address range.

**Port Translation**

Port Translation allows multiple application servers in a hidden network to be accessed using the a single IP address, based on the requested service (destination port). This has the benefit of saving on scarce public IP addresses. An typical implementation could allow an FTP server (accessible via port 21), an SMTP server (port 25) and an HTTP server (port 80) to be accessed using a single IP public address.

To use Port Translation you need to craft manual NAT rules. Port Translation rules are supported on FireWall-1 enforcement points of version NG FP3 and higher.
NAT and Anti-Spoofing

NAT is always performed after the anti-spoofing checks, and anti-spoofing checks are performed only on the source IP address of the packet. This means that irrespective of NAT, spoofing protection is configured on the interfaces of the FireWall-1 Gateway in the same way. Unlike in previous versions of FireWall-1, there are no special issues regarding anti-spoofing configuration and NAT.

Routing Issues

Static Routes on the FireWall-1 Gateway

This section is intended only for administrators who have upgraded the SmartCenter Server, where in the pre-upgrade:

- pre-NG version, automatic NAT for the server was performed on the server side, or in the
- pre-NG FP3 version, manual NAT for the server was performed on the server side.

In a client-server connection across the FireWall-1 Gateway, connections originate at the client, and the server sends reply packets back to the client.

In NG versions of FireWall-1, for both manual and automatic rules, NAT for the server is performed by default on the client side of the FireWall-1 Gateway (FIGURE 4-6). This ensures that the Operating System routes the packets correctly.

In FIGURE 4-6, for the original packet, the FireWall-1 Gateway translates the destination address to the valid address of the server, and then the packet is routed to destination.

For reply packets, no NAT is performed on the destination, and the OS correctly routes the packet back to the client.
The NG default setting ensures reliable anti-spoofing and routing. It is recommended to stick to the default setting unless you have upgraded your SmartCenter Server from a pre-NG version, and you have FireWall-1 enforcement modules whose configuration requires other settings.

If NAT for the server destination is configured to be performed on the server side, the operating system receives the packet for routing before NAT is performed. The operating system therefore sees a valid address as the destination, and will therefore route the packet back out to the Internet router rather than to the server.

To resolve this, configure Static Host Routes on the FireWall-1 Gateway, so that it forwards packets to the correct interface. For example:

```
route add 192.168.0.3 10.1.1.2
```

**Automatic and Proxy arp**

Giving a machine in the internal network an external IP address using NAT makes that machine appear to the Internet to be on the external network, on the Internet side of the firewall.
When NAT is configured automatically, the FireWall-1 Gateway machine will reply on behalf of translated network objects to arp requests from the internet router for the address of the internal machine (FIGURE 4-7).

**FIGURE 4-7** Illustrating Automatic Arp configuration

If using manual rules, you must configure proxy-arps. In other words, you must associate the translated IP address with the MAC address of the FireWall-1 Gateway interface that is on the same network as the translated addresses.

**IP Pool NAT**

An IP Pool is a range of IP addresses (an Address Range, a network or a group of one of these objects) routable to the gateway.

IP Pool NAT ensures proper routing for two connection scenarios:

- SecuRemote/SecureClient to MEP (Multiple Entry Point) Gateways
- Gateway to MEP Gateways

When a connection is opened from a SecuRemote/SecureClient or a client behind a Gateway, to a server behind the MEP Gateways, the first packet is routed through one of the MEP Gateways. Return packets in the connection must be routed back through the same Gateway in order to maintain the connection. To ensure that this happens, each of the MEP Gateways maintains a pool of IP addresses that are routable to the Gateway itself. When a connection is opened to a server, the gateway substitutes an IP address from the IP Pool for the source IP address. Reply packets from the server return to the gateway, which restores the original source IP address and forwards the packets to the source.

The pool of IP addresses is defined as an IP range or collection of ranges in the NAT page of the Gateway object.
Disabling NAT in a VPN Tunnel

When communicating within a VPN, it is usually not necessary to perform NAT. It is possible to disable NAT in a VPN tunnel with a single click in the VPN community object. Disabling NAT in a VPN tunnel by defining a NAT rule will slow down the performance of the VPN.

Planning Considerations for NAT

In This Section

- Hide Versus Static
- Automatic Versus Manual Rules
- Choosing the Hide Address in Hide NAT

Hide Versus Static

For protocols where the port number cannot be changed, Hide NAT cannot be used. When the external server must distinguish between clients based on their IP addresses, Hide NAT cannot be used, because all clients share the same IP address under Hide NAT.

To allow connections from the external network to the internal network, only Static NAT can be used.

Automatic Versus Manual Rules

Automatic NAT rules are easy to configure and so are less prone to configuration errors. Automatic ARP configuration is only effective for automatic rules.

Manually defining NAT Rules is complicated, but gives complete control over NAT. The following can only be done using Manual NAT Rules:

- Restricting rules to specified destination IP addresses, as well as to specified source IP addresses.
- Translating both source and destination IP addresses in the same packet.
- Performing Static NAT only in one direction
- Translating services (destination ports).
- Restricting rules to specified services (ports).
- Performing NAT on Dynamic objects.
Choosing the Hide Address in Hide NAT

The Hide Address is the address behind which the network, address range or node is hidden.

It is possible to either hide behind the interface of the Install on Gateway, or to hide behind a specified IP address.

Choosing a fixed public IP address is a good option if you wish to hide the address of the FireWall-1 Gateway. However, it means using an extra publicly routable IP address.

Choosing to hide behind the address of the Install On Gateway is a good option for administrative purposes. If the external IP address of the firewall changes, there is no need to change the NAT settings.

Configuring NAT

In This Section

- General Steps for Configuring NAT
- Basic Configuration - Network Node with Hide NAT
- Sample Configuration - Static and Hide NAT
- Sample Configuration - Using Manual Rules for Port Translation

General Steps for Configuring NAT

The steps for configuring NAT are always the same:

1. Determine the IP addresses to be used for translation.
2. Define Network Objects.
3. Define the Access Rules in the Security Rule Base. When defining Manual NAT rules, you must define network objects with translated addresses, whereas if using Automatic NAT Rules, you need define only one network object per real object. For example, if Static NAT is defined on an object called Alaska_Web, then the Security Rule Base need only refer to Alaska_Web (as in FIGURE 4-8), and there is no need to define a rule for Alaska_Web (Valid Address).

FIGURE 4-8  Example Security Rule Base Rule for an object with Automatic NAT

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Alaska_Web</td>
<td>Accept</td>
</tr>
</tbody>
</table>
4 Define NAT Rules (Automatic and/or Manual).
5 Install the Security Policy.

**Basic Configuration - Network Node with Hide NAT**

The following example shows how to set up basic Hide NAT for the configuration in FIGURE 4-9. The aim is to hide the IP address of the Alaska_Web web server (10.1.1.10) from connections that originate on the Internet. Alaska_GW has three interfaces, one of which faces the network on which Alaska_Web resides.

**FIGURE 4-9** Example Network Showing Network Node with Hide NAT

1 Edit the Node object for Alaska_Web, and in the NAT page, select *Add Automatic Address Translation rules* (FIGURE 4-10).
2 Select Translation Method Hide, and the option Hide behind the interface of the Install on Gateway.

3 Select the Install on Gateway. The NAT Gateway in this example is Alaska_GW, so you can select either Alaska_GW or All.

Packets originating in Alaska_Web with the Internet as their destination will have their source address translated from 10.1.1.10 to 192.168.0.1. For example, packets originating on the web server will have their source address changed from 172.16.10.3 to 192.168.0.1.

**Sample Configuration - Static and Hide NAT**

The goal is make the SMTP server and the HTTP server on the internal network available to the Internet using public addresses, and provide Internet access for all users on the internal network.
The web and mail servers require static translation because incoming connections will be made to them from the Internet. Two routable addresses are available. 192.168.0.5 will be used for the Alaska.Web HTTP server, and 192.168.0.6 for the Alaska.Mail SMTP server.

The internal clients require hide translation because they will initiate connections. No incoming connections are allowed to them from the Internet. They will hide behind the external interface of the FireWall-1 Gateway.

1. Define network objects for Alaska.Web (10.1.1.5), Alaska.Mail (10.1.1.6), Alaska_LAN (10.1.1.0 with Net Mask 255.255.255.0), and the FireWall-1 Gateway (Alaska.GW).

2. Edit the Alaska.Web object, and in the NAT page check Add Automatic Address Translation Rules, select Translation Method Static, and define the Translate to IP Address as 192.168.0.5.

3. Similarly for Alaska.Mail, select Translation Method Static, and define Translate to IP Address as 192.168.0.6.

4. Edit the Alaska_LAN object, and in the NAT page select Translation Method Hide, and select Hide behind the interface of the Install On Gateway. The effective Hide address for the internal clients on Alaska_LAN is therefore 192.168.0.1.

The resulting Address Translation Rule Base is shown in FIGURE 4-12.
Configuring NAT

FIGURE 4-12 Automatic Address Translation Rule Base for Static and Hide NAT

<table>
<thead>
<tr>
<th>NO</th>
<th>ORIGINAL PACKET</th>
<th>TRANSLATED PACKET</th>
<th>INSTALL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alaska DMZ</td>
<td>Any</td>
<td>Alaska DMZ (Valid Address)</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Alaska DMZ (Valid Address)</td>
<td>Any</td>
</tr>
<tr>
<td>3</td>
<td>Alaska DMZ</td>
<td>Any</td>
<td>Alaska DMZ (Valid Address)</td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>Alaska DMZ (Valid Address)</td>
<td>Any</td>
</tr>
<tr>
<td>5</td>
<td>Alaska LAN</td>
<td>Alaska LAN</td>
<td>Alaska LAN (Valid Address)</td>
</tr>
<tr>
<td>6</td>
<td>Alaska LAN</td>
<td>Any</td>
<td>Alaska LAN (Valid Address)</td>
</tr>
</tbody>
</table>

Sample Configuration - Using Manual Rules for Port Translation

The goal is to make an both a web server and a mail server in a DMZ network available from the Internet using a single IP address. Hide NAT is to be performed on all addresses in the DMZ.

FIGURE 4-13 Sample Configuration - illustrating Port Translation using Manual NAT

1 Define network objects for the network Alaska.DMZ.LAN (172.16.0.0/16), the web server Alaska_DMZ_Web (172.16.1.7), and the Mail server Alaska_DMZ_Mail (172.16.1.5), and the FireWall-1 Gateway (Alaska.GW).

2 On the Alaska.DMZ.LAN network object, in the NAT tab, select Add Automatic Address Translation Rules, and Translation Method Hide, and select Hide behind the interface of the Install on Gateway. This adds two automatic rules to the Address Translation Rule Base (Rules 1 and 2 in FIGURE 4-14).
3 In the Address Translation Rule Base, define a Manual NAT Rule that translates requests for the HTTP service to the Web server (Rule 3 in FIGURE 4-14), and a Manual NAT Rule to translate SMTP requests to the SMTP server (Rule 4 in FIGURE 4-14).

**FIGURE 4-14 Address Translation Rule Base for Port Mapping**

<table>
<thead>
<tr>
<th>NO.</th>
<th>ORIGINAL PACKET</th>
<th>TRANSLATED PACKET</th>
<th>INSTALL ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
<td>Original</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Any</td>
<td>Original</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Any</td>
<td>Original</td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>Any</td>
<td>Original</td>
</tr>
</tbody>
</table>

**Advanced NAT Configuration**

In This Section

- Allowing Connections Between Translated Objects on Different Gateway Interfaces
- Enabling Communication for Internal Networks with Overlapping IP addresses
- SmartCenter Behind NAT

**Allowing Connections Between Translated Objects on Different Gateway Interfaces**

The goal is to allow connections in both directions between statically translated objects (nodes, networks or address ranges) on different FireWall-1 Gateway interfaces.

If NAT is defined via the network object (as opposed to using Manual NAT Rules), then you will need to ensure that Bidirectional NAT is enabled.

**Enabling Communication for Internal Networks with Overlapping IP addresses**

**Overview**

Where two internal networks have overlapping (or partially overlapping) IP addresses, VPN-1 Pro, 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 4-15 will be used as an example.

FIGURE 4-15 Example — Class C network

Both network A and network B share the same address space (192.168.1.0/24), so standard NAT cannot be used to enable communications between network A and network B. Instead, overlapping NAT must be performed on a per-interface basis.

Users in network A who wish to communicate with users in network B will use the 192.168.30.0/24 network as a destination. Users in network B who wish to communicate with users in network A will use the 192.168.20.0/24 network as a destination.

The FireWall-1 enforcement module will translate the IP addresses differently on each interface, as follows:

**interface A**

• inbound source IP addresses will be translated to virtual network 192.168.20.0/24
• outbound destination IP addresses will be translated to network 192.168.1.0/24

**interface B**

• inbound source IP addresses will be translated to network 192.168.30.0/24
• outbound destination IP addresses will be translated to network 192.168.1.0/24
interface C

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 (192.168.4.1).

Communication Example

Suppose you wish to allow communication between internal networks and between an internal network and the Internet, as follows:

Between Internal Networks

Suppose user A at IP address 192.168.1.10 in network A wishes to connect to user B at IP address 192.168.1.10 (the same IP address) in network B. User A opens a connection to IP address 192.168.30.10.

Between an Internal Network and the Internet

Suppose user A at IP address 192.168.1.10 in network A connects to IP address 10.10.10.10 on the Internet.

### TABLE 4-2

<table>
<thead>
<tr>
<th>step</th>
<th>source IP address</th>
<th>destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface A — before NAT</td>
<td>192.168.1.10</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>interface A — after NAT</td>
<td>192.168.20.10</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>FireWall-1 enforcement module enforces Security Policy for packets from network 192.168.20.0/24 to network 192.168.30.0/24.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface B — before NAT</td>
<td>192.168.20.10</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>interface B — after NAT</td>
<td>192.168.20.10</td>
<td>192.168.1.10</td>
</tr>
</tbody>
</table>

### TABLE 4-3

<table>
<thead>
<tr>
<th>step</th>
<th>source IP address</th>
<th>destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface A — before NAT</td>
<td>192.168.1.10</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>interface A — after NAT</td>
<td>192.168.20.10</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>FireWall-1 enforcement module enforces Security Policy for packets from network 192.168.20.0/24 to the Internet.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface C — before NAT</td>
<td>192.168.20.10</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>interface C — after NAT Hide</td>
<td>192.168.4.1</td>
<td>10.10.10.10</td>
</tr>
</tbody>
</table>
Routing Consideration

In order to allow routing from network A to network B, routing needs to be configured on the firewall machine. The following examples are for Windows and Linux. For other Operating Systems, use the equivalent commands:

On Windows

```plaintext
route add 192.168.30.0 mask 255.255.255.0 192.168.3.2
route add 192.168.20.0 mask 255.255.255.0 192.168.2.2
```

On Linux

```plaintext
route add -net 192.168.30.0/24 gw 192.168.3.2
route add -net 192.168.20.0/24 gw 192.168.2.2
```

VPN-1 Pro Object Database Configuration

To implement the overlapping NAT feature, use the `dbedit` database editor GUI (or command line utility).

In the example configuration, you would set the per interface values for interface A and interface B as follows:

### TABLE 4-4

<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_dst_ipaddr</td>
<td>The overlapping IP addresses (before NAT). In the example configuration, this would be 192.168.1.0 for both interfaces.</td>
</tr>
<tr>
<td>overlap_nat_src_ipaddr</td>
<td>The IP addresses after NAT. In the example configuration, this would be 192.168.20.0 for interface A, and 192.168.30.0 for interface B.</td>
</tr>
<tr>
<td>overlap_nat_netmask</td>
<td>The net mask of the overlapping IP addresses. In the example, 255.255.255.0.</td>
</tr>
</tbody>
</table>

SmartCenter Behind NAT

The SmartCenter server sometimes uses a private IP address (as listed in RFC 1918), or some other non routable IP address. Using private addresses for the internal networks has become common, mainly because the lack of IP addresses.
Network Address Translation for the SmartCenter Server IP address is easy to configure. Static or Hide NAT on the SmartCenter Server address can be configured in one click, while still allowing connectivity with managed enforcement modules. All enforcement modules can be controlled from the SmartCenter Server, and logs can be sent to the SmartCenter Server.

Network Address Translation can also be configured for a Management High Availability server and a Log Server, as well as for a SmartCenter Server.

**Note** - SmartCenter Behind NAT is not supported for deployments in which SmartCenter also acts as an enforcement module and must be addressed from outside the NATed domain (for example, when it receives SAM commands).

**FIGURE 4-16** shows a typical scenario. The SmartCenter Server is in a network on which Network Address Translation is performed (the “NATed network”). The SmartCenter Server is able to control Check Point enforcement modules inside the NATed network, on the border between the NATed network and the outside world, and outside the NATed network.

**FIGURE 4-16** Typical configuration with NAT for the SmartCenter

In ordinary Hide NAT configurations, no connections can be established from the external side the FireWall-1 NAT gateway. In contrast, when using Hide NAT on the SmartCenter Server, enforcement modules are able to send logs to the SmartCenter Server.

When using the SmartCenter behind NAT feature, the enforcement module (that is, the remote module) automatically selects the SmartCenter address to be addressed, and simultaneously applies NAT considerations when making this selection.

NAT for the SmartCenter Server is enabled in the **NAT** page of the SmartCenter Server object by defining NAT and selecting **Apply for VPN-1 & FireWall-1 control connections**.

There are situations in which the module will decide to contact the SmartCenter with an address that does not correspond to the remote module’s deployment. For example:
• When there are enforcement modules from a version prior to NG with Application Intelligence. In such a case, refer to SecureKnowledge solution SK15558 at http://support.checkpoint.com/kb/ for further instructions.
• When the enforcement module’s automatic selection does not conform with the routing of the module’s deployment.

In the second case, you can define the masters and loggers manually. This allows the remote module to contact SmartCenter using the desired address. When an inbound connection from a managed module comes in to the FireWall-1 Gateway, port mapping is used to translate from the hiding address to the real IP address of the SmartCenter Server.

To do this select **Use local definitions for Log Servers** and **Use local definitions for Masters** and specify the correct IPs on the enforcement module.

Such a solution encompasses two cases:
• The remote module addresses the NATed IP when you would like it to address the real IP.
• The remote module addresses the real IP when you would like it to address the NATed IP. In this case, specify the SIC name of the SmartCenter in the masters file.

Note that:
• Only one object can be defined with these settings, unless the second object is defined as a Secondary SmartCenter Server or a Log Server.
• It is important to properly define the Topology settings on all enforcement modules. In FIGURE 4-16 for example, on California_GW, you must define the Primary_SmartCenter on its internal interface.
• All managed modules, and the SmartCenter Server must be of version NG with Application Intelligence and above.
• In previous versions, various workarounds were required. All previous workarounds will continue to work, with no changes in behavior.

**Configuring the SmartCenter Server Object**

1. On the Primary_SmartCenter object, In the NAT page, choose either Static NAT or Hide NAT.

   If using Hide NAT, select **Hide behind IP Address** (for example, 192.168.55.1). Do not **Hide behind Gateway** (address 0.0.0.0).

2. Install on the Gateway that protects the NATed objects or network. Do not select All. In FIGURE 4-16, **Install on Gateway:** California_GW.

3. Check **Apply for VPN-1 and FireWall-1 control connections**.
Configuring the Enforcement Module Object

California_GW must know that Primary_SmartCenter is behind it. In the California_GW Topology page, define:

- Interface Eth3

In the General tab of the Interface Properties window of this interface:

- IP Address 10.0.0.0
- Netmask 255.255.0.0

In the Topology tab of the Interface Properties window of this interface:

- Network defined by the interface IP and Net Mask.

Configuring Pre-NG with Application Intelligence Enforcement Module Objects

For managed modules that are not of version NG with Application Intelligence or higher, you must define a dummy object. Referring to FIGURE 4-16, if Florida_GW and California_GW have a version lower than NG with Application Intelligence, the dummy objects ensure that

- Florida_GW knows that its SmartCenter Server has the address 192.168.255.1.
- California_GW knows that its SmartCenter Server has the address 10.0.0.1.

Proceed as follows:

Define a dummy object with the translated address of the Primary_SmartCenter:

1. Give it a Name (Dummy-SmartCenter).
2. In the General Properties page, in the Check Point Products section, select Secondary Management Station and Log Server.

Define a dummy object for the California_GW object:

1. Give it a Name.
2. Give it the IP Address 192.168.255.1.
3. Give it the address of the Primary SmartCenter NAT definition.
4. In the General Properties page, in the Check Point Products section, select Secondary Management Station and Log Server.
5. In the Logs and Masters page:
   - Define Dummy-SmartCenter as a Master.
   - Define Dummy-SmartCenter as a Log Server (if the log server is on a separate machine, define two virtual objects).
Advanced NAT Configuration
CHAPTER 5

ISP Redundancy

In This Chapter

Need for ISP Link Redundancy  
Solution for ISP Link Redundancy  
Considerations for ISP Link Redundancy  
Configuring ISP Link Redundancy

Need for ISP Link Redundancy

As Internet access becomes increasingly critical to business, the costs associated with loss of that connectivity become greater. To protect against network downtime it makes sense to deploy redundant systems for mission critical Internet applications. Connecting to the Internet via more than one Internet Service Provider (ISP) provides that additional redundancy.

A number of solutions are available in the market to enable connections to multiple ISPs, however, these solutions require expensive specialized hardware, and need detailed knowledge to set up and maintain. A simple solution is needed that makes use of the existing boundary between the Internet and organization, namely the firewalled gateway.
Solution for ISP Link Redundancy

In This Section

ISP Redundancy Overview  page 90
ISP Redundancy Operational Modes  page 91
Monitoring the ISP Links  page 92
How ISP Redundancy Works  page 92
The ISP Redundancy Script  page 94
Manually Changing the Link Status (for isp_link)  page 94
ISP Redundancy Deployments  page 95
ISP Redundancy and VPNs  page 97

ISP Redundancy Overview

ISP Redundancy assures reliable Internet connectivity by allowing a single or clustered VPN-1 Pro gateway to connect to the Internet via redundant Internet Service Provider (ISP) links. The feature is part of the standard VPN-1 Pro installation, and does not require specialized and costly networking hardware, nor does it require new skills.

ISP Redundancy monitors the ISP links, and directs connections to the appropriate link, depending on the operating mode. The available modes are Load Sharing and Primary/Backup modes.

FIGURE 5-1 shows a typical deployment with a single ISP link, and redundant deployment with duplicate ISP links.
ISP Redundancy can work in one of two modes. These modes control the behavior of outgoing connections, that is, connections from clients in the internal networks towards the Internet:

- **Primary/Backup** mode connects to an ISP through the primary link, and switches to a backup ISP when the primary ISP link fails. When the primary link is restored, new outgoing connections are assigned to it, while existing connections are maintained over the backup link until they are complete.

- **Load Sharing** mode connects to both ISPs, while distributing the load of outgoing connections between the ISPs. New connections are randomly assigned to a link. If a link fails, all new outgoing connections are directed to the active link.

Incoming connections (connections from the Internet to application servers in the DMZ or internal networks) also benefit from the high availability of the two ISP links because VPN-1 Pro returns packets via the same ISP Link through which the connection was initiated.

In addition, in Load Sharing mode, incoming connections can reach the application servers via either ISP link. This is because VPN-1 Pro can answer DNS requests for the IP address of internal servers with addresses from both ISPs, alternating their order.
Monitors the ISP Links

ISP Redundancy monitors the status of the ISP links, and directs outgoing connections to the appropriate link.

To monitor the status of the link, VPN-1 Pro checks whether the interface is up or down, and also determines whether the cable is plugged in. The next hop router is also monitored automatically.

In addition, there is an optional way of monitoring the status of the ISP link. The administrator can configure a list of hosts that must answer to ICMP echo requests (pings) in order for the ISP link to be considered active. If one of the hosts fails to return any ICMP replies, the link is considered to be down. You may choose to include hosts such as an ISP web server or some other host on the Internet.

The status of the ISP links is reported by SmartView Status, in the *FireWall-1 Details* section.

How ISP Redundancy Works

Both outgoing connections from behind the VPN-1 Pro gateway towards the Internet, and incoming connections from the Internet, benefit from the existence of duplicate links.

Outgoing Connections

In Load Sharing mode, outgoing traffic that leaves the VPN-1 Pro gateway towards the Internet is distributed between the ISP Links. In Primary/Backup mode, outgoing traffic uses the primary link, if it is up.

Hide NAT is used to change the source address of outgoing packets to the address of the interface through which the packet leaves the VPN-1 Pro gateway. This allows return packets to be automatically routed through the same ISP link, because their destination address is the address of the appropriate link. Hide NAT must be configured by the administrator.

Incoming Connections

For external users to make incoming connections, the administrator must give each application server two routable IP addresses, one from each ISP. The administrator must also configure Static NAT to translate the routable addresses to the real server address.

If the servers handle different services (HTTP, FTP, etc.), it is possible to use NAT to make do with only two routable IP addresses for all the publicly available servers.
External clients use one of the two addresses. In order to connect, the clients must be able to resolve the DNS name of the server to the correct IP address.

**Note** - In these explanations, the subnets 172.16.0.0/24 and 192.168.0.0/24 represent public routable addresses.

This is illustrated in FIGURE 5-2. The web server **www.example.com** is assigned an IP address from each ISP: 192.168.1.2 from ISP A, and 172.16.2.2 from ISP B. If ISP link A is down, 192.168.1.2 becomes unavailable, so the clients must be able to resolve **www.example.com** to 172.16.2.2.

**FIGURE 5-2  IP address resolution for incoming connections**

The process by which an incoming connection is established, is as follows:

When a user in the Internet contacts **www.example.com**, the client machine sends a DNS query for the IP address. The DNS query reaches the VPN-1 Pro gateway.

VPN-1 Pro has a built-in mini-DNS server that can be configured to intercept DNS queries (of type A) for servers in its domain.

A DNS query arriving at an interface belonging to one of the ISP links is intercepted by VPN-1 Pro.

If VPN-1 Pro recognizes the name of the host, it will send a reply, as follows:

- In Primary/Backup mode, VPN-1 Pro replies only with the addresses associated with the primary link, as long as the primary link is active.
- In Load Sharing mode, VPN-1 Pro replies with two addresses, alternating their order.
If VPN-1 Pro is unable to handle the DNS requests, (it may not recognize the host name, for example), VPN-1 Pro passes the DNS query to its original destination, that is, the DNS server of the domain example.com.

When the external client receives the reply to its DNS query, it opens a connection. Once the packets reach the gateway, VPN-1 Pro uses Static NAT to translate the destination address 192.168.1.2 or 172.16.2.2 to the real server address 10.0.0.2.

VPN-1 Pro routes reply packets from the server to the client through the same ISP link that was used to initiate the connection.

### The ISP Redundancy Script

Whenever VPN-1 Pro starts or an ISP link changes state, a script runs. Depending on whether the ISP link is up or down, this script automatically changes the default route of the VPN-1 Pro enforcement module.

If one of the ISP links is a dialup interface, it is possible to manually edit the ISP Redundancy script, to make VPN-1 Pro take the dialup interface up or down when the ISP links change state, or when VPN-1 Pro starts.

The script can be configured to perform any other action. For example, to issue a SAM command to block certain traffic when the primary link goes down, in order to decrease the traffic load on the link.

The name and location of the ISP Redundancy script is $FWDIR/bin/cpisp_update.

### Manually Changing the Link Status (fw isp_link)

Use the `fw isp_link` command to configure the ISP link on VPN-1 Pro to **Down** or **Up**. This command is useful:

- To test your configuration.
- If you know the ISP link is down but VPN-1 Pro thinks otherwise. In that case, take care to use the command again to bring the link back up when the link in reality becomes available.

This command can be executed locally on the enforcement module or remotely from the SmartCenter Server. In the latter case the target argument must be supplied.

```
fw isp_link [target] link-name up|down
```
TABLE 5-1  fw isp_link arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>The name of the enforcement module.</td>
</tr>
<tr>
<td>link-name</td>
<td>The name of the ISP link, as defined in the ISP Redundancy page of the Gateway or Gateway Cluster object.</td>
</tr>
</tbody>
</table>

ISP Redundancy Deployments

A number of deployments are supported. Considerations for choosing each deployment are described in “Considerations for ISP Link Redundancy” on page 100.

Two External Interfaces

The simplest way of connecting to two ISPs is to connect each VPN-1 Pro gateway interface to a different ISP via a LAN, as in FIGURE 5-3. The next hop routers are either at the boundary of the organization or at the ISP.

FIGURE 5-3  Two ISPs connected to different external VPN-1 Pro gateway interfaces

One External Interface

If only one external interface is available on the VPN-1 Pro gateway, you can configure two subnets on the same external interface. Both ISP links are then connected to the same VPN-1 Pro interface, but to different next hop routers (usually via a switch). This is illustrated in FIGURE 5-4.
FIGURE 5-4  Two ISPs connected to the same VPN-1 Pro gateway external interface

One Permanent and One Dialup (Backup) Interface
To connect to one of the ISPs via a dialup network (a modem), and to the other ISP via a LAN, connect each VPN-1 Pro gateway external Interface to a different ISP link, as in FIGURE 5-5. This deployment is useful if you have a dialup connection to your backup ISP.

FIGURE 5-5  One ISP link is a LAN, and the other is a dialup network

Gateway Cluster Connection
If you have a ClusterXL gateway cluster, connect each cluster member to both ISPs via a LAN using two interfaces, as in FIGURE 5-6.
Configure ClusterXL in the usual way. Note however that the member interfaces must
be on the same subnet as the cluster external interfaces. For details, see the ClusterXL
guide.

**FIGURE 5-6** Both ISP links are LANs connected to a Gateway cluster

ISP Redundancy and VPNs

When ISP Redundancy is configured on the VPN-1 Pro gateway, VPN (that is,
encrypted) connections will survive a failure of one of the ISP links on the gateway. ISP
Redundancy works with both gateway to gateway VPNs and
SecuRemote/SecureClient Remote Access VPNs.

For configuration details, see “Configuring a VPN Gateway for ISP Redundancy” on
page 106.

The following section explains how ISP redundancy works with encrypted connections,
and how incoming and outgoing VPN traffic is handled by the ISP Redundancy
mechanism.
Outgoing encrypted traffic

In both High Availability and Load Sharing modes of ISP Redundancy, encrypted traffic is sent through the current default route specified in the routing table, unless a more specific route exists.

When an ISP link failure is detected, the default route is automatically changed by the `cpisp_update` script, and outgoing encrypted traffic is routed through the second link. If a specific route is used rather than the default route, the `cpisp_update` script must be manually changed so that in the event of a link failure, outgoing encrypted traffic is routed through the second link.

When the original link comes back up, traffic is again sent through the original route.

Incoming encrypted traffic

In gateway to gateway VPNs and in SecuRemote/SecureClient Remote Access VPNs, the remote peers use a mechanism called Dynamic IP Resolution to continuously probe the status of the ISP links on the enforcement module.

When the remote peers detect an ISP link failure they send all encrypted traffic to the second ISP link.

VPN peer gateways can be configured to encrypt with the ISP Redundancy gateway in one of two ways:

1. **First to Respond**, where the VPN peer sends encrypted traffic to the first interface to respond to the Dynamic Interface Resolution probes, and fails over to another interface if the first interface on the ISP Redundancy gateway becomes unavailable. This is the default mode. Remote Access VPN gateways can only work with the First to Respond mode.

2. **Primary Interface**, where the VPN peer sends encrypted traffic to a primary interface, and fails over to a second interface if the primary interface on the ISP Redundancy gateway becomes unavailable. Configuring a primary interface is useful if one of the VPN gateway interface is preferred. If both gateway interfaces are identical, there is no benefit to defining a primary interface.

ISP Redundancy and 3rd Party VPNs

The ability of a 3rd party VPN device to detect an ISP link failure depends on the 3rd party device implementation. A failure of an ISP link could lead to a VPN failure for two reasons:

1. The 3rd party device may not recognize incoming encrypted traffic from the secondary link as coming from the enforcement module.
2 The 3rd party device may be unable to detect an ISP link failure and may therefore keep encrypting traffic to the failed link.
Considerations for ISP Link Redundancy

Choosing the Deployment

The choice of deployment that best suits your own particular needs will usually be very clear:

- The simplest configuration is to use a different interface for each ISP link, as in FIGURE 5-3.
- If only one external interface is available on the VPN-1 Pro gateway, you can connect both ISPs to the same interface. This is done by defining two subnets, one for each ISP, on the same interface. Such a configuration is illustrated in FIGURE 5-4.
- If one of the ISP links is a dialup network (that is, a connection via a modem), to be used for backup, use the deployment in FIGURE 5-5, and choose the Primary/Backup mode of operation.
- If the ISP links are connected to a VPN-1 Pro gateway Cluster, use the deployment in FIGURE 5-6.

Choosing the Redundancy Mode

If both ISPs are essentially the same, use Load Sharing mode. That way you will be making best use of both ISPs.

You may prefer to use one of your two ISPs who may, for example be more cost-effective in terms of price and reliability. In that case, use Primary/Backup mode, and use the more cost-effective ISP for the Primary ISP link.
Configuring ISP Link Redundancy

In This Section

Introduction to ISP Link Redundancy Configuration
Registering the Domain and Obtaining IP Addresses
DNS Server Configuration for Incoming Connections
Dialup Link Setup for Incoming Connections
SmartDashboard Configuration
Configuring the Default Route for the ISP Redundancy Gateway
Configuring a VPN Gateway for ISP Redundancy
Example DNS Server Configuration Script

Introduction to ISP Link Redundancy Configuration

The following configuration allows outgoing connections from behind the VPN-1 Pro gateway, towards the Internet, and for incoming connections from the Internet to the networks behind the VPN-1 Pro gateway.

If the gateway configured for ISP Redundancy is part of a VPN community, you must perform the additional configuration steps described in “Configuring a VPN Gateway for ISP Redundancy” on page 106.

Note · For advanced configuration options see SecureKnowledge solution sk23630 at http://support.checkpoint.com/kb/ (username and password required).

In the configuration explanations, the subnets 192.168.1.0/24 and 172.16.2.0/24 represent public routable addresses.

Registering the Domain and Obtaining IP Addresses

The VPN-1 Pro gateway or a DNS server behind it must respond to DNS queries and resolve IP addresses that belong to publicly accessible servers in the DMZ (or other internal network). It is not necessary to have an actual DNS server, because the VPN-1 Pro gateway will intercept the DNS queries if configured to do so.

1 Obtain one routable IP address from each ISP for the DNS server or for the VPN-1 Pro gateway that will intercept DNS queries. Alternatively, if routable IP addresses are not available, make the DNS server accessible from the Internet using manual NAT, as described in step 23, below.

2 Register your domain (e.g. example.com) with both ISPs.
3 Inform the ISPs of the two addresses of the DNS server that will respond to DNS queries about the domain example.com.

4 To allow incoming connections, obtain one routable IP address from each ISP for each application server that is to be accessed from the Internet. For example, in FIGURE 5-2, obtain two IP addresses for the web server in DMZ-net. Alternatively, it is possible to avoid using routable IP addresses for the publicly available servers, as described in step 23, below.

DNS Server Configuration for Incoming Connections

The following procedure configures VPN-1 Pro to:

- Intercept DNS queries about www.example.com that arrive at the VPN-1 Pro external interfaces, and
- Respond to them with 192.168.1.2 and 172.16.2.2 (as in FIGURE 5-2 on page 93).

Proceed as follows:

5 Use GuiDBedit (located in the SmartConsole installation directory) to edit the Gateway object. Change the property misp_dns_active from false to true.

6 VPN-1 Pro responds to DNS queries with either one or two IP addresses, depending on the status of the ISP link and on the Redundancy mode. To configure this behavior, map each server name to an IP address pair. Using GuiDBedit go to the Gateway object, find the property misp_dns_entries, and populate it with entries. Each entry consists of:

- misp_host_name, to which you must add a host name (such as www.example.com).
- misp_dns_addresses, to which you must add two IP addresses (such as 192.168.1.2 and 172.16.2.2 in FIGURE 5-2 on page 93).

Give the index value 0 to the IP address that is associated with the first ISP link in the SmartDashboard ISP Redundancy page (such as ISP_A shown in FIGURE 5-7), and index value 1 to the IP address associate with the second ISP link.

Note • The length of each host name must not exceed 62 characters.
This process can be automated using a `dbedit` script. See “Example DNS Server Configuration Script” on page 107.

7 It is important to ensure that DNS servers in the Internet do not store out-of-date address information. Each DNS reply has a Time To Live (TTL) field which indicates to the recipients of the reply how long the information in the reply may be cached. By default, VPN-1 Pro replies with a TTL of 15 seconds. This can be changed by using `dbedit` or `GuiDBedit` to change the value (in seconds) of `misp_dns_ttl`.

**Dialup Link Setup for Incoming Connections**

8 If one of the ISP links is a dialup network, edit the ISP Redundancy Script located in `$FWDIR/bin/cpisr_update`. In the script, use the Linux or SecurePlatform operating system command to bring up or to take down the dialup interface.

9 You can connect SecurePlatform to ISPs that provide xDSL services using PPPoE or PPTP xDSL modems. If using one of these connections, then in the PPPoE or PPTP configuration of SecurePlatform, uncheck **Use Peer Gateway**.

**SmartDashboard Configuration**

10 Define a Security Rule Base rule that accepts DNS traffic through the VPN-1 Pro gateway. Use the `domain_udp` service.

11 In the **Check Point Gateway** window, **Topology** page, define the VPN-1 Pro interfaces leading to the ISPs.

12 In the **Topology > ISP Redundancy** page, check **Support ISP Redundancy**.

13 Perform either **Automatic ISP Link Configuration** or **Manual ISP Link Configuration**. Automatic configuration will only work if there are exactly two external interfaces defined in the **Topology** page, and is not possible for a Gateway Cluster object.
Configuring ISP Link Redundancy

Automatic ISP Link Configuration

14 Click Automatic ISP Links configuration. This configures the ISP links based on information taken from the routing table of the enforcement module, and from the Topology page of the enforcement module object.

15 To work in Primary/Backup mode:

   1 In the Redundancy Mode section, select Primary/Backup.
   
   2 Select and Edit the link you wish to be primary. In the ISP Link Properties window, General tab, check Primary ISP.

16 Examine the automatically configured ISP Links configuration for correctness.

17 Continue with step 20.

Manual ISP Link Configuration

18 In the Redundancy Mode section, select Load Sharing or Primary/Backup.

19 Define two ISP links. For each ISP link, click Add. In the ISP Link Properties window, General tab:

   1 Give the ISP link a Name, and choose the Interface leading to the ISP.
   
   2 Specify the Next Hop IP Address by clicking Get from routing table. If the ISP link is a dialup connection, leave the Next Hop IP Address field blank.
   
   In the example of FIGURE 5-3 on page 95, the next hop router on the way to ISP A has IP address 192.168.1.1, and the next hop router on the way to ISP B has IP address 172.16.2.1.

   3 In Primary/Backup mode, define whether the ISP link is Primary.

20 If you wish, define a list of hosts to be monitored in order to verify that the link is operational. To specify those hosts, move to the Advanced tab of the ISP Link Properties window, and Add the desired hosts to the list of Selected hosts.

21 Define Tracking. Choose an option for both ISP failure and ISP recovery.

Allowing Incoming and Outgoing Connections

22 To allow outgoing connections via both ISP links, define automatic Hide NAT on network objects that initiate the outgoing connections.

For example, in FIGURE 5-2 on page 93, edit the internal_net object. In the Network Properties window General tab, check Add Automatic Address Translation Rules, select Translation Method Hide, and choose Hide behind Gateway.
To allow incoming connections via both ISP links, to the application servers and the DNS server, define manual Static NAT rules.

If you have only one routable IP address from each ISP, and those addresses belong to the VPN-1 Pro gateway, you can allow specific services to reach specific servers. Using FIGURE 5-2 on page 93 as an example, define NAT rules as in TABLE 5-2. Incoming HTTP connections from both ISPs reach the web server www.example.com, and DNS traffic from both ISPs reaches the DNS server.

TABLE 5-2 Manual Static Rules for a Web Server and a DNS Server

<table>
<thead>
<tr>
<th>Original</th>
<th>Translated</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Destination</td>
<td>Service</td>
</tr>
<tr>
<td>Any</td>
<td>192.168.1.2</td>
<td>http = 10.0.0.2 (Static)</td>
</tr>
<tr>
<td>Any</td>
<td>172.16.2.2</td>
<td>http = 10.0.0.2 (Static)</td>
</tr>
<tr>
<td>Any</td>
<td>192.168.1.2</td>
<td>domain _udp = 10.0.0.3 (Static)</td>
</tr>
<tr>
<td>Any</td>
<td>172.16.2.2</td>
<td>domain _udp = 10.0.0.3 (Static)</td>
</tr>
</tbody>
</table>

If you have a routable address from each ISP for each publicly reachable server (in addition to the addresses that belong to the VPN-1 Pro gateway), you can allow any services to reach all the application servers. Give each server a non-routable address, and in the NAT Rule Base in TABLE 5-2:

- Use the routable addresses in the Original Destination.
- Use the non-routable address in the Translated Destination.
- For Original Service, use Any.

Note: If using Manual NAT, automatic arp won't work for the NATed addresses. You may need to implement SecureKnowledge solution sk8022.

Save and install the Security Policy.

Configuring the Default Route for the ISP Redundancy Gateway

Configure the ISP Redundancy gateway machine to have only a single default route. Do not give it any metric.
When working in a Primary/Backup mode, set the IP address of the router leading to the primary ISP as the default route.

When working in Load Sharing mode, use the router of the first ISP link in the **Check Point Gateway > Topology > ISP Redundancy** window as the default route. When an ISP link fails, the default route of the gateway is automatically changed by means of the ISP Redundancy script. When the link goes up again, the original default route will be reinstated.

**Configuring a VPN Gateway for ISP Redundancy**

For a detailed explanation of how ISP Redundancy works with VPNs, see “ISP Redundancy and VPNs” on page 97.

To allow a VPN-1 Pro gateway that is configured for ISP Redundancy to act as a VPN peer, you need to configure the VPN-1 Pro gateway for Dynamic IP resolution, that is, continuous RDP probing of its interfaces by remote peers. The VPN tunnel is set up through the interface which responds.

The configuration details depend on whether the VPN-1 Pro gateway is used for Site to Site VPNs, or whether it is used for Remote Access VPNs. If it is used for both Site to Site and Remote Access VPNs, perform both procedures.

**If the VPN-1 Pro Gateway is Used for Site to Site VPNs**

26 From the main menu, select **Policy > Global Properties**. In the **VPN > Advanced** page, **Resolving mechanism** section, select **Enable dynamic interface resolving per gateway (must be defined per gateway)**.

27 Edit the VPN-1 Pro gateway object. In the **Check Point Gateway** window, **VPN > VPN Advanced** page click **Dynamic Interface resolving configuration…**. The **Dynamic Interface resolving configuration** window opens.

28 Select **Enable dynamic resolution by peer VPN-1 gateways**.

29 Select **Upon fail-over event**. With this option, the status of all the Gateway’s interfaces are constantly polled. If an interface goes down, the connection moves to another interface.

**Configuring a Primary interface to which Site to Site VPN peers Should Encrypt**

If one of the gateway interface is preferred, configure a primary IP address on the VPN gateway to which VPN peers should encrypt. If both gateway interfaces are identical, there is no benefit to configuring a primary interface.
30 Using the Database Tool (dbedit) or the Graphical Database Tool (GuiDbEdit), set the property `interface_resolving_ha_primary_if_GW` on the VPN gateway object, to the IP address of the preferred interface.

**If the VPN-1 Pro Gateway is Used for Remote Access VPNs**

31 From the main menu, select **Policy > Global Properties**. In the **Remote Access > VPN > Advanced** page, **Resolving mechanism** section, select **Enable dynamic interface resolving by SecuRemote/SecureClient peers (must be defined per gateway)**.

32 Edit the VPN-1 Pro gateway object. In the **Check Point Gateway** window, **VPN > VPN Advanced** page click **Dynamic Interface resolving configuration...**. The **Dynamic Interface resolving configuration** window opens.

33 Select **Enable dynamic resolution by SecuRemote/SecureClient**.

34 Select **Upon every connection initialization**. With this option, the status of all the Gateway’s interfaces are constantly polled. If an interfaces goes down, the current connection is lost but subsequent connections go through a different interface.

**Example DNS Server Configuration Script**

The following is an example script for configuring the VPN-1 Pro mini-DNS server. It uses dbedit commands to automate the process described in “DNS Server Configuration for Incoming Connections” on page 102. After executing the script, the VPN-1 Pro gateway `corporate-gw` will be able to reply to DNS queries for the IP addresses of `www.example.com` and `ftp.example.com`.

- `www.example.com` will be resolved to 192.168.1.80 and 172.16.2.80.
- `ftp.example.com` will be resolved to 192.168.1.21 and 172.16.2.21.
To execute the dbedit script, run

```
dbedit -s <SmartCenter> -u <user> -p <password> -f <script_name>
```

### TABLE 5-3 dbedit script arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartCenter</td>
<td>Name of the SmartCenter Server.</td>
</tr>
<tr>
<td>user</td>
<td>SmartDashboard Administrator user name.</td>
</tr>
<tr>
<td>password</td>
<td>SmartDashboard Administrator password.</td>
</tr>
<tr>
<td>script_name</td>
<td>Name of the dbedit script.</td>
</tr>
</tbody>
</table>

**Note**: Make sure the lines are not broken over two lines. Blank lines are not allowed.

### CODE EXAMPLE 5-1 Example dbedit script

```bash
# Start of dbedit script
# Activate the DNS feature
modify network_objects corporate-gw firewall_setting::misp_dns_active true
# Add the first entry (www.example.com, 192.168.1.80, 172.16.2.80)
create misp_dns_entry tmp_name
modify owned tmp_name misp_host_name www.example.com
addelement owned tmp_name misp_dns_addresses 192.168.1.80
addelement owned tmp_name misp_dns_addresses 172.16.2.80
add owned remove name network_Objects corporate-gw firewall_setting::misp_dns_entries owned:tmp_name
delete owned tmp_name
# Add the second entry (ftp.example.com, 192.168.1.21, 172.16.2.21)
create misp_dns_entry tmp_name
modify owned tmp_name misp_host_name ftp.example.com
addelement owned tmp_name misp_dns_addresses 192.168.1.21
addelement owned tmp_name misp_dns_addresses 172.16.2.21
add owned remove name network_Objects corporate-gw firewall_setting::misp_dns_entries owned:tmp_name
delete owned tmp_name
# Update the object
update network_objects corporate-gw
quit
```

# end of dbedit script

# end of dbedit script
In This Chapter

The Need for Server Load Balancing  page 109
The ConnectControl Solution for Server Load Balancing page 110
Configuring ConnectControl page 117

The Need for Server Load Balancing

While Check Point offers optimal performance for single server deployment, there are several disadvantages to relying on a single server to host an application. While a server's capabilities can often be expanded with additional processors and RAM, in many cases a lone machine cannot handle the traffic volume, which results in poor response times and connection timeouts. Additionally, server maintenance and other unplanned downtime are problematic in a single server environment. Sharing network traffic intelligently among multiple servers can shorten response times and reduce the risk to the application by any one machine failure.
The ConnectControl Solution for Server Load Balancing

In This Section

- Introduction to ConnectControl  page 110
- Load Balancing Methods  page 110
- ConnectControl Packet Flow  page 111
- Logical Server Types  page 112
- Persistent Server Mode  page 114
- Server Availability  page 116
- Load Measuring  page 116

Introduction to ConnectControl

ConnectControl is Check Point’s solution for server load balancing. It allows you to distribute network traffic among a number of servers, which reduces the load on a single machine, improves network response time, and provides high availability. Beside the performance benefits of this feature, spreading the load over multiple machines creates redundancy for your application, thus reducing the risk of downtime.

Load-balanced servers are represented by a single virtual IP address. Clients are thus unaware that more than one server may be serving their requests. This is accomplished using a Logical Server, a network object defined in SmartDashboard that represents a of physical servers. The Logical Server fields service requests for the load-balanced application and directs them to the appropriate physical server.

ConnectControl runs on the enforcement points and does not impose any additional memory or processing requirements. It continuously checks the availability of each server. If a server fails, or is unreachable, ConnectControl stops directing connections to that server until it becomes available.

Load Balancing Methods

ConnectControl not only spreads out the network traffic to your load-balanced servers; it also allows you to distribute that traffic according to predefined balancing methods. There are five available methods from which to choose:

- **Server Load** measures the load on each server to determine which has the most available resources to service a request. Each server in the group runs a load measuring agent that automatically reports the current system load to the ConnectControl module on the VPN-1 Pro Gateway. Server Load may be a good
choice for your environment if your servers are running other demanding applications in addition to supporting your load-balanced application. See “Load Measuring” on page 116 for more details.

- **Round Trip** ensures that incoming requests are handled by the server with the fastest response time. ConnectControl ascertains the response times of the servers in the group at a user-defined interval, whereupon the enforcement module executes a series of ICMP echo requests (pings) and reports the server with the shortest average round trip time. ConnectControl then directs the service request to that server. The round trip method may be a good choice if there are large variations in the traffic load on your network, or when load balancing over WAN connections.

- **Round Robin** assigns service requests to the next server in the sequence. The round robin method provides optimal load balancing when the load-balanced servers all have similar RAM, CPU, and are located on the same segment.

- **Random** assigns service requests to servers at random. The random method provides optimal load balancing when the load-balanced servers all have similar RAM, CPU, and are located on the same segment.

- **Domain** directs service requests based on domain name.

**ConnectControl Packet Flow**

When a client requests access to an application load-balanced by ConnectControl, the packet flow is as follows (the following steps correspond with FIGURE 6-1):

1. A client initiates a connection with the logical IP address of the application server, which is in actuality the address assigned to the Logical Server.

2. The service request arrives at the gateway, and is matched by the Logical Server rule in the Rule Base. VPN-1 Pro directs the packet to the Logical Server.

3. ConnectControl determines which of the servers in the group will fulfill the request based on the load balancing method.
Logical Server Types

When creating the Logical Server object, you must identify the server type as either HTTP or Other. This distinction is meaningful, as ConnectControl handles the connection to the client differently for each server type. To direct network traffic, server type HTTP uses HTTP redirection, while server type Other uses address translation.

HTTP

The Logical Server of type HTTP employs HTTP redirection as its method of distributing network traffic, and as such supports only HTTP services. The redirection mechanism ensures that all sessions comprising an HTTP connection are directed to a single server. This is vital for many Web applications, such as those using HTTP-based forms, which require that a single server process all user data.

The HTTP redirection mechanism works in conjunction with ConnectControl’s load balancing methods. The initial HTTP connection is directed to the proper server based on the chosen load balancing method. ConnectControl then notifies the client that subsequent connections should be directed to the IP address of the selected physical server rather than the IP address of the Logical Server. The IP address can be that of a server behind the firewall, or offsite. The remainder of the session is conducted without ConnectControl intervention. All operations are transparent to end-users.

The Logical Server may direct the client to an HTTP server behind the firewall, or to an offsite HTTP server, depending on the result of ConnectControl’s load balancing. FIGURE 6-2 depicts a connection being directed to an offsite server.
All further communication between the client and the server take place without the intervention of ConnectControl.

**Other**

The Logical Server of type **Other** can be used for all services supported by VPN-1 Pro, including HTTP. It uses address translation to direct network traffic to the grouped servers. ConnectControl mediates each service request, even when clients continue a session. When you create a Logical Server of type **Other**, ConnectControl allows the connection by automatically placing entries in VPN-1 Pro’s kernel table. ConnectControl determines which server will receive the request, and uses NAT to modify the destination IP address of the incoming packet. If a return connection is opened, the connection is automatically established between the server and the client, and the server's source address in the packet is translated to that of the Logical Server. **FIGURE 6-3** depicts a connection being directed to a NATed FTP server inside the firewall.
On the packet’s return journey, the firewall translates the packet’s origin address to that of the Logical Server.

You can use a Logical Server of type **Other** to handle HTTP service requests as well. In contrast to type **HTTP**, once a connection between client and server has been established, the Logical Server of type **Other** does not disconnect from the conversation. Instead ConnectControl handles each HTTP service request from the client, and multiple service requests from one client may be directed to different servers.

**Considering Logical Server Types**

In considering the proper implementation for your environment, there are three decisive criteria: use of HTTP forms, server location, and servers configured for NAT. Type **HTTP** supports offsite HTTP servers and form-based applications, but works only with the HTTP protocol. Type **Other** supports all protocols and may provide the most accurately balanced load, but requires servers to be NATed by the gateway.

**Persistent Server Mode**

Persistent server mode is a ConnectControl feature that maintains a client’s connection to the server to which it was first directed (see “Persistent Server Timeout” on page 115 for more on length of persistent sessions). You must choose whether the persistency is by server or by service.
Persistency By Server
Persistency by server is useful for certain types of HTTP applications, such as forms support. For example, consider a load-balanced environment of three web servers, as illustrated in FIGURE 6-4. With Persistency by server enabled, ConnectControl directs an HTTP client to a specific server, and each subsequent request by the client is directed to that same server. This mode allows clients to fill out forms without the data loss that would occur if separate service requests were directed to different servers. If you are supporting forms, make sure Persistent server mode is enabled (the default setting) and Persistency by server is set as well.

Persistency By Service
Persistency by service is useful if you are load balancing multiple services in your server group. For example, consider a redundant environment of two machines, each running HTTP and FTP.

FIGURE 6-4 Example of Persistency by Service

With persistency by service, the client can be directed to one server for HTTP services, and another for FTP services. This provides the benefit of not becoming locked in to a server under a heavy load, as you might be if you were running persistency by server in this configuration. Thus ConnectControl allows you to configure Persistency by service, which directs previously load-balanced clients who request a different service to be load-balanced and directed to the appropriate server again.

Persistent Server Timeout
One aspect of Persistency is configured on the ConnectControl page of the Global Properties window. The Persistent server timeout sets the amount of time that a client, once directed to a particular server, will continue to be directed to that same server. In
the event that a server becomes unavailable, new connections will be directed to an available server even if persistent server mode is enabled. If you desire the optimal load balance among your servers, uncheck **Persistent server mode**, and all of your application’s traffic will be distributed according to the load balance method.

**Server Availability**

ConnectControl allows you to configure aspects of its system to check the availability of servers in the Logical Server group. You can control how often the module pings the servers to make sure they are still active. You can also configure the number of attempts it will make to contact a non-responsive server, after which ConnectControl stops directing connections to it.

These settings are located on the **ConnectControl** page of the **Global Properties** window. **Server availability check interval** sets how often the servers are pinged, and **Server check retries** sets the number of attempts to contact non-responsive servers.

**Load Measuring**

The server load balancing method is unique in that it requires a special load measuring agent to run on each server in the group. The agent is lightweight and does not add additional latency or system overhead to the server. It uses the UDP transport protocol to support communication between the load measuring agent and the ConnectControl module. Check Point provides a sample load measuring agent application for installation on servers, as well as a load measuring application programming interface (API) for organizations who wish to write their own agents. You can download the load agent application for your OS from SecureKnowledge at: [https://support.checkpoint.com/login/login.jsp](https://support.checkpoint.com/login/login.jsp). Sign in with your User Center email and password, and enter the SecureKnowledge ID 47.0.1569467.2530820.

You can configure certain aspects of the load measuring agent on the **ConnectControl** page of the **Global Properties** window. The **Load agents port** property specifies the port the load agent uses to communicate with VPN-1 Pro. All the load measuring agents in a configuration must use the same port number. The **Load measurement interval** property sets the interval at which the agent returns information about the server’s load to the firewall. The default is every 20 seconds.

For Windows servers, configure and enable the load agent with the syntax:

```
load_agent_nt <port_number> <load_value>.
```

The default port used by ConnectControl for version NG is 18212. The values for **load_value** are 0, 1, 2, where:

* 0 measures the load over a 1 minute interval
* 1 measures the load over a 5 minute interval
• 2 measures the load over a 15 minute interval

**Configuring ConnectControl**

**Create Network Objects for the Application Servers**

1. In SmartDashboard, right click on Network Objects in the Network Objects tree, and select New > Node > Host.

2. Define a server object that represents a server that will be load-balanced.

3. Repeat step 2 for each server you place in the group.

**Create a Network Group Object to Group the Application Servers**

4. In SmartCenter, right click on Network Objects, and select New > Group > Simple Group.

5. Name the group (ex. HTTP_Server_Group).

6. Add the server objects to the group in the Group Properties box. It is recommended to add no more than 29 Logical Servers to a group.

**Create a Logical Server Object to Pool the Application Servers**

7. In SmartDashboard, right click on Network Objects in the Network Objects tree, and select New > Logical Server. Make sure the IP address you assign is a routable IP address. All traffic to be load-balanced should be directed through the gateway.

8. Select the Server's Type.

9. In Servers Group, add the Group Object you created in step 3.

10. If you intend to use persistent server mode, select Persistency by service or server. The default mode is Persistency by service. Deselect Persistent server mode if you don’t want to use it.


12. Add the following rule to the Rule Base:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Logical_Server</td>
<td>[load-balanced service(s)]</td>
<td>Accept or User Auth or Client Auth or Session Auth</td>
</tr>
</tbody>
</table>
For applications using HTTP redirection (Logical Server of type HTTP), add a second rule to allow the physical server group to communicate directly with clients after sessions are started:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>HTTP_Server_Group</td>
<td>http</td>
<td>Accept</td>
</tr>
</tbody>
</table>

**Configure ConnectControl Global Properties**

13 In the **Policy** menu, choose **Global Properties** > **ConnectControl**. Review the default settings and adjust according to your implementation.

- **Servers Availability** settings manage how often ConnectControl checks to make sure the load balanced servers are running and responding to service requests, and how many times ConnectControl attempts to contact a server before ceasing to direct traffic to it.
  - **Server availability check interval**: default is 20 seconds
  - **Server check retries**: default is 3 times.

- **Servers Persistency** sets the amount of time that a client, once directed to a particular server, will continue to be directed to that same server.
  - **Persistent server timeout**: default is 1800 seconds

- **Servers Load Balancing** settings manage how often the load measuring agents (if employed) report their load status to ConnectControl, and on what port they communicate with ConnectControl.
  - **Load agents port**: default is 18212
  - **Load measurement interval**: default is 20 seconds
Section 3: SmartDefense

This chapter gives a conceptual overview of SmartDefense, which enables customers to configure, enforce and update network and application attack defenses. The DShield StormCenter is also described in detail. For information about specific protections, see the SmartDefense HTML pages and the online configuration help.
CHAPTER 7

SmartDefense

In This Chapter

Need for Active Defense page 121
The SmartDefense Solution for Active Defense page 122
Configuring SmartDefense page 132
SmartDefense StormCenter Module page 133

Need for Active Defense

The threats to network security are many, and they are evolving in sophistication as well as variety.

FIGURE 7-1 Network Attacks

Since access control devices like Check Point's VPN-1 Pro have prevented unauthorized traffic from passing through the gateway, hackers are now focusing their efforts on the misuse of allowed traffic and services. Some of the most serious threats in today's Internet environment come from attacks that attempt to exploit the application
layer. Of particular interest to hackers are services such as HTTP (TCP port 80) and HTTPS (TCP port 443), which are commonly open in many networks. Access control devices cannot easily detect malicious attacks aimed at these services.

Consider the following two examples of Denial of Service (DoS) attacks. Let’s say that you have decided to allow ICMP requests (pings) on your network. A DoS attack may exploit this to flood your network with pings, thereby preventing other connections. Without a defense that automatically detects and prevents this attack, your only recourse may be to disallow pinging, certainly not an ideal solution. But what do you do when a DoS attack exploits the protocol you use to communicate on the Internet? That’s what happens with a SYN attack, which disrupts TCP/IP traffic by sending SYN packets and then not acknowledging the TCP/IP server’s response packet. This causes the server to keep signaling until it eventually times out, a very effective attack. Certainly disabling TCP/IP is not an option.

Other solutions available, such as content security applications like virus scanners, are important, but inadequate for this purpose. While they do inspect the content of individual packets, content security applications are limited to specific services, and are unable to detect patterns of malicious activity.

Securing the network with the most up-to-date methods of detecting and preventing attacks is critical for safeguarding data and communications. The only solution that addresses these types of threats is an active, intelligent, and reliably up-to-date defense. The following section details Check Point’s solution to the mutating nature of attacks on the perimeter of the network.

The SmartDefense Solution for Active Defense

In This Section

Introduction to SmartDefense  
Application Intelligence-Defending Against the Next Generation of Threats  
Network and Transport Layers: Necessary for Application Intelligence  
SmartDefense Subscription Service  
How SmartDefense Works  
Categorizing SmartDefense Capabilities  
The SmartDefense Tree Structure
Introduction to SmartDefense

Check Point SmartDefense provides a unified security framework for various components that identify and prevent attacks. SmartDefense actively defends your network, even when the protection is not explicitly defined in the Security Rule Base. It unobtrusively analyzes activity across your network, tracking potentially threatening events and optionally sending notifications. It protects organizations from all known, and most unknown, network attacks using intelligent security technology.

Keeping up-to-date with the latest defenses does not require up-to-the-minute technical knowledge. A single click updates SmartDefense with all the latest defenses from the SmartDefense website.

SmartDefense provides a console that can be used to:

- Choose the attacks that you wish to defend against, and read detailed information about the attack.
- Easily configure parameters for each attack, including logging options.
- Receive real-time information on attacks, and update SmartDefense with new capabilities.

Application Intelligence—Defending Against the Next Generation of Threats

A growing number of attacks attempt to exploit vulnerabilities in network applications rather than target the firewall directly. Check Point Application Intelligence is a set of advanced capabilities, integrated into VPN-1 Pro and SmartDefense, which detects and prevents application-level attacks. Based on INSPECT intelligent inspection technology, Check Point Application Intelligence gives SmartDefense the ability to protect against application attacks and hazards.

FIGURE 7-2 OSI (Open Systems Interconnection) Reference Model
Network and Transport Layers: Necessary for Application Intelligence

Application Intelligence is primarily associated with application level defenses. However, in practice many attacks aimed at network applications actually target the network and transport layers.

Hackers target these lower layers as a means to access the application layer, and ultimately the application and data itself. Also, by targeting lower layers, attacks can interrupt or deny service to legitimate users and applications (e.g., DoS attacks). For these reasons, SmartDefense addresses not only the application layer, but also network and transport layers.

Preventing malicious manipulation of network-layer protocols (e.g., IP, ICMP) is a crucial requirement for multi-level security gateways. The most common vehicle for attacks against the network layer is the Internet Protocol (IP), whose set of services resides within this layer.

As with the network layer, the transport layer and its common protocols (TCP, UDP) provide popular access points for attacks on applications and their data.

SmartDefense Subscription Service

SmartDefense functionality is freely included with VPN-1 Pro. However, subscribing customers can automatically update SmartDefense and Web Intelligence with a single click. Customers who purchase a SmartDefense subscription service can obtain the following updates as soon as they are released, from the Check Point SmartDefense site http://www.checkpoint.com/techsupport/documentation/smartdefense/index.html

1  HTTP and CIFS worm patterns.
2  INSPECT file updates.
3  Dynamic Attack protection.
Customers with a valid subscription license also receive special SmartDefense Advisories that provide updated SmartDefense and Web Intelligence attack protections, as well as information, tools and best practice methods to mitigate different attacks.

Note: SmartDefense is integrated with Check Point gateways of version NG FP2 and higher. Previous versions do not receive the SmartDefense configurations. It is recommended to keep your gateway version up-to-date, as the newest defenses are incorporated into only the latest version of Check Point software.

How SmartDefense Works

SmartDefense is integrated with all VPN-1 Pro versions of NG FP2 and higher. As all inbound traffic is routed through the firewall, this is the natural place for active defense to reside. Some of SmartDefense’s capabilities are enforced on the network boundary, while others, such as Abnormal Behavior Analysis, are directed from the SmartCenter Server. The SmartDefense protections that you enable are distributed as part of the Security Policy to each enforcement point from the SmartCenter Server. SmartDefense blocks attacks at the network boundary using Check Point’s Stateful Inspection technology.

Categorizing SmartDefense Capabilities

Check Point SmartDefense protects organizations against attacks and other non-legitimate or undesired network activity. Its capabilities can be categorized as follows:

- Defense against attacks page 125.
- Information Disclosure Prevention page 126.
- Abnormal Behavior Analysis page 126.

Some SmartDefense features provide more than one category of capability. The Initial Sequence Number Defender (ISN Defender) for example, provides both defense against a specific attack, and Implicit Defense.

Defense against attacks

Check Point SmartDefense protects organizations from known and unknown network attacks. Attacks are stopped at the gateway, and are prevented from affecting the target server.

SmartDefense is easy to configure, and defends against attacks while freeing the administrator from the need to understand the technical details of the attack.

SmartDefense features protection against the following types of attack:

- Denial of Service Attacks
- TCP/IP Attacks
The SmartDefense Solution for Active Defense

• Web and Application Vulnerabilities
• Network Probing
• HTTP Worms

For example, consider a type of TCP/IP attack called ISN Guessing. TCP/IP connections are initiated by way of a three-way handshake. The client sends a SYN packet, the server replies with a SYN/ACK, and the client sends an ACK packet to acknowledge the connection. With each SYN/ACK, the server also generates an initial sequence number (ISN or SN) that identifies the connection.

The SNs are generated using a key of some sort, and for some operating systems it is possible to guess the next SN from the previous SN. If an external client can successfully guess the next valid SN, it can then open a connection to the server by sending a SYN/ACK packet with a valid SN. This connection could be from a non-existent IP address, and may carry damaging data.

SmartDefense fends off this sort of attack by replacing the server as the SN generator, and uses an encrypted key to generate SNs much less susceptible to attack.

Information Disclosure Prevention
Implicit Defense prevents information about network entities from reaching the Internet, where this information could be misused.

To return to our SN vulnerability example, when an internal server establishes a TCP connection, it sends successive SNs. In certain conditions, these SNs can be used to identify the source’s operating system. SmartDefense uses “fingerprint spoofing” to replace this fingerprint with another, thereby making it impossible for external clients to discover the operating system used by the internal servers.

Abnormal Behavior Analysis
SmartDefense provides reporting and analysis of patterns of network behavior. It detects these patterns by analyzing logs sent to the SmartCenter by the VPN-1 Pro enforcement modules. If a suspicious pattern is detected, the administrator can track the activity via a log or other kind of alert, depending on the configuration setting.

The Port Scan detection feature is an example of abnormal behavior analysis. When enabled, SmartDefense senses when its ports are being scanned, logs the activity and can be configured to issue an alert.
The SmartDefense Tree Structure

The SmartDefense console is divided into a tree structure that classifies the defenses provided by SmartDefense. The following summarizes the major categories in the tree.

**Note** - When updating SmartDefense, new categories, as well as attack defenses, may be added to the tree structure.

**General**

This page allows you to easily update SmartDefense with the latest information on new and emerging attacks (provided you participate in the subscription program).

**Anti-Spoofing Configuration Status**

This page indicates how anti-spoofing is configured on the gateways. It identifies any Check Point gateways on which anti-spoofing is not enabled, i.e., the attribute **IP address behind this interface** of the offending gateway is configured as **Not Defined**. You can change the settings by reconfiguring the individual gateways.

For more information, see the SmartDefense HTML pages and online help.

**Network Security**

These pages allow you to configure various SmartDefense protections against attacks on the network and transport level. The effect of such attacks, on the IP, TCP, UDP or ICMP network protocols, range from simple identification of the operating systems used in your organization, to denial of service attacks on hosts and servers on the network.

**Denial of Service**

Denial of Service (DoS) attacks are aimed at overwhelming the target with spurious data to the point where it is no longer able to respond to legitimate service requests. The attacks in this section exploit operating system bugs to remotely crash machines.

For more information, see the SmartDefense HTML pages and online help.

**IP and ICMP**

This page allows you to enable a comprehensive sequence of layer 3 tests (IP and ICMP protocols).

For example, the fragmentation timeout logs feature generates logs when detecting packets purposefully fragmented for a Firewall bypassing or Denial of Service attack.

For more information, see the SmartDefense HTML pages and online help.
TCP

VPN-1 Pro 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 TCP packets are legitimate, the following tests are conducted:
- protocol type verification
- protocol header analysis
- protocol flags analysis and verification

SYN Attack Protection prevents attacks in which TCP connection initiation packets are sent to the server in an attempt to cause Denial of Service.

The sequence verifier is a mechanism matching the current TCP packet’s sequence number against a TCP connection state. Packets that match the connection in terms of the TCP session but have incorrect sequence numbers are either dropped or stripped of data.

For more information, see the SmartDefense HTML pages and online help.

Fingerprint Scrambling

It is sometimes possible to identify the operating system used by a machine, or to impersonate an existing connection, by means of a fingerprint that characterizes the operating system or the connection. SmartDefense can prevent this by distorting the fingerprint to make such identification impossible.

For more information, see the SmartDefense HTML pages and online help.

Successive Events

Successive Events detection provides a mechanism for detecting malicious or suspicious events and notifying the security administrator.

Successive Events detection runs on the SmartCenter Server and analyzes logs from VPN-1 Pro enforcement modules by matching log entries to attack profiles.

The security administrator can modify attack detection parameters, turn detection on or off for specific attacks, or disable the Successive Events feature entirely.

Logs which do not reach the SmartCenter Server (for example, local logs and logs sent to the Log Server) are not analyzed.

For more information, see the SmartDefense HTML pages and online help.
DShield Storm Center

Storm Centers gather logging information about attacks. This information is voluntarily provided by organizations from across the world for the benefit of all. Storm Centers collate and present reports on real-time threats to network security in a way that is immediately useful.

The SmartDefense Storm Center Module updates your organization with the latest attack information from the Storm Centers, and allows you to contribute your attack logs to their databases.

One of the leading Storm Centers is SANS DShield.org. Check Point SmartDefense integrates with the SANS DShield.org Storm Center in two ways:

- The DShield.org Storm Center produces a Block List report, which is a list of address ranges that are worth blocking. This Block List is frequently updated. The SmartDefense Storm Center Module retrieves and adds this list to the Security Policy in a way that makes every update immediately effective.
- You can decide to send logs to the Storm Center in order to help other organizations combat the threats that were directed at your own network. You can decide which logs to send by selecting the rules for which you want to send logs.

For more information about the SmartDefense DShield Storm Center integration, see “SmartDefense StormCenter Module” on page 133.

Port Scan

Port Scanning is a method of collecting information about open TCP and UDP ports in a network. Gathering information is not in itself an attack, but the information can be used later to target and attack vulnerable computers.

Port scanning can be performed either by a hacker using a scanning utility such as nmap, or by a worm trying to spread itself to other computers. Port Scanning is most commonly done by trying to access a port and waiting for a response. The response indicates whether or not the port is open.

Port numbers indicate a specific network service. Connecting to port 80 on the host www.example.com accesses the HTTP service. Other familiar services include FTP (port 21), Telnet (port 23), and DNS (port 53). TCP and UDP port numbers are listed in http://www.iana.org/assignments/port-numbers.

To offer a service to other computers, a host has to open a port for that service. Ports often remain open from a default installation, and the administrator may not know about them. This can leave the host vulnerable to attack. For example, if the FTP service is left open by default, an attacker can try to guess the default username and password in order to get access to the machine.
For more information, see the SmartDefense HTML pages and online help.

**Dynamic Ports**

A number of applications (such as FTP under heavy load, and SIP protocols) can set up connections by opening ports dynamically. These ports can turn out to be the same as those used by one of the pre-defined services in the SmartDashboard. Use this page to define whether to drop a connection with a dynamically opened port that is the same as a pre-defined service port. Also use this page to choose whether to drop dynamic port connections that use low ports (below 1024).

For more information, see the SmartDefense HTML pages and online help.

**Application Intelligence**

These pages allow you to configure various protections at the application layer, using SmartDefense's Application Intelligence capabilities.

**Mail**

The SMTP security server allows strict enforcement of the SMTP protocol. It protects against malicious mail messages, provides SMTP protocol centered security, prevents attempts to bypass the Rule Base using mail relays, and prevents Denial of Service and spam mail attacks. Usually the security server is activated by specifying resources or authentication rules in the Security Rule Base.

These pages allow you to select what types of enforcement will be applied to SMTP connections passing through the security server. Clicking **Configuration applies to all connections** will forward all SMTP connections to the SMTP security server and enforce the defined settings on all connections, without having to define a resource in the Rule Base. Clicking **Configurations apply only to connections related to rule base defined objects** applies these configurations only to SMTP connections for which a resource is defined in the Rule Base.

For more information, see the SmartDefense HTML pages and online help.

**FTP**

These pages allow you to configure various protections related to the FTP protocol. For example, preventing FTP port overflow checks foils any attempt to use an FTP server as an agent for a malicious operation.

For more information, see “FTP Security” on page 211, and also the SmartDefense HTML pages and online help.
Microsoft Networks

These pages allow you to configure various protections at the application layer, using SmartDefense's Application Intelligence capabilities.

For more information, see “Microsoft Networking Services (CIFS) Security” on page 209, and also the SmartDefense HTML pages and online help.

Peer to Peer

SmartDefense can block Peer to Peer traffic by identifying the proprietary protocols and preventing the initial connection to the Peer to Peer networks. This prevents not only downloads, but also search operations. SmartDefense can identify the protocol even if the peer to peer application switches port numbers. The detection does not, for example, rely on identifying HTTP header signatures.

For more information, see the SmartDefense HTML pages and online help.

Instant Messengers

These pages allow you to block Instant Messaging applications that use VoIP protocols. Instant Messaging applications have many capabilities, including voice calls, message transfer, and file sharing.

For more information, see “Securing Instant Messaging Applications” on page 203, and also the SmartDefense HTML pages and online help.

DNS

The DNS protocol is used to identify servers by their IP addresses and aliases. DNS protocol messages can be transported over TCP or UDP.

This option checks that all the connections on the DNS port over UDP are DNS-related. In addition, certain restrictions are imposed on the type of data allowed in queries and answers.

For more information, see the SmartDefense HTML pages and online help.

VoIP

Voice and video traffic, like any other information on the corporate IP network, has to be protected as it enters and leaves the organization. Possible threats to this traffic are

- Call redirections, where calls intended for the receiver are redirected to someone else.
- Stealing calls, where the caller pretends to be someone else.
- Systems hacking using ports opened for VoIP connections
VoIP calls involve a whole series of complex protocols, each of which can carry potentially threatening information through many ports.

SmartDefense makes sure that addresses of the caller and receiver are where they are claimed to be, and that the caller and receiver are allowed to make and receive VoIP calls. In addition, SmartDefense examines the contents of the packets passing through every allowed port, to make sure they contain proper information. Full stateful inspection on H.323, SIP, MGCP and SCCP commands ensures that all VoIP packets are structurally valid, and that they arrive in a valid sequence.

For more information, see “Securing Voice Over IP (VoIP)” on page 155.

**SNMP**

SmartDefense enables you to protect against SNMP vulnerabilities by providing the option of enforcing SNMPv3 (the latest SNMP version) while rejecting previous versions. In addition, SmartDefense can allow all SNMP versions while dropping requests with SNMPv1 and SNMPv2 default community strings. A monitor-only mode makes it possible to track unauthorized traffic without blocking it.

For more information, see the SmartDefense HTML pages and online help.

**Configuring SmartDefense**

Configuring SmartDefense is simple and intuitive. Proceed as follows:

1. In the SmartDashboard toolbar, click the SmartDefense icon.
2. In the **SmartDefense Settings** window, select the SmartDefense category to view information about the category. To view details of a specific attack, click [+] to expand the branch, and select the attack.
3. Check the attacks you wish to defend against, and configure **Settings** for the categories and the specific attacks.
4. Install the Security Policy. You need to reinstall the Security Policy in order to implement changes to the SmartDefense configuration.

**Updating SmartDefense with the Latest Defenses**

To obtain updates of all the latest defenses from the SmartDefense website, open the **SmartDefense Settings > General** page, and click **Update SmartDefense**.
The Need for Cooperation in Intrusion Detection

In This Section

- The Need for Cooperation in Intrusion Detection  page 133
- Check Point Solution for Storm Center Integration  page 134
- Planning Considerations  page 138
- Configuring Storm Center Integration  page 138

The Need for Cooperation in Intrusion Detection

The range and sophistication of the techniques used by hackers and crackers to penetrate private networks is increasing all the time. Very few organizations can hope to maintain up-to-the-minute protection against the latest attacks. Network Storm Centers are collaborative initiatives that have been set up to help the beleaguered Security Administrator fight back. Storm Centers gather logging information about attacks. This information is voluntarily provided by organizations from across the world for the benefit of all. Storm Centers collate and present report on real-time threats to network security in a way that is immediately useful.

FIGURE 7-3 Cooperation between organizations and the Storm Center
Check Point Solution for Storm Center Integration

In This Section

Introduction ............................................. page 134
How the Block List is Received ....................... page 135
How Logs are Submitted to the Storm Center ...... page 136
What a Submitted Log Contains ..................... page 136
Removing Identifying Information from the Submitted Log ........................................ page 137
How Authenticity is Assured ......................... page 137
Size of Logs and Effect on VPN-1 Pro Performance ........................................ page 138

Introduction

The SmartDefense Storm Center Module is included in the standard VPN-1 Pro product installation. It enables a two way information flow between the network Storm Centers and the organizations requiring network security information.

One of the leading Storm Centers is SANS DShield.org http://secure.dshield.org/. DShield.org gathers statistics and presents it as a series of reports at http://secure.dshield.org/reports.html.

Check Point SmartDefense integrates with the SANS DShield.org Storm Center in two ways, illustrated in FIGURE 7-4.

- The DShield.org Storm Center produces a Block List report, which is a list of address ranges that are worth blocking. This Block List is frequently updated. The SmartDefense Storm Center Module retrieves and adds this list to the Security Policy in a way that makes every update immediately effective.
- You can decide to send logs to the Storm Center in order to help other organizations combat the threats that were directed at your own network. You can decide which logs to send by selecting the Security rules and SmartDefense/Web Intelligence protections for which you want to send logs.
**How the Block List is Received**

The Security Administrator configures the SmartDefense option **Network Security > DShield Storm Center > Retrieve and Block Malicious IPs**. Malicious IP can be blocked for all gateways, or for specific gateways.

An agent (daemon) on each VPN-1 Pro Gateway for which malicious IP are to be blocked receives the Block List of malicious IP addresses from [http://secure.dshield.org/block_list_info.html](http://secure.dshield.org/block_list_info.html) via HTTPS. Every refresh interval (the default is three hours), the agent takes the Block List, and updates the Security Policy with the IP address ranges in the Block List. This process is logged in the SmartView Tracker, in the FireWall-1 log, as shown in **FIGURE 7-5**.
How Logs are Submitted to the Storm Center

The Security Administrator decides which type of logs should be submitted. For example, it is possible to specify that all logs of type Alert or User Defined Alert will be submitted. Logs of detected attacks (such as HTTP Worm patterns) can also be submitted.

A log submitting agent (daemon) on the SmartCenter Server generates two kinds of logs. As well as regular logs, a compact log digest is created. The digest includes only the number of Drops and Rejects per port.

The Storm Center tells the log submitting agent to send either regular logs, or digests, or both kinds of log.

The log submitting agent sends to the Storm Center the logs chosen by the Security Administrator, of the type requested by the Storm Center. Log submission is done using HTTPS POST. The logs are compressed into a database.

What a Submitted Log Contains

The logs that are submitted to the Storm Center contain the following information:

- Connection parameters: Source IP Address, Destination IP Address, Source Port, Destination Port (that is, the Service), IP protocol (such as UDP, TCP or ICMP).
- Rule Base Parameters: Time, action.
A detailed description of the log.

For HTTP Worm patterns, the log contains the same connection parameters, the same Rule Base parameters, and also the name of attack and the detected URL pattern.

Submitted logs are SmartDefense logs, as shown in FIGURE 7-6.

**FIGURE 7-6** Showing the submission of logs to the Storm Center in the SmartView Tracker

Removing Identifying Information from the Submitted Log

It is possible to delete identifying information from internal IP addresses in the submitted log, by specifying a designated number of bits to mask.

The mask can be used to delete as many bits as desired from the internal IP addresses. A zero bit mask obscures the whole of the IP address. A 32 bit mask reveals the whole of the internal IP address. An 8 bit mask reveals 8 valid bits, and converts an IP address such as 192.168.46.88 to 0.0.0.88.

**How Authenticity is Assured**

The Block List and the Submitted logs are securely transferred and authenticated via SSL. The Certificate of the Storm Center Certificate Authority comes with the Storm Center Module, and is stored locally. The locally stored certificate is used for two purposes:

1. To check the authenticity of the origin of the received Block List, by verifying the validity of the certificate received with the Block List.
2. To establish an SSL connection with the Storm Center when submitting logs, while assuring that the logs are indeed sent to the Storm Center and to no one else.

The Certificate Authority of SANS DShield.org is Equifax. The file name of the locally stored certificate is `equifax.cer`, and it is stored in the `conf` directory of the Storm Center Module installation.
To send logs to DShield.org, you must register with them. DShield.org authenticate the submitters of logs with a username and password that submitters obtain when registering.

**Size of Logs and Effect on VPN-1 Pro Performance**

Receiving the Block List has no effect on VPN-1 Pro performance because only a very small amount of data is received.

The submitted log is only a small subset of the full SmartDefense log, and is compressed. The size of the log depends on the log interval, and the maximum size of the log database. As a rough guide, 10,000 lines of logs take up 200 KB.

**Planning Considerations**

**Which Logs to send to the Storm Center**

Storm Centers have a special interest in receiving logging information about:

1. Unwanted port 80 traffic reaching the organization.
2. The Drop All rule (the last Rule in the Rule Base, that drops any traffic not explicitly allowed in previous rules).
3. Logs generated by blocking of malicious IPs.
4. SmartDefense and Web Intelligence protections.

**Which Logs NOT to send to the Storm Center**

Do not send logs from rules that log internal traffic.

**Which Identifying Information to Remove from Submitted Logs**

Decide on what part of your organizations IP addresses to obscure from the submitted logs. If all your internal addresses are private, non-routable addresses, you may not feel it is necessary to mask the addresses. On the other hand, even non-routable addresses can reveal information about your internal network topology.

**Configuring Storm Center Integration**

**To Retrieve and Block Malicious IPs**

1. VPN-1 Pro Gateways and SmartCenter Server(s) must be able to connect to the Storm Center using HTTPS. In the Security Rule Base, define an appropriate Rule if necessary.
2. In SmartDefense, configure **Network Security > DShield Storm Center > Retrieve and Block Malicious IPs**. You can block connections from IPs in the Block List at all Gateways, or at selected Gateways.

   **Note**: Make sure that the Block List is enforced on perimeter Gateways ONLY.

3. If you are also submitting logs to DShield, and would like to report logs generated by blocking malicious IPs, make the **Track** setting identical to the **Submit Logs of Type** setting in SmartDefense **DShield Storm Center > Report to DShield**.

4. Install the Security Policy.

**Manual Configuration for Blocking Malicious IPs**

The DShield Block List, when configured via SmartDefense, is enforced before the Rule Base. Because DShield uses statistical analysis, and the Block List is made up of /24 (Class C) networks, those IPs are not necessarily all malicious. Therefore, to prevent reputable IP addresses from being blocked, you can manually add a Block List Rule in the Security Rule Base.

1. In SmartDefense **Network Security > DShield Storm Center**, UNCHECK **Retrieve and Block Malicious IPs**.

2. Add the Block List Rule, as shown in **FIGURE 7-7**.
   - Place the Block List rule as high as possible in the Security Rule Base, but below all authentication rules, and any other rules for trusted sources that should not be blocked.
   - If you want to retrieve and block malicious IPs only at particular gateways, specify them in the **Install On** cell of the rule.

   **Note**: Make sure that the Block List is enforced on perimeter Gateways ONLY.

   - If you are also submitting logs to DShield, and would like to report logs generated by blocking malicious IPs, make the **Track** setting identical to the **Submit Logs of Type** setting in SmartDefense **DShield Storm Center > Report to DShield**.
3 Install the Security Policy.

**To Submit logs to DShield.org**

1 To submit logs to DShield.org, you must register at http://secure.dshield.org/cp/register.php. You will receive a username and password. (You can receive the Block List without registering.)

2 DShield can supply you with reports and statistics about the logs you have submitted. To see those reports, you need to login to DShield at http://secure.dshield.org/cp/login.php.

3 VPN-1 Pro Gateways and SmartCenter Server(s) must be able to connect to the Storm Center using HTTPS. In the Security Rule Base, define an appropriate Rule if necessary.

4 In SmartDefense, configure **Network Security > DShield Storm Center > Report to DShield**. The option **Submit all logs of type** determines which logs will be sent to the Storm Center. For example, it is possible to specify that all logs of type Alert or User Defined Alert will be submitted. Set the **Track** option of any rule or SmartDefense/Web Intelligence protection whose logs you wish to submit, to the **Track** option defined here.

5 Configure the option **Hide internal networks using this mask** to prevent the internal network topology from being exposed by the submitted logs. A mask of 0.0.0.0 reveals the whole of the internal IP address. A mask of 255.255.255.0 reveals 8 valid bits, and converts an IP address such as 192.168.46.88 to 0.0.0.88. Make sure that the Topology is correctly defined for all Gateways (in the Gateway object **Topology** page).

6 Install the Security Policy.
Section 4: Application Intelligence

Check Point Application Intelligence is a set of advanced capabilities, integrated into FireWall-1 and SmartDefense, which detect and prevent application-level attacks. This section describes how to protect against application-level attacks for each application protocol, and work with anti-virus (CVP) and URL filtering (UFP) applications.
Anti Virus Protection

In This Chapter

- Introduction to Integrated Anti Virus Protection  page 143
- Architecture  page 144
- Configuring Integrated Anti Virus Scanning  page 144
- Understanding Scan By Direction and Scan By IP  page 145
- Scanning by Direction: Choosing the Data to Scan  page 149
- File Type Recognition  page 151
- Continuous Download  page 152
- Signature Update Mechanism  page 152
- Logging and Monitoring  page 153
- Scan Failure  page 153

Introduction to Integrated Anti Virus Protection

Viruses are a major threat to business. They have become more dangerous and sophisticated, and have evolved into worms, blended threats (which use combinations of malicious code and vulnerabilities for infection and spread), and trojans.

Check Point Express CI (Content Inspection) gateways include integrated Anti Virus technology.

As an integrated Anti Virus solution, no extra IT resources are required. Businesses gain the benefits of the easy management using the familiar Check Point SMART infrastructure that includes policy management, logging and monitoring. As a single box solution, hardware management is also simplified.
Anti Virus protection is available for the HTTP, FTP, and SMTP protocols. By default all protocols are scanned, and options for each protocol can be centrally configured.

**Architecture**

When Anti Virus scanning is enabled, traffic for the selected protocols is trapped in the kernel and forwarded to the security server. The security server forwards the data stream to the Anti Virus engine. The data is allowed or blocked based on the response of the Anti Virus engine.

Anti Virus scanning is applied only to accepted traffic, that has been allowed by the Security Policy.

With Express CI R57 Anti Virus configuration makes CVP resource configuration obsolete. In cases were both Anti Virus and CVP are used only Anti Virus will work.

**Configuring Integrated Anti Virus Scanning**

1. For all Check Point Express CI gateway objects, check **Anti Virus** in the **Check Point Products** section of the **General Properties** page.

2. In the **Topology** page, define the gateway topology, specifying the internal networks, and the DMZ.

3. Use the **Security** Rule Base to allow services. Anti Virus scanning is applied only to accepted traffic.

4. In the **Content Security** tab select the services that should be scanned using the options provided:
   - In the **Anti Virus** page, configure options for file handling and scan failures.
   - In the **Signature Updates** page, configure when to perform automatic signature updates, or initiate a manual signature update.
   - In the **SMTP**, **FTP** and **HTTP** pages, configure Anti Virus scanning options for these services.
   - In the **File Types** page, configure whether to Scan, Block or Pass traffic according to the file type, and configure continuous Download settings for FTP and HTTP.

**Note** - SMTP file type recognition scan, block and pass are not enabled. Anti Virus scanning is performed on the entire email message.
Understanding Scan By Direction and Scan By IP

In This Section

Definition of Scan By Direction and Scan By IP  page 145
Comparing Scan by Direction and by IP  page 146

Definition of Scan By Direction and Scan By IP

There are two ways to specify the files to be scanned: Scan By direction and Scan by IP. In both cases, Anti Virus scanning is performed only on traffic that is allowed by the Security Rule Base.

Scan By Direction

Specifies whether to scan files passing to or from the external, internal and/or DMZ networks.

This method (the default) is an intuitive way of specifying which files will be scanned without having to specify hosts or networks.

Use this method if you wish to scan all traffic in a given direction. It is possible to specify exceptions, that is, locations to or from which files will not be scanned.

Note - Scan By Direction works only when Check Point Express CI R57 is connected as a gateway, and is placed inline between the external and the Internal/DMZ networks. It does not work when Check Point Express CI R57 is connected as a node, in Proxy mode.

In addition, Scan By Direction only works when the Gateway topology is correctly defined.

Scan By IP Address

Scan by IP address allows you to define very precisely which traffic to scan. For example, if all incoming traffic from external networks reaches the DMZ, Scan by IP allows you to specify that only traffic to the FTP, SMTP, and HTTP servers will be scanned, whereas Scan by Direction scans all traffic to the DMZ.

When choosing to Scan by IP address, you use a Rule Base to specify the source and destination of the data to scan. For FTP, for each rule, you can choose to scan either the GET or PUT methods, or both. For HTTP, for each rule, you can choose to scan either the HTTP Request, or the HTTP Response, or both.
Comparing Scan by Direction and by IP

Scan by Direction allows you to specify which files to scan according to where the file (and not necessarily the connection) originated from and according to its recipients location.

Scan by IP allows you to specify files to scan according to the connection they are sent through and the protocol phase/command where applicable.

As a general rule, when you want most or all files in a given direction to be Anti-Virus scanned, you should use Scan by Direction.

On the other hand, if you want to granularly specify a connection or part of a connection's source or destination to be scanned, you should use Scan by IP.

Comparing Scan by Direction and by IP for SMTP

For SMTP, Scan by Direction and by IP are essentially the same. FIGURE 8-1 shows that for SMTP, the files (data) are always sent in the same direction as the connection. SMTP is used for sending mail. Protocols that are used for receiving email (such as POP3 and IMAP) are not scanned when SMTP is selected.

FIGURE 8-1 Comparing Scan By Direction to Scan by IP address for SMTP
Comparing Scan by Direction and by IP for FTP

For FTP, the difference between Scan by IP and Scan by direction is illustrated in FIGURE 8-2. When the FTP GET command is used, files are transferred in the opposite direction to the connection. When the FTP PUT command is used, files are transferred in the same direction as the connection. The Scan files by direction option allows you to scan files, without having to consider the direction of the connection.

FIGURE 8-2  Comparing Scan by Direction to Scan by IP address for FTP
Comparing Scan by Direction and by IP for HTTP

For HTTP, the difference between Scan by IP and Scan by direction is illustrated in FIGURE 8-3. When choosing to scan by IP, the Source and Destination of the connection are specified, and also whether the Request, Response or both will be scanned. This makes it possible to specify what will be scanned in a very precise way.

FIGURE 8-3 Comparing Scan By Direction to Scan by IP address for HTTP
Scanning by Direction: Choosing the Data to Scan

If Scan by Direction is chosen, it is necessary to choose the direction of the data to scan, depending on whether you wish to scan files to or from the internal networks and the DMZ.

What is a DMZ?

The DMZ (demilitarized zone) is an internal network with an intermediate level of trust. Its trust level lies between that of trusted internal networks, such as a corporate private LAN, and that of untrusted external networks such as the Internet.

Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

The Scan By Direction options allow you to specify a level of Anti Virus scanning that is specific to the DMZ. For example, you can decide not to scan traffic passing from external networks to the DMZ, while scanning traffic passing from the DMZ to internal networks, and from the external to internal networks.

An internal interface can be defined as leading to the DMZ in the Check Point Express CI Gateway topology.

Scan By Direction Options

The Scan By Direction options are as follows:

- **Incoming files arriving to** (see FIGURE 8-4) - this refers to files arriving from external interfaces.
  - the internal networks (1).
  - the DMZ (2).
  - the DMZ and internal networks (1 and 2).

---

**FIGURE 8-4** Options for scanning Incoming files arriving to

---

- **Outgoing files leaving** (see FIGURE 8-5) - this refers to files leaving through external interfaces.
Scanning by Direction: Choosing the Data to Scan

- the internal networks (1).
- the DMZ (2).
- the DMZ and internal networks (1 and 2).

**FIGURE 8-5** Options for scanning Outgoing files leaving

![](image)

- **Internal files** (see **FIGURE 8-6**)
  - **IF THERE IS NO DMZ**
    - passing between all internal networks (1).
  - **IF THERE IS A DMZ**
    - passing between the DMZ and internal networks (2).
    - passing between all internal networks (i.e. between internal networks (1), from the DMZ to internal networks (2), and from internal networks to the DMZ (3)).

**FIGURE 8-6** Options for scanning Internal files
File Type Recognition

Check Point Express CI R57 has a built-in File Type recognition engine, which positively identifies the types of files passed as part of the connection. This also enables you to define a per-type policy for handling files of a given type.

It is possible to specify “safe” file types that will be allowed to pass through the Check Point Express CI Gateway without being scanned for viruses. It is also possible to configure file types that will be scanned or blocked. The following actions can be configured for each file type:

- **Scan** performs Anti Virus scanning for files of this type, according to the settings in the FTP and HTTP pages. By default, all unrecognized file types are scanned.
- **Block** does not allow files of this type. There are file types that are preset to be blocked according to SmartDefense advisories.
- **Pass** allows files of this type to pass through the Check Point Express CI gateway without being scanned for viruses. Files of this type are considered safe.

**Note** - SMTP file type recognition scan, block and pass are not enabled. Anti Virus scanning is performed on the entire email message for all file types.

File types can be considered safe because they are not known to contain viruses. For example, some picture and video files are considered safe. Other formats can be considered safe because they are relatively hard to tamper with. What is considered safe can change according to published threats, and depends on how the administrator balances security versus performance considerations.

Check Point Express CI reliably identifies binary file types by examining the file type signatures (magic numbers). Check Point Express CI does not rely on the file extension (such as *.GIF) which can be spoofed. It also does not use the MIME headers (such as image/gif) in HTTP and mail protocols, which can also be spoofed.
**Continuous Download**

The Anti Virus engine acts as a proxy which caches the scanned file before delivering it to the client only for files that need to be scanned.

When large files are being scanned, if the whole file is checked before being made available, the user may experience an unacceptably long delay before the file is delivered. A similar problem may arise when using client applications with short timeout periods (certain FTP clients for example) to download large files. If the whole file is cached and scanned before being delivered, the client applications may time out while waiting.

To address this, Continuous Download trickles information to the client while the Anti Virus scanning is taking place. If a virus is found during the scan, the file delivery to the client is terminated.

For HTTP and FTP it is possible to specify file types for which Continuous Download will not take place. Some file types (such as Adobe Acrobat PDF files and Microsoft PowerPoint) can open on a client computer before the whole file has been downloaded. If Continuous Download is allowed for those file types, and a virus is present in the opened part of the file, it could infect the client computer.

*Note - SMTP supports Continuous Download per the entire email message.*

**Signature Update Mechanism**

*Note - If the Express CI R57 gateway and/or the SmartCenter Server download from a Check Point server, they must have http and https internet connectivity and DNS must be properly configured on them. To download signature updates verify that you have a valid Check Point User Center username and password.*

*Automatic* updates of the virus signature can be scheduled at any chosen interval. *Manual* updates of virus signatures can be initiated at any time.

The following two signature update mechanisms are available. For both mechanisms, the default update interval is 120 minutes:

- **Signature redistribution on SmartCenter**, by which updates are downloaded only by the SmartCenter Server from the default Check Point signature distribution server, and then redistributed by the SmartCenter Server to all Check Point Express CI gateways. This method is useful when Internet access is not available for all gateways or when it is required that the download only occur once for all the gateways. The gateways communicate only with the SmartCenter, using Secure internal Communication (SIC).
**Default signature distribution server**, by which updates are downloaded directly to the Check Point Express CI gateways. This method will likely result in faster update times, because the gateways get the update from the Check Point signature distribution server as soon as it becomes available. This mechanism is only available for *automatic* updates. It is not available for *manual* updates.

---

**Logging and Monitoring**

Logging information about the Anti Virus scan is sent to the SmartCenter Server, and can be viewed using SmartView Tracker. Information about the results is shown in the logs. For FTP and HTTP, there is also a log for scanned clean data.

In addition, there are logs for signature updates, new update checks and download results.

Monitoring Anti Virus status is performed with SmartView Status. The Anti Virus status will appear under the Firewall-1 product. This status contains information about the currently installed Signature file and the Anti Virus engine version. The Anti Virus status also includes statistics about scanned files and found viruses.

---

**Scan Failure**

The default settings in the Anti Virus window have been configured to prevent the Anti Virus engine from overloading. It is recommended that you use the default settings provided.

If the Anti Virus engine becomes overloaded you can use the options in the Anti Virus window to determine:

- whether you would like to take the chance of allowing files that have not been scanned to pass. This option will leave you open to virus attacks.
- whether you would like to block all files. If you select to block all files a connectivity problem may arise.
**File Handling**

- **Maximum file size to scan** limits the file size that will be allowed through the gateway. Before performing Anti Virus scanning, the gateway reassembles the entire file and then scans it.

**Archive File Handling**

- **Maximum archive file size to scan** limits the archive file size that is allowed through the gateway. Before performing Anti Virus scanning, the gateway reassembles the archive, expands it, and then scans the entire file. An archive is a file that contains one or more files in a compressed format. Archives (and all other file types) are recognized by their binary signature (also known as the “magic number”). By default, any file type that is not positively identified as being non-archive, is assumed to be an archive, and the Anti Virus engine tries to expand it.
The Need to Secure Voice Over IP

Many organizations are using IP connectivity over the Internet between different branches of the company to carry not only data, but voice and video as well. This eliminates the costs of long distance calls using traditional telephony. IP connectivity can also be used for video conferences and for other uses that can lead to significant cost savings for an organization.

Voice and video traffic, like any other information on the corporate IP network, has to be protected as it enters and leaves the organization. Possible threats to this traffic are

- Stealing calls, where the caller pretends to be someone else (by registering the calls in the name of another user).
- Call hijacking, where calls intended for the receiver are redirected to the hijacker.
- Systems hacking using ports opened for VoIP connections.
Check Point Solution for Secure VoIP

In This Section

- **Introduction to the Check Point Solution for Secure VoIP**  page 156
- **Control Signalling and Media Protocols**  page 157
- **VoIP Handover**  page 157
- **VoIP Application Intelligence**  page 159
- **VoIP Logging**  page 160
- **Securing SIP Based VoIP**  page 161
- **Securing H.323-Based VoIP**  page 167
- **Securing MGCP Based VoIP**  page 173
- **Securing SCCP Based VoIP**  page 178

**Introduction to the Check Point Solution for Secure VoIP**

FireWall–1 secures VoIP traffic in H.323, SIP, MGCP and SCCP environments. VoIP calls involve a whole series of complex protocols, each of which can carry potentially threatening information through many ports. **FIGURE 9–1** gives an overview of the VoIP protocols supported by FireWall–1.

**FIGURE 9–1** Secured VoIP Protocols: SIP, H.323, MGCP and SCCP

FireWall–1 makes sure that addresses of the caller and receiver are where they are claimed to be, and that the caller and receiver are allowed to make and receive VoIP calls. In addition, FireWall–1 examines the contents of the packets passing through every
allowed port, to make sure they contain proper information. Full stateful inspection on H.323, SIP, MGCP and SCCP commands ensures that all VoIP packets are structurally valid, and that they arrive in a valid sequence.

**Control Signalling and Media Protocols**

A phone call on both an ordinary digital phone network and a VoIP network is made up of media together with control signals. The voice conversation itself is the media stream. Dial tones and ringing tones, for example, are an indication that call control processes are taking place.

The various VoIP protocols all use very different technologies, though they have the same aims. As illustrated by FIGURE 9-1 on page 156, VoIP protocols handle call control (or gateway) control, and media.

- Call Control (also called signalling) aspects of the call include setting up the call, finding the peer, negotiating coding protocols, making the connection, and ending the call.
- Gateway control is the same as call control, but applies to communication between VoIP devices called Gateways, rather than between endpoint phones. These Gateways act as intermediaries on behalf of the phones.
- Media is the actual voice. Both VoIP and ordinary phone networks use RTP/RTCP for the media. RTP carries the actual media and RTCP carries status and control information.

Control signals open both fixed (known) and dynamic ports. The parties to a call then use control signals to negotiate dynamically assigned ports that each side will open to receive the RTP/RTCP media stream.

**VoIP Handover**

The simplest method of communication between VoIP endpoints involves sending both the signalling and media endpoint to endpoint. In many VoIP networks however, the endpoints cannot know the location of their peers. In that case, the call is managed by an entity that we will refer to as a **handover** device, which allows a VoIP phone call to reach its peer.

Where a handover device is used, the signalling follows a different route through the network than the media. Handover is done in

- SIP by the **Proxy, Redirect Server, and/or Registrar**,
- H.323 by the **Gatekeeper and/or Gateway**,
- MGCP by the **Call Agent** (also called Media Gateway Controller),
- SCCP by the **CallManager**.
In a regular phone network and in H.323, a user is identified with a telephone number. In other VoIP networks a user can be identified in various other ways as well, such as an email address, an IP address or a URL. The phone makes itself known in the network by registering on an entity that is responsible for mapping each user identity to an IP address. The endpoints are then able to make calls.

When making a VoIP call, the endpoint making the call first uses control signals to contact a handover device. This device in turn contacts the destination endpoint, either directly, or via another handover device. After the call setup phase, the RTP/RTCP media always passes endpoint to endpoint.

The example in FIGURE 9-2 illustrates a conversation that VoIP terminal A initiates with VoIP Terminal B using handover. The handover device manages a group of VoIP Phones (endpoints), including endpoints A and B.

**FIGURE 9-2 Understanding handover**

1. Endpoint A sends control signals to the handover device. The handover device and the endpoints agree on the ports they will use to communicate. The way this is done depends on the protocol and the topology.
2. The handover device ‘routes the control signal to Endpoint B.
3. The handover device provides A with the IP address and destination port of B.
4. A sends the media directly to B, endpoint to endpoint.
VoIP Application Intelligence

Introduction to VoIP Application Intelligence

FireWall-1 secures VoIP networks by protecting against all common threats to VoIP traffic. These threats include call hijacking, where calls intended for the receiver are redirected to someone else, call theft, where the caller pretends to be someone else, and network hacking using ports opened for VoIP connections. Other threats are Denial of Service (DoS) attacks by sending malformed or fragmented packets.

FireWall-1 provides VoIP security by inspecting the VoIP control signals that pass through the enforcement point. Using information derived from the control signals, FireWall-1 is able to do the following:

- Restricting Handover Locations using VoIP Domains.
- Controlling Signalling and Media Connections.
- Protocol Specific Application Intelligence.

The following sections explain more about these checks.

Restricting Handover Locations using VoIP Domains

Handover devices are responsible for rerouting call control signals. FireWall-1 makes it possible to prevent the abuse of the redirection capabilities of the signaling protocols. This is done by defining a VoIP Domain.

The handover device is allowed to route calls only to the endpoints in its VoIP Domain. The VoIP Domain also controls the allowed direction of the call.

For example, in FIGURE 9-3, if A and B are in the VoIP domain of the handover device C, FireWall-1 ensures that A sends its media streams only to B, by ensuring that the address of B that the handover device C provides to A (step 3 in FIGURE 9-3), is in the VoIP Domain. This prevents unwanted callers getting through the firewall.

FIGURE 9-3  VoIP Security by FireWall-1
Controlling Signalling and Media Connections

The control signals always pass through the FireWall-1 enforcement point. FireWall-1 is therefore able to secure the call by opening RTP/RTCP ports only for those endpoints that were negotiated during the signalling. It also keeps those ports open only for as long as required, and closes them as soon as the call ends, without waiting for a timeout. The order and direction of the packets is also enforced.

FireWall-1 closes the RTP/RTCP data connections because there is potentially a major security problem in VoIP billing. The problem occurs because the control connection and the media connections follow different routes. The module that is responsible on the billing is the handover device, but the RTP, which is the voice media itself, is not routed through this device. Instead, RTP is routed directly between the IP Phones. The potential security problem is that IP Phones can send VoIP control messages that indicates that the call is ended, but actually continue sending and receiving the media (RTP connection).

FireWall-1 ensures the security and integrity of billing processes by enforcing the relationship between the control and media connections. FireWall-1 inspects the VoIP services, and deletes the media connection when the messages in the control connection specify that the media connection must be ended.

If both endpoints are on the are on the same side of the FireWall-1 enforcement point, FireWall-1 is aware of this fact, and does not open any ports for the media.

Protocol Specific Application Intelligence

FireWall-1 understands the complex VoIP protocols and performs application layer filtering of SIP, H.323, MGCP and SCCP packets. See

- "Application Intelligence for SIP" on page 163.
- "Application Intelligence for H.323" on page 170.
- "MGCP Network Security and Application Intelligence" on page 176.
- "SCCP Network Security and Application Intelligence" on page 179

VoIP Logging

FireWall-1 provides detailed, protocol specific logs for VoIP. If VoIP logging is turned on in the Global Properties Log and Alert page. SIP, H.323, MGCP and SCCP events are logged in the SmartView Tracker. The VoIP specific log fields are:

- **Reg. IP-phones** is for call registration events. For SIP and MGCP, this field shows the URL (for example, example@checkpoint.com). For H.323 this field shows the phone number (1234567, for example)
- **Source IP Phone** and **Destination IP Phone** logs call setup events.
Media Type flowing between the source and destination IP Phones. It can be audio, video, instant messaging, applications, or unknown.

Information Logging information contains call information as well as security information. For example port used, commands used and illegal direction, and setup messages. For MGCP, the commands are shown.

There is also a predefined SmartView Tracker Voice Over IP log query.

If VoIP logging is not turned on, only standard logging will take place, showing the source, destination, protocol and so on.

Protocol-Specific Security: SIP, H.323, MGCP and SCCP

The following sections deal with the specific security requirements of the VoIP protocols supported by FireWall-1.

In This Section

- Securing SIP Based VoIP  page 161
- Securing H.323-Based VoIP  page 167
- Securing MGCP Based VoIP  page 173
- Securing SCCP Based VoIP  page 178

Securing SIP Based VoIP

Note -

- Before reading this section, read “Introduction to the Check Point Solution for Secure VoIP” on page 156 to “Protocol-Specific Security: SIP, H.323, MGCP and SCCP” on page 161.
- The SIP protocol is described in this section only to the extent required to secure SIP traffic using FireWall-1.

In This Section

- SIP Architectural Elements in the Security Rule Base  page 162
- Secured SIP Topologies  page 162
- Application Intelligence for SIP  page 163
- Securing SIP-Based Instant Messenger Applications  page 164
- Synchronizing User Information  page 164
- SIP Services  page 164
- Using SIP on a Non-Default Port  page 165
SIP Architectural Elements in the Security Rule Base

SIP has the following architectural elements, all of which are supported by FireWall-1:

- **SIP Terminal (IP Phone)** — Supports real-time, two way communication with another SIP entity. It supports both signalling (that is, the SIP commands themselves) and media. In SIP, only IP enabled phones can be used.
  
  IP Phones are usually defined in SmartDashboard as a network of IP Phones. There is normally no need to define network objects for individual IP Phones.

- **Proxy** — Manages a number of IP phones. Contacts one or more clients or next-hop servers and passes the call request further.

- **Redirect Server** — Converts SIP URL address into zero or more new addresses, and returns those addresses to the client. It does this before the VoIP connection begins. It does not initiate requests or accept calls.

- **Registrar** — A server that accepts REGISTER requests. A registrar is typically co-located with a proxy or redirect server and MAY offer location services.

The Proxy, Redirect Server and Registrar are handover devices. Handover devices are defined in SmartDashboard as host nodes which manage a VoIP Domain. If you wish to limit handover locations, define a VoIP Domain. A VoIP Domain will typically be a network or group of networks. If the handover devices have the same IP address, only one VoIP Domain need be defined, otherwise, a VoIP Domain must be defined for each one.

To allow SIP conversations you need only create rules to allow the SIP control signals through the FireWall-1 Gateway. There is no need to define a media rule that specifies which ports to open and which endpoints will talk. FireWall-1 derives this information from the signalling. Given a particular VoIP signalling rule, FireWall-1 automatically opens ports for the endpoint to endpoint RTP/RTCP media stream.

Secured SIP Topologies

FireWall-1 can secure all SIP topologies. The handover devices can be on the protected or the unprotected side of the FireWall-1 Gateway, or in a DMZ. Typical SIP topologies include

- **Peer to Peer**, where both signalling and media pass endpoint to endpoint.
One or more handover devices, where signalling passes through one or more Proxies, Redirect Servers or Registrars. Once the call has been set up, the media passes peer to peer.

The Rule Base is defined according to the topology, as described in “Procedure for Configuring SIP-Based VoIP” on page 181.

Application Intelligence for SIP

FireWall-1 restricts handover locations and controls signalling and data connections, as described in “VoIP Application Intelligence” on page 159. For SIP, FireWall-1 Application Intelligence ensures packets conform to RFC 3261 for SIP over UDP/IP (SIP over TCP is not supported), and inspects SIP-based Instant Messaging protocols. It protects against Denial of Service (DoS) attacks, and against penetration attempts such as connection hijacking and connection manipulation.

FireWall-1 validates the expected usage of the SIP protocol. For example, if an end of call message is sent immediately after the start of the call, the call will be denied, because this behavior is characteristic of a DoS attack.

Application Level checks include

- Checking for binaries and illegal characters in the packets.
- Strict RFC enforcement for header fields.
- Restricting the length of header fields.
- Removal of unknown media types.

SmartDefense can perform additional security checks for SIP connections.

Configuration is done by selecting Application Intelligence > VoIP > SIP. The following options are available:

- **Verify SIP header content**. removes characters that should not be used for addresses and checks the structure of the SIP URL.

- **Allow calls using a proxy or a redirect server** allows calls to be made by means of a SIP server. If this option is not checked, only endpoint to endpoint calls are allowed. The additional security obtained by configuring VoIP Domains in the Security Rule Base is only possible for calls using a proxy or a redirect server.

- **Allow the destination to re-invite calls** allows the destination to make a new call to the source while a call from source to destination is in progress. The destination can return data on the same call, for example, open a white board application. The source can always make additional calls to the destination even if this property is not enabled.

- **Maximum invitations per call (from both directions)** defines the maximum number of participants that can take part in a conference call.
• **Block SIP-based video** blocks all applications that use SIP to carry video. This includes the video components of MSN Messenger, when it is configured to use SIP. The default is not to block.

• **Block SIP-based audio** blocks all applications that use SIP to carry audio. This includes the audio components of MSN Messenger when it is configured to use SIP. The default is not to block.

• **Block SIP-based Instant Messaging** blocks all applications that use SIP for instant messaging. The default is to allow. To *selectively* block applications provided by MSN Messenger, do not check this option. Instead, configure **Instant Messengers > MSN over SIP Messenger**. Some peer to peer applications also allow Instant Messaging, and these can be blocked via **Application Intelligence > Peer to Peer**.

### Securing SIP-Based Instant Messenger Applications

For information about Securing SIP-Based Instant Messenger Applications in general, and about MSN Messenger over SIP in particular, see “Securing Instant Messaging Applications” on page 203.

### Synchronizing User Information

The user IP Phone sends SIP messages to the Redirect Server in order to register itself on the network. Once a phone is registered, it can make calls.

These SIP messages cross FireWall-1, which reads them. The VoIP user databases on FireWall-1 and the Redirect Server are therefore always synchronized with each other.

Registration makes it possible to initiate calls from outside the FireWall-1 enforcement point to phones whose addresses are translated using Hide NAT.

If the FireWall-1 machine is rebooted, the VoIP user database is deleted. The cpstop/cpstart commands do not delete the user database.

### SIP Services

Two predefined SIP services are available: *sip* and *sip_any*.

**Note** - The services *sip* and *sip_any* cannot be used in the same rule because they contradict each other.

• *sip* is used to enforce handover. Use a VoIP Domain in the source or destination of the rule, together with the *sip* Service.
When this service is used, registration message are tracked and a database is maintained that includes the details of the IP phones and the users. If an incoming call is made to a Hide NAT ed address, FireWall-1 verifies that the user exists in the sip registration database. This can prevent DoS attacks.

To see a list of the on-line IP phones, run the command `fw tab -t sip_registration -f`.

- `sip_any` is used if not enforcing handover. In that case, do not place a VoIP Domain in the Source or Destination of the rule. Instead, use `Any` or a network object, together with the `sip_any` Service. If a VoIP Domain is used with the `sip_any` service, the packet is dropped.

**Using SIP on a Non-Default Port**

SIP uses UDP port 5060 by default. However, SIP phones and SIP Proxies can be configured to use a different port. VPN-1 Pro can enforce SIP security on any SIP port. To do so, a new UDP service must be defined in SmartDashboard. SIP rules can then be defined in the Security Rule Base that use this new service. It is possible to use both the newly defined service and the predefined services (sip and sip_any) in the same Rule.

To configure a new SIP Service, proceed as follows.

1. From the SmartDashboard main menu, choose Manage > Services > New... > UDP. In the UDP Service Properties window, give it a Name, and specify the new SIP port.
2. Press Advanced.... In the Advanced UDP Service Properties window, choose Protocol Type `SIP_UDP`, and press OK.
3. Define a Rule in the Security Rule Base that use this new service.

**NAT Support for SIP**

All FireWall-1 features can be used with SIP, with the following restrictions regarding Network Address Translation (NAT):

- Static NAT can be used in both automatic and manual NAT rules.
- Hide NAT can be used on endpoints that make outgoing calls.
- Hide NAT can be used on endpoints that allow incoming calls (This is possible because the phone number in incoming call is associated with the real telephone number by means of the database on the Redirect Server). However, Manual Hide NAT rules cannot be used with Hide NAT, for incoming calls. For security reasons, when using Hide NAT for incoming calls, the Destination of the VoIP call in the appropriate rule in the Security Rule Base cannot be `Any`. 

Where both endpoints are on the trusted side of the FireWall-1 enforcement point, calls cannot be made from the same source to two endpoints, where one endpoint is NATed (either Static or Hide) and the other is not.

When using NAT, the Proxy, Redirect Server and Registrar must reside in the external network in order to enable FireWall-1 to track the registration messages, and to allow incoming calls.

NAT on a Proxy, Redirect Server or Registrar is not supported.

Bidirectional NAT of VoIP calls is not supported.

ClusterXL Support for SIP

SIP calls can be made across a ClusterXL Gateway cluster in a High Availability mode. Load Sharing modes are not supported.

Advanced SIP Properties

The following advanced SIP-related properties are available. Default values are indicated in **bold**.

- `fw_sip_allow_mcast` (true, false) allows or drops multicast RTP traffic. This is a per-module property. To change the value, run the following command on the module:
  ```
  fw_ctl set int fw_sip_allow_mcast
  ```

- `sip_accept_unknown_messages` (true, false) allows or drops unknown SIP messages. This is a global property. To change the value, in SmartDashboard **Global Properties> Advanced Customization** page, click **Configure**. In the **Advanced Configuration** window, select **FireWall-1> VoIP> SIP**.

- `sip_allow_two_media_conns` (true, false) either allows or prevents the RTP/RTCP connection passing as two different unidirectional streams instead of one bidirectional stream. This is a global property. To change the value, in SmartDashboard **Global Properties> Advanced Customization** page, click **Configure**. In the **Advanced Configuration** window, select **FireWall-1> VoIP> SIP**.
Securing H.323-Based VoIP

In This Section

- IP phones, which are IP devices that handle both signalling (that is, the H.323 commands themselves) and media. They connect to an H.323 gatekeeper.
- Conventional telephones connect to an H.323 gateway. These are not IP devices, and there is no need to define them in SmartDashboard.
- A Gatekeeper manages a collection of H.323 devices such as phones. It converts phone numbers to IP addresses. A Gatekeeper usually provide Gateway services as well.
- A Gateway provides interoperability between different networks. It translates between the telephony protocol and IP.

FIGURE 9-4 shows the H.323 architectural elements. It does not necessarily represent an actual topology.
The Gatekeeper and Gateway are handover devices. Handover devices are defined in SmartDashboard as host nodes which manage a VoIP Domain. If you wish to limit handover locations, define a VoIP Domain. A VoIP Domain will typically be a network or group of networks. If the handover devices have the same IP address, only one VoIP Domain need be defined. If these devices have different IP addresses, a VoIP Domain must be defined for each one.

To allow H.323 conversations you need only create rules to allow the H.323 control signals through the FireWall-1 Gateway. There is no need to define a rule for the media that specifies which ports to open and which endpoints will talk. FireWall-1 derives this information from the signalling. Given a particular VoIP signalling rule, FireWall-1 automatically opens ports for the endpoint to endpoint RTP/RTCP media stream.

**Secured H.323 Topologies**

FireWall-1 secures the following three H.323 Topologies:

- **Gatekeeper to Gatekeeper**—each Gatekeeper controls a separate endpoint domain (see FIGURE 9-5).
• **Gatekeeper in the DMZ**—the same Gatekeeper controls both endpoint domains. This topology makes it possible to provide Gatekeeper services to other organizations (see FIGURE 9-6).

**FIGURE 9-6** H.323 Topology: Gatekeeper in the DMZ

• **Endpoint to Endpoint**—the IP Phones communicate directly, without a Gatekeeper or a Gateway (see FIGURE 9-7).
FIGURE 9-7  H.323 Topology: Direct endpoint-to-endpoint communication

Application Intelligence for H.323

FireWall-1 supports H.323 version 2, which includes H.225 version 2 and H.245 version 3. It performs the following application layer checks:

- Strict enforcement of the protocol, including the order and direction of H.323 packets.
- If the phone number sent is longer than 24 characters the packet is dropped. This prevents buffer overruns in the server.
- Dynamic ports will only be opened if the port is not used by another service. For example: If the Connect message sends port 80 for the H.245 it will not be opened. This prevents well-known ports being used illegally.

The following additional Application Intelligence checks can be configured via SmartDefense Application Intelligence > VoIP > H.323:

- **Allow to re-direct connections** allows conversations to be handed over on both sides. It must be checked in order to use Gatekeepers or Gateways.
- **Prevent blank source phone numbers for gatekeeper connections** rejects connections in which the source phone number is blank. By default, they are prevented. If a field that should be present in the packet is missing, the packet is dropped.
- **Enable dynamic T.120** allows application-sharing file transfer, used for white board conferencing in applications such as Microsoft NetMeeting. T.120 is not allowed by default.
- **H.245 Tunneling** encapsulates one or more H.245 messages in any Q.931 message. This conserves resources, synchronizes call signaling and control, and reduces call setup time.
Gatekeeper and Gateway Call Routing

H.323 routing modes define which control protocols should pass between the Gatekeepers or Gateways, and which between the endpoints. FireWall-1 can be configured to allow one or more routing modes. To understand routing modes, a basic understanding is required of H.323 protocols and the sequence in which they are used.

Signaling and Media Protocols for H.323

The media in H.323 uses the RTP/RTCP protocols. Signalling is handled by the following H.323 protocols:

- RAS manages registration, admission and status. Uses fixed ports.
- Q.931 manages call setup and termination. Uses fixed ports.
- H.245 negotiates channel usage and capabilities. Uses dynamically assigned ports.

As an H.323 call is processed by a Gatekeeper, these protocols are used in sequence and then the media passes. To end a call, the signaling protocols are used in reverse order.

The protocol sequence for a Gateway is the same, other than the fact that the Gateway only uses RAS to communicate with the Gatekeeper.

Routing Modes

H.323 routing modes define which control protocols should pass between the Gatekeepers or Gateways, and which between the endpoints. FireWall-1 can be configured to allow one or more of the routing modes. At least one of the routing modes must be selected. If FireWall-1 is configured to allow more than one routing mode, the Gatekeeper/Gateway is free to decide which routing mode to use.

FIGURE 9-8 illustrates the three routing modes that can be selected.

FIGURE 9-8 Gatekeeper and Gateway Routing Modes

The routing modes illustrated in FIGURE 9-8 are as follows:
**Direct** mode is for Gatekeepers only. Only the RAS signals pass through the Gatekeeper. All other signalling (Q.931 and H.245) as well as the RTP/RTCP media passes directly endpoint to endpoint.

**Call Setup (Q.931)** mode allows RAS (used only by Gatekeepers) and Q.931 to pass through the Gatekeeper/Gateway. H.245 and the RTP/RTCP media pass endpoint to endpoint.

**Call Setup (Q.931) and Call Control (H.245)** mode allows RAS (for a Gatekeeper only), Q.931 and H.245 to pass through the Gatekeeper/Gateway. Only the RTP/RTCP media passes endpoint to endpoint.

### H.323 Services

The following predefined services are available for use in H.323 rules. They can be used to limit the protocols that are permitted during each stage of the H.323 call. Separate rules can be defined for the different protocols:

- **H.323_ras_only** allows only RAS. Use for call registration only. Cannot be used to make calls. If this service is used, no Application Intelligence checks are made. Do not use in the same rule as the H.323_ras service.

- **H.323_ras** allows a RAS port to be opened, followed by a Q.931 port. Q.931 then opens a H.245 port, which in turn opens ports for RTP/RTCP. Do not use in the same rule as the H.323_ras_only service.

- **H.323** allows a Q.931 to be opened, followed by a H.245 port, which in turn opens ports for RTP/RTCP. Do not use in the same rule as the H.323 service.

- **H.323_any** is like the H.323 service, but also allows the Source and Destination in the rule to be ANY rather than a network object. Only use H.323_any if you do not know the location of the endpoints and are not enforcing handover using a VoIP Domain. Do not use in the same rule as the H.323 service.

### NAT and ClusterXL Support for H.323

- H.323 NAT (both hide and static mode) is only supported in direct (peer to peer) mode.

- ClusterXL gateway clusters are supported in both High Availability and Load Sharing modes.

### Advanced H.323 Security

FireWall-1 supports the following advanced H.323 capabilities:

- **Fast Connect** ensures that audio is available as soon as the phone is answered. This feature is active by default, and is always available.
Securing MGCP Based VoIP

**H.245 Tunneling** encapsulates one or more H.245 messages in any Q.931 message. This conserves resources, synchronizes call signaling and control, and reduces call setup time. Activate this capability by checking **Allow H.245 tunneling** in SmartDefense (**Application Intelligence > VoIP > H323**).

The following H.323-related global properties cannot be changed from SmartDashboard. To change the values, use SmartDashboard **Global Properties > Advanced Customization** page and click **Configure**. In the **Advanced Configuration** window, select **FireWall-1 > VoIP > H.323**. Default values are indicated in **bold**.

- **allow_h323_through_ras** (true, false) allows all H.225 connections thorough RAS.
- **h323_t120_timeout** (3600) defines T.120 timeout values. Value is in seconds.
- **h323_enforce_setup** (true, false) defines whether to enforce the requirement that the first H.225 message in a call will be a setup message.

### Securing MGCP Based VoIP

**Note**
- Before reading this section, read “Introduction to the Check Point Solution for Secure VoIP” on page 156 to “Protocol-Specific Security: SIP, H.323, MGCP and SCCP” on page 161.
- The MGCP protocol is described in this section only to the extent required to secure MGCP traffic using FireWall-1.

The Need for MGCP

Regular phones are relatively inexpensive because they don't need to be complex; they are fixed to a specific switch at a central switching location. IP phones and devices, on the other hand, are not fixed to a specific switch, so they must contain processors that enable them to function and be intelligent on their own, independent from a central switching location. This makes the terminal (phone or device) more complex, and therefore, more expensive.

The MGCP (Media Gateway Control Protocol) protocol is meant to simplify standards for VoIP by eliminating the need for complex, processor-intense IP telephony devices, thus simplifying and lowering the cost of these terminals.
MGCP interoperates with SIP and H.323, but does not replace them. MGCP converts audio signals carried on telephone circuits (PSTN) to data packets carried over the Internet or other packet networks.

**MGCP Protocol and Devices**

MGCP is a protocol for controlling telephony gateways from external call control devices called *Call Agents* (also known as *Media Gateway Controllers*).

MGCP is a master/slave protocol, which means it assumes limited intelligence at the edge (endpoints) and intelligence at the core (Call Agent). In this it differs from SIP and H.323, which are peer-to-peer protocols.

The MGCP assumes that the call control devices, or Call Agents, will synchronize with each other to send commands to devices under their control called *Media Gateways*. Call Agents can also connect directly to IP Phones. The Media Gateways or IP Phones are expected to execute commands sent by the Call Agents. *FIGURE 9–9* shows the MGCP elements and a simplified call control process.

*FIGURE 9–9  MGCP Elements*

The Call Agent and Media Gateways are defined in SmartDashboard, usually as Node objects. There is normally no need to define network objects for phones that are managed using MGCP.
To allow MGCP conversations you need only create rules to allow the MGCP control signals through the FireWall-1 Gateway. There is no need to define a rule for the media that specifies which ports to open and which endpoints will talk. FireWall-1 derives this information from the signalling. Given a particular VoIP signalling rule, FireWall-1 automatically opens ports for the endpoint to endpoint RTP/RTCP media stream.

**Call Agent or Media Gateway Controller**

A Call Agent is a network device that
- Provides call signaling, control and processing intelligence to the media gateway.
- Sends and receives commands to/from the media gateway.

**Media Gateway**

A Media Gateway is a network device that
- Provides conversion between the audio signals carried on telephone circuits and data packets carried over the Internet or over other packet networks.
- Sends notification to the call agent about endpoint events.
- Executes commands from the call agents.

Media Gateways normally support features such as conference calls, 3-way brokering and supervisor inspection. All of these features are supported by the predefined FireWall-1 MGCP services (MGCP-CA and MGCP-MG).

**MGCP, SIP and H.323**

MGCP does not replace SIP or H.323. MGCP interoperates with H.323 and SIP. MGCP interoperates with H.323 and SIP.

SIP and H.323 are comparable protocols that provide call setup, call teardown, call control, capabilities exchange, and supplementary features.

MGCP is a protocol for controlling media gateways from call agents. In a VoIP system, MGCP can be used with SIP or H.323. SIP or H.323 will provide the call control functionality and MGCP can be used to manage media establishment in media gateways.

For example, in **FIGURE 9-10**, a host has an SCCP Call Agent on one interface, and an H.323 gateway or SIP Proxy on a second interface.

1. A Call Agent provides signaling and accepts SIP or H.323 call setup requests.
2. The Call Agent uses MGCP to control the Media Gateway.
3. The Media Gateway establishes media sessions with other H.323 or SIP endpoints.
FireWall-1 provides full network level security for MGCP. FireWall-1 enforces strict compliance with RFC-2705, RFC-3435 (version 1.0) and ITU TGCP specification J.171. In addition, all FireWall-1 capabilities are supported, such as inspection of fragmented packets, anti spoofing, protection against Denial of Service attacks. Note however that NAT on MGCP devices is not supported.

FireWall-1 restricts handover locations and controls signalling and data connections, as described in “VoIP Application Intelligence” on page 159.

SmartDefense can perform additional content security checks for MGCP connections, thereby providing a greater level of protection. MGCP specific Application Intelligence security is configured via SmartDefense, under Application Intelligence > VoIP > MGCP.

Three options are available:
- Blocked/Accepted Commands
- Verify MGCP Header Content
- Allow Multicast RTP Connections
Blocked/Accepted Commands

There are nine pre-defined MGCP commands. Some commands are made by the Call Agent, and others by the Gateway, as shown in TABLE 9-1. It is possible to allow or disallow any command as dictated by the security needs.

TABLE 9-1  MGCP commands

<table>
<thead>
<tr>
<th>Call Agent Commands</th>
<th>Gateway Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>EndpointConfiguration (EPCF)</td>
<td>Notify (NTFY)</td>
</tr>
<tr>
<td>NotificationRequest (RQNT)</td>
<td>DeleteConnection (DLXC)</td>
</tr>
<tr>
<td>CreateConnection (CRCX)</td>
<td>RestartInProgress (RSIP)</td>
</tr>
<tr>
<td>ModifyConnection (MDCX)</td>
<td></td>
</tr>
<tr>
<td>DeleteConnection (DLCX)</td>
<td></td>
</tr>
<tr>
<td>AuditEndpoint (AUEP)</td>
<td></td>
</tr>
<tr>
<td>AuditConnection (AUCX)</td>
<td></td>
</tr>
</tbody>
</table>

In addition, it is possible to define additional proprietary commands, and whether to allow or block those commands. By default, all undefined commands are blocked.

FireWall-1 verifies that the new commands are RFC compliant.

MGCP packets contain an optional SDP header. This header contains information such as the destination port number, the destination IP address and the media type (audio or video). The predefined MGCP commands MDCX and CRCX have an SDP header.

When defining an MGCP command, it is possible to specify whether or not the command contains an SDP header. FireWall-1 knows how to parse the header and check it has the correct syntax. If the destination address and port in the header are allowed, FireWall-1 allows the media connection through the Gateway.

Verify MGCP Header Content

Use this option to block binary characters, in order to prevent executable binary files being sent in the MGCP headers. This option also blocks various potentially dangerous control characters, and the null character.

Allow Multicast RTP Connections

RTP is the protocol used for VoIP media. Multicast RTP can be used for radio. If the server sends a packet with a multicast address, the Media Gateway opens a port, and any client can listen to multicast on that port. Use this option to block or allow MGCP multicasts.
Securing SCCP Based VoIP

Note:
- Before reading this section, read “Introduction to the Check Point Solution for Secure VoIP” on page 156 to “Protocol-Specific Security: SIP, H.323, MGCP and SCCP” on page 161.
- The SCCP protocol is described in this section only to the extent required to secure SCCP traffic using FireWall-1.

In This Section

The SCCP Protocol .......................................................... page 178
SCCP Devices ............................................................... page 178
SCCP Network Security and Application Intelligence ............... page 179
ClusterXL Support for SCCP ............................................. page 179

The SCCP Protocol

Many Cisco® devices use the Cisco proprietary VoIP protocol, SCCP (Skinny Client Control Protocol). The SCCP protocol is also licensed to a number of Cisco partners.

SCCP uses TCP on port 2000 for the control signals. Media is transmitted using RTP over UDP to and from a SCCP client or H.323 terminal for audio.

The protocol headers are binary headers (unlike MGCP, for example, which uses text headers).

The SCCP protocol defines hundreds of messages. They can be broadly divided into three groups:
- Registration and management messages.
- Media Control Messages.
- Call Control Messages.

SCCP Devices

SCCP has a centralized call-control architecture. The CallManager manages SCCP clients (VoIP endpoints), which can be IP Phones or Cisco ATA analog phone adapters. The CallManager controls all the features of the endpoints. It requests information such as the station capabilities, and sends to the VoIP endpoints information such as the button template, and the date/time.

The CallManagers are defined in SmartDashboard, usually as Node objects. The networks containing directly-managed IP Phones are also defined in SmartDashboard. There is normally no need to define network objects for individual phones. Cisco ATA devices that are managed by a CallManager must be defined in SmartDashboard, but the connected analog phones are not defined.
To allow SCCP conversations you need only create rules to allow the SCCP control signals through the FireWall-1 Gateway. There is no need to define a rule for the media that specifies which ports to open and which endpoints will talk. FireWall-1 derives this information from the signalling. Given a particular VoIP signalling rule, FireWall-1 automatically opens ports for the endpoint to endpoint RTP/RTCP media stream.

**SCCP Network Security and Application Intelligence**

FireWall-1 provides full connectivity and network level and security for SCCP based VoIP communication. All SCCP traffic is inspected, and legitimate traffic is allowed to pass while attacks are blocked. All FireWall-1 capabilities are supported, such as anti-spoofing and protection against Denial of Service attacks. Fragmented packets are examined and secured using kernel based streaming. However, NAT on SCCP devices is not supported.

FireWall-1 restricts handover locations, and controls signalling and data connections, as described in “VoIP Application Intelligence” on page 159.

FireWall-1 tracks state and verifies that the state is valid for all SCCP message. For a number of key messages, it also verifies of existence and correctness of the message parameters.

SmartDefense can perform additional content security checks for SCCP connections, thereby providing a greater level of protection. Under Application Intelligence > VoIP > SCCP, two options are available:

**Verify SCCP Header Content**

Use this option to block various potentially dangerous control characters, and the null character.

**Allow Multicast RTP Connections**

RTP is the protocol used for VoIP media. Multicast RTP can be used for radio. If a server sends a packet with a multicast address, the CallManager opens a port, and any client can listen to multicast on that port. Use this option to block or allow SCCP multicasts.

**ClusterXL Support for SCCP**

SCCP calls can be made across a ClusterXL Gateway cluster. However, calls do not survive failover.
Considerations for Secure VoIP

Enforcing Handover

Enforcing handover using a VoIP Domain adds security by providing access control for the VoIP signal protocols.

However, it is sometimes not possible to define a VoIP domain. The handover device may be maintained by an external carrier, so that you do not know which machines the handover device controls. It may also be the case that the handover device is trusted. In these cases it is either impossible or unnecessary to enforce the handover, and there is no need to define a VoIP Domain.

Know Your Network Topology

To create the Security Rule Base rule, you need to know the location of the VoIP machine (handover device) relative to the FireWall-1 enforcement point. For example, for outgoing calls, if the VoIP machine is on the trusted side of the firewall, then the VoIP machine is in the Source of the Rule. If the VoIP machine is behind an untrusted interface (in the DMZ or in the Internet), then it will be the Destination.
Configuring VoIP

In This Section

- Configuring SIP-Based VoIP  page 181
- Configuring H.323-Based VoIP  page 185
- Configuring MGCP-Based VoIP  page 191
- Configuring SCCP-Based VoIP  page 196

Configuring SIP-Based VoIP

In This Section

- Procedure for Configuring SIP-Based VoIP  page 181
- SIP Rules for an Endpoint to Endpoint (no-Proxy) Topology  page 182
- SIP Call Direction  page 182
- SIP Rules for a Proxy Topology  page 182
- SIP Rule for Internal Network Access  page 184

Procedure for Configuring SIP-Based VoIP

1. Define the Network objects (Nodes or Networks) for the IP Phones that will be managed by the VoIP SIP Proxy, Redirect Server or Registrar.

2. Define the Group object for the VoIP endpoint domain. This is a group all the Network objects defined in step 1.

3. Define the Network object for the machine on which the VoIP gateway is installed.

4. Define the VoIP Domain object.
   If the Proxy, Redirect Server and Registrar are all on one machine with a single IP address, define only one VoIP Domain. If they have different IP addresses, define a VoIP Domain for each IP address.
   From the SmartDashboard menu, select Manage>Network Objects>New...>VoIP Domains>VoIP Domain SIP Proxy. Give the Domain object a Name. For the Related endpoints domain choose the Group object defined in step 2. For the VoIP Gateway installed at choose the Node object defined in step 3.

5. Define the VoIP Rule(s) that are appropriate for the topology. See the scenarios in the following sections:
   - “SIP Rules for an Endpoint to Endpoint (no-Proxy) Topology” on page 182
6 Set the SmartDefense options under Application Intelligence > VoIP > SIP as required.
7 Install the Security Policy.

**SIP Rules for an Endpoint to Endpoint (no-Proxy) Topology**
For peer to peer topology, define the following rule:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network object</td>
<td>Network object</td>
<td>sip</td>
<td>Accept</td>
<td></td>
</tr>
</tbody>
</table>

**SIP Call Direction**
To allow both incoming and outgoing calls you need to create bidirectional rules. For example, the following rule allows calls to be made from IP phones in Net_A to phones in Net_B.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net_A</td>
<td>Net_B</td>
<td>sip</td>
<td>Accept</td>
<td>Outgoing calls only</td>
</tr>
</tbody>
</table>

To allow IP phones in Net_B to call Net_A, add the reverse Source and Destination to the rule, as follows:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net_A</td>
<td>Net_B</td>
<td>sip</td>
<td>Accept</td>
<td>Bidirectional calls</td>
</tr>
</tbody>
</table>

**SIP Rules for a Proxy Topology**
A typical topology with a SIP proxy is shown FIGURE 9-11:
To allow calls from the VoIP Domain of the Proxy to Net_B,

1 Define a VoIP Domain. VoIP_Domain_A is the VoIP Domain object with endpoint domain Net_internal. The VoIP is installed on the host called Registrar_Proxy. The object definition is illustrated in FIGURE 9-12.
2 Define the following rule:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP_Domain_A</td>
<td>Net_B</td>
<td>sip</td>
<td>Accept</td>
<td>Outgoing SIP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Handover enforced.</td>
</tr>
</tbody>
</table>

3 To allow bidirectional calls, add the reverse Source and Destination to the rule.

4 If your organization maintains a Proxy/Redirect Server/Registrar on the trusted side of the FireWall-1 Gateway, and you wish to allow outgoing calls to locations that use some other proxy, consider enforcing handover for inbound traffic only, as follows:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net_internal</td>
<td>Any</td>
<td>sip_any</td>
<td>Accept</td>
<td>Outgoing SIP calls</td>
</tr>
<tr>
<td>Any</td>
<td>VoIP_Domain_A</td>
<td>sip</td>
<td>Accept</td>
<td>Incoming SIP calls</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Handover enforced.</td>
</tr>
</tbody>
</table>

5 If you do not wish to enforce handover, define the following rule:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net_internal</td>
<td>Net_B</td>
<td>sip_any</td>
<td>Accept</td>
<td>Outgoing SIP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No handover enforced.</td>
</tr>
</tbody>
</table>

**SIP Rule for Internal Network Access**

*FIGURE 9-13 Internal SIP Access*
Where the end user IP Phones are behind the FireWall-1 enforcement point, and the SIP Registrar/Proxy/Redirect Server are on the other side of the firewall (as in FIGURE 9-13):

1 Define a VoIP Domain. VoIP_Domain_A is the VoIP Domain object with endpoint domain Net_internal. The VoIP is installed on the host called Registrar_Proxy. The object definition is illustrated in FIGURE 9-12 on page 183.

2 Define the following rule allows conversations between all the internal phones.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net_internal</td>
<td>VoIP Domain</td>
<td>sip</td>
<td>Accept</td>
</tr>
</tbody>
</table>

There is no need for an explicit rule permitting control connections between the Registrar and the IP phones. This is because in this case all registration events cross the FireWall-1 enforcement point, so the firewall tracks the registration of the SIP entities and automatically opens the appropriate ports between the Proxy and SIP entities. This implicitly allows SIP control connection between the Proxy and the end user IP phones.

**Configuring SIP-Based Instant Messenger Applications**

For information about configuring MSN Messenger over SIP, see “Configuring SIP-based Instant Messengers” on page 207.

**Configuring H.323-Based VoIP**

In This Section

- Procedure for Configuring H.323-Based VoIP  
  page 185
- H.323 Rule for an Endpoint to Endpoint Topology  
  page 186
- H.323 Call Direction  
  page 187
- H.323 Rules for a Gatekeeper to Gatekeeper Topology  
  page 187
- H.323 Rules for a Gatekeeper in DMZ Topology  
  page 189

**Procedure for Configuring H.323-Based VoIP**

1 Define the Network objects (Nodes or Networks) for the IP Phones that will be managed by the VoIP H.323 Gatekeeper or Gateway.

2 Define the Group object for the VoIP endpoint domain. This is a group all the Network objects defined in step 1.
3 Define the Network object for the machine on which the VoIP gateway is installed.

4 Define the Gatekeeper or Gateway VoIP Domain object(s).
   If the Gatekeeper and Gateway have different IP addresses, define a VoIP Domain
   for each one. If the Gateway and Gatekeeper are on single machine, and have the
   same IP address, define only a single **VoIP Domain H.323 Gatekeeper** object.
   From the SmartDashboard Network objects tree, right click and select **New...>VoIP
   Domains>VoIP Domain H.323 Gatekeeper** or **VoIP Domain H.323 Gateway**.

5 Give the Domain object a **Name**. For the **Related endpoints domain** choose the
   Group object defined in step 2. For the **VoIP Gateway installed at** choose the Node
   object defined in step 3.

6 In the **Routing Mode** tab, define permitted routing modes for the Gateways and
   Gatekeepers. If in doubt, select all the options. It is important to select at least one
   option.

7 Define the VoIP Rule(s) that are appropriate for the topology. See the scenarios in
   the following sections. The scenarios show rules that allow unidirectional calls only.
   For bidirectional calls, change the rules as described in “H.323 Call Direction” on
   page 187.
   • “H.323 Rule for an Endpoint to Endpoint Topology” on page 186
   • “H.323 Rules for a Gatekeeper to Gatekeeper Topology” on page 187
   • “H.323 Rules for a Gatekeeper in DMZ Topology” on page 189

   **Note** - The services **H.323** and **H.323_any** cannot be used in the same rule because they
   contradict each other. Similarly, the services **H.323_ras** and **H.323_ras_any** cannot be used
   in the same rule.

8 It is recommended to make the timeout of the H.323 services identical to the
   Gatekeeper registration timeout. Configure the timeouts in the **Advanced Properties**
   window of the Service object.

9 Make sure that call redirection is allowed in SmartDefense under **Application
   Intelligence > VoIP > H.323**, and set the other options appropriately.

10 Install the Security Policy.

**H.323 Rule for an Endpoint to Endpoint Topology**

An endpoint to endpoint topology is shown in FIGURE 9-14.
For this topology, define the following rules:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network object</td>
<td>Network object</td>
<td>H.323</td>
<td>Accept</td>
<td>If the Source or Destination is Any, use the H.323_any service.</td>
</tr>
</tbody>
</table>

**H.323 Call Direction**

To allow both incoming and outgoing calls you need to allow calls in both directions. For example, the following rule allows calls to be made from IP phones in Net_A to phones in Net_B.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net_A</td>
<td>Net_B</td>
<td>H.323</td>
<td>Accept</td>
<td>Outgoing calls only</td>
</tr>
</tbody>
</table>

To allow IP phones in Net_B to call Net_A, add the reverse Source and Destination to the rule, as follows:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net_A</td>
<td>Net_B</td>
<td>H.323</td>
<td>Accept</td>
<td>Bidirectional calls</td>
</tr>
<tr>
<td>Net_B</td>
<td>Net_A</td>
<td>H.323</td>
<td>Accept</td>
<td></td>
</tr>
</tbody>
</table>

**H.323 Rules for a Gatekeeper to Gatekeeper Topology**

A Gatekeeper to Gatekeeper topology is shown in FIGURE 9-15, with Net_A and Net_B on opposite sides of the FireWall-1 enforcement point.
By H.323-based VoIP with a Gatekeeper managing a VoIP domain, define Security
Rule Base rules either with or without handover domain, as follows.

The rule in TABLE 9-2 uses a VoIP Domain, and allows any endpoint in Net_A to
initiate a H.323 call to any endpoint in Net_B:

TABLE 9-2  H.323 rules with a VoIP domain

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP_Domain_A</td>
<td>VoIP_Domain_B</td>
<td>H323_ras</td>
<td>Accept</td>
</tr>
</tbody>
</table>

VoIP_Domain_A is the VoIP Domain object with endpoint domain Net_A, and
VoIP_Domain_B is the VoIP Domain object with endpoint domain Net_B. The VoIP
domain object configuration for VoIP_Domain_B is illustrated in FIGURE 9-16.
The rules without a VoIP domain shown in TABLE 9-3 are more restrictive than the rule with a VoIP domain. They allow only specific Gatekeeper to initiate the H.323 session. Gatekeeper_A is the machine on which the Gatekeeper for Net_A is installed, and Gatekeeper_B is the machine on which the Gatekeeper for Net_B is installed.

**TABLE 9-3  H.323 rules without a VoIP domain**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gatekeeper_A</td>
<td>Gatekeeper_B</td>
<td>H323_ras_only</td>
<td>Accept</td>
</tr>
<tr>
<td>Net_A</td>
<td>Net_B</td>
<td>H323</td>
<td>Accept</td>
</tr>
</tbody>
</table>

For an explanation of the H.323 services, see “H.323 Services” on page 172.

**H.323 Rules for a Gatekeeper in DMZ Topology**

Starting NG with Application Intelligence, FireWall-1 supports an H.323-based VoIP topology where a Gatekeeper is installed in the DMZ, illustrated in FIGURE 9-17.
In the examples for this topology, Net_A and Net_B are on opposite sides of the FireWall-1 enforcement point.

For this topology, define rules either with or without a VoIP Domain.

**TABLE 9-4** shows a H.323 rule with a VoIP Domain that allows any host in Net_A to initiate H.323 call to any host in Net_B. VoIP Domain B is the VoIP Domain object with endpoint domain Net_B. The VoIP domain object configuration for VoIP_Domain_B is illustrated in **FIGURE 9-16** on page 189.

**TABLE 9-4**  H.323 rule with a handover domain, for a Gatekeeper in the DMZ

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net_A</td>
<td>VoIP_Domain_B</td>
<td>H323_ras</td>
<td>Accept</td>
</tr>
</tbody>
</table>

**TABLE 9-5** shows H.323 rules that also allow any host in Net_A to initiate H.323 call to any host in Net_B, but without using a VoIP Domain. Host_A is the machine on which the VoIP Domain Gatekeeper for Net_A is installed.

**TABLE 9-5**  H.323 rules without a VoIP routing domain, for a Gatekeeper in the DMZ

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host_A</td>
<td>Host_B</td>
<td>H323_ras_only</td>
<td>Accept</td>
</tr>
<tr>
<td>VoIP_Domain_A</td>
<td>VoIP_Domain_B</td>
<td>H323</td>
<td>Accept</td>
</tr>
</tbody>
</table>

For an explanation of the H.323 services, see “H.323 Services” on page 172.
Configuring MGCP-Based VoIP

1. **Procedure for Configuring MGCP-Based VoIP**

   Configure the required options in SmartDefense under Application Intelligence > VoIP > MGCP, and set the options appropriately.

2. Define the Network objects (Nodes or Networks) for the Media Gateways and IP Phones that are controlled by the Call Agents.

3. Define a Group object for the VoIP endpoint domain. This is a group all the Network objects defined in step 2.

4. Define the network object for the machine on which the Call Agent is installed.

5. Define the VoIP Domain object.
   
   From the SmartDashboard menu, select Manage>Network Objects>New...>VoIP Domains>VoIP Domain MGCP. Give the Domain object a Name. For the Related endpoints domain choose the Group object defined in step 3. For the VoIP Gateway installed at choose the network object defined in step 4.

6. Define the VoIP Rule(s) that are appropriate for the topology. Place both predefined MGCP services in the Service column of the rule:
   * MGCP-CA is Call Agent service. It uses port 2727.
   * MGCP-MG is the Media Gateway service. It uses port 2427.

   MGCP interoperates with H.323 and SIP. However, MGCP configuration is independent of the other VoIP protocol configuration. Define separate rules for MGCP and the other VoIP protocols.

   The rules depend on the network topology. For details, see the following sections:
   * “MGCP Rules for a Call Agent in the DMZ” on page 192
   * “MGCP Rules for a Call Agent in the Internal Network” on page 193
   * “MGCP Rules for a Call Agent in an External Network” on page 194

7. Install the Security Policy.
MGCP Rules for a Call Agent in the DMZ

In a DMZ topology shown in FIGURE 9-18, the Media Gateways are in the internal and external networks, and the Call Agent is in a DMZ network connected to a separate interface of the FireWall-1 enforcement point.

FIGURE 9-18 MGCP Call Agent in the DMZ

The rules in TABLE 9-6 allows any telephone managed by MG_Int and MG_Ext to make calls to each other.

### TABLE 9-6  MGCP rules for a Call Agent in the DMZ

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>MG_Int</td>
<td>VoIP_Call_Agent</td>
<td>mgcp_CA</td>
<td>Accept</td>
</tr>
<tr>
<td>MG_Ext</td>
<td>VoIP_Call_Agent</td>
<td>mgcp_MG</td>
<td>Accept</td>
</tr>
<tr>
<td>VoIP_Call_Agent</td>
<td>MG_Int</td>
<td>mgcp_CA</td>
<td>Accept</td>
</tr>
<tr>
<td></td>
<td>MG_Ext</td>
<td>mgcp_MG</td>
<td></td>
</tr>
</tbody>
</table>

VoIP_Call_Agent is the VoIP Domain object with endpoint domain that includes both MG_Int and MG_Ext. Create the VoIP Domain object as shown in FIGURE 9-19. Add both Media Gateway objects to a Group object, and use it as the Related endpoints domain. In the VoIP installed at field, put the Call Agent object.
FIGURE 9-19 VoIP Domain of the MGCP Call Agent

MGCP Rules for a Call Agent in the Internal Network

In the topology shown in FIGURE 9-20, there are Media Gateways in the internal network and in an external network. The Call Agent is in the internal network.

FIGURE 9-20 MGCP Call Agent in an Internal Network
The rules in TABLE 9-7 allows any telephone managed by MG_Int and MG_Ext to make calls to each other. Each rule allows calls in one direction.

**TABLE 9-7** MGCP rules for a Call Agent in the internal network

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP_Call_Agent</td>
<td>MG_Ext</td>
<td>mgcp_CA</td>
<td>Accept</td>
<td>Outgoing calls</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mgcp_MG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MG_Ext</td>
<td>VoIP_Call_Agent</td>
<td>mgcp_CA</td>
<td>Accept</td>
<td>Incoming calls</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mgcp_MG</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

VoIP_Call_Agent is the VoIP Domain object with endpoint domain that includes both MG_Int and MG_Ext. Create the VoIP Domain object as shown in FIGURE 9-19 on page 193. Add both Media Gateway objects to a Group object, and use it as the Related endpoints domain. In the VoIP installed at field, put the Call Agent object.

**MGCP Rules for a Call Agent in an External Network**

In the topology shown in FIGURE 9-21, there are Media Gateways in the internal network and in an external network. The Call Agent is in the external network.

**FIGURE 9-21** MGCP Call Agent in an External Network
The first rule in TABLE 9-8 allows any telephone managed by MG_Int1 and MG_Int2 to call any telephone managed by MG_Ext. The second rule allows calls in the opposite direction. In this case, no VoIP Domain is needed, because the Call Agent is in the external network. Make sure that in the FireWall-1 Gateway object Topology page, the interface that faces the Internet is defined as External.

**TABLE 9-8** MGCP rules for a Call Agent in the internal network

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>MG_Int1</td>
<td>Call_Agent</td>
<td>mgcp_CA</td>
<td>Accept</td>
<td>Outgoing calls</td>
</tr>
<tr>
<td>MG_Int2</td>
<td></td>
<td>mgcp_MG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call_Agent</td>
<td>MG_Int1</td>
<td>mgcp_CA</td>
<td>Accept</td>
<td>Incoming calls</td>
</tr>
<tr>
<td></td>
<td>MG_Int2</td>
<td>mgcp_MG</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Allowing Internal Calls When the Call Agent is in an External Network**

If the Call Agent is in an external network, and you wish to allow internal calls between phones managed by different Media Gateways behind the same interface of the FireWall-1 Gateway, you must define a VoIP Domain. This configuration is illustrated in FIGURE 9-21 on page 194. The rules in TABLE 9-9 allow calls between MG_int1 and MG_Int2.

**TABLE 9-9** MGCP rules for a Call Agent in the internal network

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>MG_Int1</td>
<td>VoIP_Call_Agent</td>
<td>mgcp_CA</td>
<td>Accept</td>
<td>Outgoing calls</td>
</tr>
<tr>
<td>MG_Int2</td>
<td></td>
<td>mgcp_MG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP_Call_Agent</td>
<td>MG_Int1</td>
<td>mgcp_CA</td>
<td>Accept</td>
<td>Incoming calls</td>
</tr>
<tr>
<td></td>
<td>MG_Int2</td>
<td>mgcp_MG</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

VoIP_Call_Agent is the VoIP Domain object with endpoint domain that includes both MG_Int1 and MG_Int2. Create the VoIP Domain object as shown in FIGURE 9-19 on page 193. Add both Media Gateway objects to a Group object, and use it as the Related endpoints domain. In the VoIP installed at field, put the Call Agent object.
Configuring SCCP-Based VoIP

Procedure for Configuring SCCP-Based VoIP
1. Configure the SmartDefense settings for SCCP under Application Intelligence > VoIP > SCCP.

2. Define the Network objects (Nodes or Networks) for the Cisco ATA devices or IP Phones that are controlled by the CallManagers.

3. Define a Group object for the VoIP endpoint domain. This is a group all the Network objects defined in step 2.

4. Define the network object for the machine on which the CallManager is installed.

5. Define the VoIP Domain object.
   From the SmartDashboard menu, select Manage>Network Objects>New...>VoIP Domains>VoIP Domain SCCP. Give the Domain object a Name. For the Related endpoints domain choose the Group object defined in step 3. For the VoIP Gateway installed at choose the network object defined in step 4.

6. Define the VoIP Rule(s) that are appropriate for the topology. Place the predefined SCCP service in the Service column of the rule:
   SCCP interoperates with other VoIP protocols. However, SCCP configuration is independent of the other VoIP protocol configuration. Define separate rules for SCCP and the other VoIP protocols.
   The rules depend on the network topology. For details, see the following sections:
   - “SCCP Rules for a CallManager in the DMZ” on page 196.
   - “SCCP Rules for a CallManager in the Internal Network” on page 198.
   - “SCCP Rules for a CallManager in an External Network” on page 199.

7. Install the Security Policy.

SCCP Rules for a CallManager in the DMZ
In a DMZ topology shown in FIGURE 9-22, the Cisco ATA devices or IP Phones are in the internal and external networks, and the CallManager is in a DMZ network connected to a separate interface of the FireWall-1 enforcement point.
FIGURE 9-22 SCCP CallManager in the DMZ

The rules in TABLE 9-10 allows any telephone managed by ATA_Int and ATA_Ext to make calls to each other.

TABLE 9-10 SCCP rules for a CallManager in the DMZ

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATA_Int</td>
<td>VoIP_Call_Manager</td>
<td>SCCP</td>
<td>Accept</td>
</tr>
<tr>
<td>ATA_Ext</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP_Call_Manager</td>
<td>ATA_Int</td>
<td>SCCP</td>
<td>Accept</td>
</tr>
<tr>
<td></td>
<td>ATA_Ext</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

VoIP_Call_Manager is the VoIP Domain object with endpoint domain that includes both ATA_Int and ATA_Ext. Create the VoIP Domain object as shown in FIGURE 9-23. Add both Cisco ATA device or IP Phone objects to a Group object, and use it as the Related endpoints domain. In the VoIP installed at field, put the CallManager object.
Configuring VoIP

**FIGURE 9-23 VoIP Domain of the SCCP CallManager**

![VoIP Domain Skinny - General](image1)

**SCCP Rules for a CallManager in the Internal Network**

In the topology shown in **FIGURE 9-24**, there are Cisco ATA devices or IP Phones in the internal network and in an external network. The CallManager is in the internal network.

**FIGURE 9-24 SCCP CallManager in an Internal Network**

![SCCP CallManager in an Internal Network](image2)
The rules in **TABLE 9-11** allows any telephone managed by ATA_Int and ATA_Ext to make calls to each other. Each rule allows calls in one direction.

**TABLE 9-11** SCCP rules for a CallManager in the internal network

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP_Call_Manager</td>
<td>ATA_Ext</td>
<td>SCCP</td>
<td>Accept</td>
<td>Outgoing calls</td>
</tr>
<tr>
<td>ATA_Ext</td>
<td>VoIP_Call_Manager</td>
<td>SCCP</td>
<td>Accept</td>
<td>Incoming calls</td>
</tr>
</tbody>
</table>

VoIP_Call_Manager is the VoIP Domain object with endpoint domain that includes both ATA_Int and ATA_Ext. Create the VoIP Domain object as shown in FIGURE 9-23 on page 198. Add both Cisco ATA device or IP Phone objects to a Group object, and use it as the Related endpoints domain. In the VoIP installed at field, put the CallManager object.

**SCCP Rules for a CallManager in an External Network**

In the topology shown in FIGURE 9-25, there are Cisco ATA devices or IP Phones in the internal network and in an external network. The CallManager is in the external network.

**FIGURE 9-25** SCCP CallManager in an External Network
The first rule in *TABLE 9-12* allows any telephone managed by ATA_Int and in the Skinny_LAN to call any telephone managed by ATA_Ext. The second rule allows calls in the opposite direction. In this case, no VoIP Domain is needed, because the CallManager is in the external network. Make sure that in the FireWall-1 Gateway object **Topology** page, the interface that faces the Internet is defined as *External*.

**TABLE 9-12**  SCCP rules for a CallManager in the internal network

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATA_Int</td>
<td>Call_Manager</td>
<td>SCCP</td>
<td>Accept</td>
<td>Outgoing calls</td>
</tr>
<tr>
<td>Skinny_LAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call_Manager</td>
<td>ATA_Int</td>
<td>SCCP</td>
<td>Accept</td>
<td>Incoming calls</td>
</tr>
<tr>
<td>Skinny_LAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Allowing Internal Calls When the CallManager is in an External Network**

If the CallManager is in an external network, and you wish to allow internal calls between phones managed by different Cisco ATA devices or IP Phones behind the same interface of the FireWall-1 Gateway, you must define a VoIP Domain. This configuration is illustrated in **FIGURE 9-25 on page 199**. The rules in **TABLE 9-13** allow calls between ATA_Int and the IP Phones in Skinny_LAN.

**TABLE 9-13**  SCCP rules for a CallManager in the internal network

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATA_Int</td>
<td>VoIP_Call_Manager</td>
<td>SCCP</td>
<td>Accept</td>
<td>Outgoing calls</td>
</tr>
<tr>
<td>Skinny_LAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VoIP_Call_Manager</td>
<td>ATA_Int</td>
<td>SCCP</td>
<td>Accept</td>
<td>Incoming calls</td>
</tr>
<tr>
<td>Skinny_LAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

VoIP_Call_Manager is the VoIP Domain object with endpoint domain that includes both ATA_Int and Skinny_LAN. Create the VoIP Domain object as shown in **FIGURE 9-23 on page 198**. Add both Cisco ATA device or IP Phone objects to a Group object, and use it as the **Related endpoints domain**. In the **VoIP installed at** field, put the CallManager object.
Troubleshooting SIP

To see a list of all the online IP phones, you can view the list of phones that the FireWall-1 notes as having registered. Run the command

```
fw tab -t sip_registration -f
```

The output of this command is a list with the format

```
username; IP address
```

To obtain a lot of useful information about the current SIP calls, run the following command:

```
fw tab -t sip_state -f
```

The output of the command lists all the calls with the following information for each:

- Control connection (source, destination).
- RTP connection (endpoint IP addresses).
- Call state (established, ended, registration).
- Media type (audio, video, audio/video, application).
- Number of reinvites (number of participants in a conference call).
The Need to Secure SIP-based Instant Messenger Applications

SIP is emerging as the de-facto standard for instant messaging applications in the enterprise. There are several known security issues associated with SIP-based instant messaging applications. These are similar to the vulnerabilities associated with SIP when used for Voice Over IP (VoIP), with additional vulnerabilities caused by the nature of Instant Messengers and the way that it is used in the enterprise.

Common Instant Messenger capabilities are file transfer, remote collaboration and remote assistance. File transfers for example are a potential source of virus and worm infections. Traditional content filters do not look for IM traffic and as a result most of the new worms and Trojans use instant messenger and peer to peer networks to propagate. Remote assistance allows help desk staff to control the PC to improve the Total Cost of Ownership, and reduce MIS costs. However, it can also be used by hackers to take control of a remote computer.

The Instant Messaging protocols themselves have vulnerabilities that can be exploited to cause a Denial of Service attack. For example, passing an over-long user name and password for authorization may for some applications cause a buffer overflow that could bring down the SIP server.
Check Point Solution for Securing Instant Messengers

**Introduction to Instant Messenger Security**

FireWall-1 and SmartDefense give powerful and flexible security for SIP-based Instant Messengers. MSN Messenger in particular, in its SIP mode of operation, can be secured with an extra level of granularity.

Instant messenger applications allow communication and collaboration between business users using various modes of communication, such as Instant Messaging, Voice and Video, Application Sharing, White board, File Transfer, and Remote Assistance.

It is possible to block the audio or video capabilities of any SIP-based Instant Messaging application. The Security rule base can be used to allow communication to and from specified locations. For SIP-based MSN Messenger communication, SmartDefense can be used to selectively allow only certain MSN Messenger capabilities.

FireWall-1 and SmartDefense secure all MSN Messenger over SIP topologies. MSN Messenger over SIP requires the use of a SIP proxy, and does not support endpoint to endpoint calls.

**Understanding Instant Messengers Security**

To understand the principles of securing SIP-based Instant Messenger communication, it is highly recommended to read Chapter 9, “Securing Voice Over IP (VoIP)”: “Introduction to the Check Point Solution for Secure VoIP” on page 156 to “Securing SIP Based VoIP” on page 161 (inclusive).

Some Peer to Peer applications also have Instant Messenger capabilities, and these can be blocked or allowed. For details, see the HTML pages and online help for the SmartDefense Application Intelligence > Peer to Peer category.

For detailed information about MSN Messenger and the protocols it uses, see the Microsoft web pages at:

Logging Instant Messenger Applications

FireWall-1 provides detailed, protocol specific logs for Instant Messenger conversations. The following events are logged in SmartView Tracker:

<table>
<thead>
<tr>
<th>Event or Application</th>
<th>SmartView Tracker Field name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call registration</td>
<td>registered IP-phones</td>
<td>SIP address</td>
</tr>
<tr>
<td>Instant message</td>
<td>media type</td>
<td>instant messaging</td>
</tr>
<tr>
<td>Audio</td>
<td>media type</td>
<td>Audio</td>
</tr>
<tr>
<td>Video</td>
<td>media type</td>
<td>Video</td>
</tr>
<tr>
<td>Application sharing and Whiteboard (MSN Messenger only)</td>
<td>media type</td>
<td>Application</td>
</tr>
<tr>
<td>File transfer (MSN Messenger only)</td>
<td>media type</td>
<td>File_Transfer</td>
</tr>
<tr>
<td>Remote Assistant (MSN Messenger only)</td>
<td>media type</td>
<td>Remote_Assistance</td>
</tr>
</tbody>
</table>

The ports used when setting up and maintaining an Instant Messenger call can be either fixed or dynamically assigned. They depend on the call setup sequence, which varies with the event and application. The Service and Source Port fields of the smartView Tracker log record shows the port numbers used.

NAT Support for MSN Messenger over SIP

VPN-1 Pro and SmartDefense allow all SIP-based MSN Messenger applications to work seamlessly with Static Network Address Translation (NAT). Hide NAT is fully supported for instant messenger (chat) and audio connections. For the other MSN Messenger applications, some Hide NAT operations are not supported due to the inconsistent behavior of MSN Messenger. TABLE 10-2 details how Hide NAT can be used with SIP-based MSN Messenger applications.
### TABLE 10-2  Support for Hide NAT with SIP-based MSN Messenger Capabilities

<table>
<thead>
<tr>
<th>Hide NAT</th>
<th>Instant Messaging</th>
<th>Application Sharing and Whiteboard</th>
<th>File Transfer and Remote Assistance</th>
<th>Audio</th>
<th>Video and Audio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal → External</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>(outbound traffic)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External → Internal</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>(inbound traffic)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal → Internal</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>(internal traffic)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Check Point Solution for Securing Instant Messengers
Configuring SIP-based Instant Messengers

FireWall-1 and SmartDefense makes it possible to block or allow SIP-based instant messenger applications. For MSN Messenger over SIP, more granular control is possible. MSN Messenger supported capabilities can be selectively blocked or allowed, these being file transfer, application sharing, white board remote assistant, audio, and video.

To completely block SIP-based instant messenger applications, no configuration is needed, because a security rule is required to allow them.

To selectively block SIP-based instant messenger applications, you must define a security rule that allows them, and then configure SmartDefense. Proceed as follows:

### Defining the Rule Allowing SIP-based Instant Messengers

1. Create a network group object that contains all clients that are allowed to work with the SIP proxy (call it `allowed_phones`, for example).
2. Create a VoIP domain object for the SIP proxy (call it `SIP_domain`, for example).
3. Define the rule that includes all the services that you wish to allow. The rule in **TABLE 10-3** includes all the relevant services, and allows calls in both directions.

**TABLE 10-3**  Example rule allowing SIP-based Instant Messengers

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>allowed_phones</code></td>
<td><code>SIP_domain</code></td>
<td><code>sip</code></td>
<td>Accept</td>
<td>Log</td>
</tr>
<tr>
<td><code>SIP_domain</code></td>
<td><code>allowed_phones</code></td>
<td><code>sip_dynamic_ports</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>T.120</code></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>MSN_Messenger_File_Transfer</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The relevant service are:

- **sip** allows the use of a proxy server and enforces handover via a VoIP Domain. See “SIP Services” on page 164.
- **sip_dynamic_ports** is required for all SIP-based instant messaging applications
- **T.120** is needed for application sharing and whiteboard applications
- **MSN_Messenger_File_Transfer** is used for the MSN Messenger File Transfer application.
Configuring the SmartDefense Instant Messengers options

4 Configure the following options in the SmartDefense Application Intelligence > VoIP > SIP branch:

- **Block SIP-based video** blocks or allows all applications that use SIP to carry video. This includes the video components of MSN Messenger, when it is configured to use SIP. The default is not to block.

- **Block SIP-based audio** blocks or allows all applications that use SIP to carry audio. This includes the audio components of MSN Messenger when it is configured to use SIP. The default is not to block.

- **Block SIP-based Instant Messaging** blocks or allows all applications that use SIP for instant messaging. The default is to block. To selectively allow applications provided by MSN Messenger, configure the options in Application Intelligence > Instant Messengers > MSN over SIP.

5 Some peer to peer applications also have instant messenger capabilities. Block or allow peer to peer applications using the options in Application Intelligence > Peer to Peer.
Microsoft Networking Services (CIFS) Security

In This Chapter

- Securing Microsoft Networking Services (CIFS)  page 209
- Restricting Access to Servers and Shares (CIFS Resource)  page 210

Securing Microsoft Networking Services (CIFS)

CIFS (Common Internet File System) is a protocol used to request file and print services from server systems over a network.

The protocol is an extension of the Server Message Block (SMB) protocol. CIFS is used as the underlying transport layer for the NETBIOS session (nbsession) service over TCP using port 139. In Windows networking, CIFS is used over the Microsoft-DS protocol (port 445) for networking and file sharing. More information on CIFS can be found at http://samba.org/cifs/.

By default, a Windows server has default shares open for administrative purposes (C$, ADMIN$, PRINT$) and so is an easy target for internal attacks such as brute-force password attacks on file servers.

FireWall-1 secures Microsoft Networking Services in the Inspection Module, without requiring a Security Server. This meets the high performance requirements of LAN security (Fast Ethernet and Gigabit Ethernet).

The CIFS resource can be used to enforce the following security checks on CIFS connections:

- Correctness of the protocol.
- Preventing CIFS and NETBIOS messages issued by the client from pointing to beyond message boundaries.
Restricting access to a list of CIFS servers and disk shares.

Logging disk share access.

**Restricting Access to Servers and Shares (CIFS Resource)**

1. Define a new CIFS Resource
2. Configure the CIFS Resource. **Allowed Disk\Print Shares** is a list of allowed CIFS servers and disk shares. Note that the use of wildcards is allowed. Use **Add/Edit/Delete** to modify the list. For example to allow access to the disk share PAUL on the CIFS server BEATLES proceed as follows:
   - Click **Add** and type BEATLES in the **Server Name** field and IPC$ in the **Share Name** field. Click **OK**.
   - Click **Add** again and type BEATLES in the **Server Name** field and PAUL in the **Share Name** field. Click **OK**.
3. Add a new rule. Under **Service**, add either nbsession or Microsoft-DS together with the configured Resource.
4. Install the Security Policy.
CHAPTER 12

FTP Security

Introduction to FTP Content Security

Content Security for FTP connections is provided both by the FireWall-1 kernel and
the FTP Security Server.

CVP checking can be performed on FTP traffic. This is done by redirecting the FTP
traffic to a CVP server. This is configured in the FTP Resource object.

FTP Enforcement by the FireWall-1 kernel

The FireWall-1 kernel enforces RFC compliant use of the PORT commands issued by
the client, to ensure that no arbitrary syntax is sent. FireWall-1 enforces additional
security limitations, including:

- Proper use of the IP field in the PORT command. This verifies that an IP address
  presented on a PORT command is identical to the source address of the client. This
  protects against the FTP bounce attack. A monitor-only setting for this protection
  is available using SmartDefense Application Intelligence > FTP > FTP Bounce.
- Proper use of the Port in the PORT command. Data connections to well-known
  ports are not allowed.
Unidirectional data flow on the data connections. This is a second line of defense to avoid using the data connection for non-FTP data that require bi-directional data flow.

**FTP Enforcement by the FTP Security Server**

The FTP Security Server provides a number of capabilities, as follows.

**Control the Allowed Protocol Commands**

Only a predefined list of FTP commands is allowed, which gives full control over the character of the FTP traffic. Some seldom-used FTP commands may compromise FTP application security and integrity, and so are blocked. These include the commands SITE, REST, MACB, and mail commands such as MAIL and MSND. The SITE command is enabled once, upon login, to allow common FTP applications to work properly. Allowed FTP commands are controlled via SmartDefense Application Intelligence > FTP > FTP Security Server > Allowed FTP Commands

FireWall-1 enables control over the desired mode of FTP traffic, both for passive FTP, where the client initiates the data connection, and for active FTP, where the server initiates the data connection. Typically, the firewall should block connections initiated from outside the protected domain.

**Maintaining Integrity of Other Protected Services**

The FTP security Server validates the random ports used in PORT command by the FTP client or by the FTP security server. This prevents a port being randomly chosen that is in use by a defined service. This protects against the risk of data connection initiation to another active/working service in the protected domain.

**Avoiding Vulnerabilities in FTP Applications**

An exploit could be placed in the value of the PORT command. PORT commands are usually interpreted using string manipulation functions that cause security risks. The FTP Security Server performs a sanity validation for the PORT command parameter.

**Content Security**

It is possible to scan FTP connections for viruses and malicious content using the antivirus scanning capabilities that are integrated into Check Point Express CI. This is configured in the Content Security tab. For details, see “Anti Virus Protection” on page 143.
It is also possible to inspect FTP connections by integrating with third party OPSEC certified CVP and UFP applications. This is configured using an FTP Resource object. For details see “Virus checking an FTP connection using CVP” on page 221.

Configuring Restricted Access to Specific Directories

It is possible to allow only file downloads (by specifying GET as an allowed method) or only uploads (by specifying PUT as an allowed method), or both in an FTP resource.

It is also possible to restrict connections to a particular path and/or filename. This protects against exposure of the FTP server's file system.

The following procedure restricts access to a specific directory on the FTP Server when uploading files from the internal network, but allow files to be downloaded from anywhere on the FTP Server to the internal network.

Two resources must be created. One for upload, and one for download.

1. Create an FTP Resource to allow file downloads (Manage > Resources, click New > FTP...).
   
   In the General tab, Name the resource (Download, for example), and choose a Tracking Option (such as Log).
   
   In the Match tab, type the allowed directory path using wildcards, for example, * to allow any directory and filename. Under Methods, select GET.

2. Create an FTP Resource to allow file uploads.
   
   In the General tab, Name the resource (Upload, for example), and choose a Tracking Option.
   
   In the Match tab, type the allowed directory path and filename, using wildcards. For example /uploads/*. Under Methods, select PUT.

Define a Rule to allow file uploads, and another Rule to allow file downloads. For a LAN called Alaska_LAN and an FTP Server in the DMZ called Alaska.DMZ.ftp, the rules should look similar to the ones in FIGURE 12-1.
**FIGURE 12-1** Example Rules for FTP Upload and Download

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
<th>Time</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alaska_Lan</td>
<td>Alaska.DMZ.ftp</td>
<td>ftp-&gt;Upload</td>
<td>Accept</td>
<td>Log</td>
<td>*Policy Targets</td>
<td>Any</td>
<td>ftp upload to /uploads/*</td>
</tr>
<tr>
<td>Alaska_Lan</td>
<td>Alaska.DMZ.ftp</td>
<td>ftp-&gt;Upload</td>
<td>Accept</td>
<td>Log</td>
<td>*Policy Targets</td>
<td>Any</td>
<td>ftp download from*</td>
</tr>
</tbody>
</table>

3 Install the Security Policy.
In This Chapter

The Need for Content Security  page 215
Check Point Solution for Content Security  page 216
Configuring Content Security  page 226
Advanced CVP Configuration: CVP Chaining and Load Sharing  page 234

The Need for Content Security

Protecting corporate resources is a major concern of most businesses. Blocking undesirable content is an important part of a corporate security policy. For example:

- Computer viruses, Trojans and ActiveX components containing malicious code can bring down entire networks.
- Viewing undesirable Web content wastes time and resources.

Access control firewalls prevent unauthorized traffic from passing through the gateway. However, hackers also attempt to misuse of allowed traffic and services. Some of the most serious threats in today's Internet environment come from attacks that attempt to exploit the application layer. Access control devices cannot easily detect malicious attacks aimed at these services.

Content security applications like virus scanners inspect the content of individual packets for specific services,
Check Point Solution for Content Security

In This Section

- **Introduction to Content Security**
- **Security Servers**
- **Deploying OPSEC Servers**
- **CVP Servers for Anti-Virus and Malicious Content Protection**
- **Using URL Filtering (UFP) to Limit Web Surfers**
- **The TCP Security Server**

**Introduction to Content Security**

VPN-1 Pro provides Content Security by integrating with best-of-breed OPSEC certified applications that complement the VPN-1 Pro Content Security capabilities. OPSEC applications enable organizations to choose the content screening applications that best meet their needs, while managing Content Security centrally, as part of the security policy. These applications:

- Protect against network viruses, by scanning data and URLs to prevent viruses, malicious Java and ActiveX components, and other malicious content from entering your organization.
- Prevent users browsing to undesirable web sites, by filtering URLs.
- Provide auditing capabilities and detailed reports


The Content Vectoring Protocol (CVP) is an API specification developed by Check Point that is mainly used for integration with anti-virus servers. This API defines an asynchronous interface to server applications that perform file content validation. An important feature of this is scanning files for viruses or harmful applets as they pass through firewalls. CVP defines a client/server relationship that enables different FireWall-1 enforcement points to share a common content validation server.

The URL Filtering protocol (UFP) is used to block user access to forbidden Web sites, allowing administrators to define undesirable or inappropriate types of Web sites. No configuration is required at the client machine. It is useful where companies wish to avoid a loss of employee productivity. In Service Provider environments, it can be
offered as an add-on to Internet services, where it may be used for parental restriction of child Web surfing, or on behalf of businesses that have an inherent distrust of Internet content.

**Note** - It is possible to scan HTTP, FTP and SMTP connections for viruses and malicious content using the antivirus scanning capabilities that are integrated into Express CI R57. For details, see "Anti Virus Protection" on page 143.

## Security Servers

Security Servers are Check Point processes that are integrated into VPN-1 Pro. They are user mode processes that perform Content Security for

- HTTP
- FTP
- SMTP

There is also a generic TCP Security Server. Security Servers employ many ways of enforcing Content Security, including, for example, checking whether the connections for these protocols are well formed, stripping script tags for HTTP, email address translation for SMTP and file name matching for FTP.

As well as Content Security, Security Servers also perform Authentication. The Authentication functions of the Security Servers are covered in "Authentication" on page 33.

### How a Security Server Mediates a Connection

**FIGURE 13-1** shows how the Security Servers mediate a connection. The HTTP Security Server is used as an example, but the method is the same for all Security Servers.

When a packet is matched to a Rule which contains a Resource, the Inspection Module diverts (also called “folds”) a connection to a Security Server. The Security Server performs the Application Security checks, and if necessary diverts the connection to a Content Vectoring Protocol (CVP) server application or a URL Filtering (UFP) server application. The Security Server then returns the connection to the Inspection Module, which opens a second connection that is sent on the destination HTTP Server.
FIGURE 13-1 How the Security Server mediates a connection

The source IP address that appears to the destination server is the IP address of the client that originally opened the connection. The connection leaves the security server with the source IP address of the VPN-1 Pro enforcement module, and the outbound kernel performs NAT so that the source IP address is that of the original client.

Deploying OPSEC Servers

OPSEC solutions, such as CVP and UFP servers are deployed on dedicated servers (FIGURE 13-2). These servers are typically either placed in the DMZ, or on a private network segment. This allows fast, secure connections between the CVP servers and the VPN-1 Pro Gateway.

Performing scanning at the network perimeter is both safer and more efficient than performing the scanning at the desktop or the application servers.
FIGURE 13-2 OPSEC Server Integration with VPN-1 Pro
CVP Servers for Anti-Virus and Malicious Content Protection

In This Section

CVP and Anti-Virus Protection for SMTP and HTTP Traffic page 220
How a connection is handled by the HTTP Security Server page 220
Improving CVP Performance for Web Traffic page 221
Virus checking an FTP connection using CVP page 221

CVP and Anti-Virus Protection for SMTP and HTTP Traffic

To perform virus scanning, the HTTP or SMTP security server transfer packets from the VPN-1 Pro Gateway to another server running an OPSEC Certified virus scanner. This method uses the Content Vectoring Protocol (CVP) to transfer packets to and from an OPSEC virus scanning server.

The virus scanning CVP server determines if there is a virus. If it finds a virus it can either:

• Return the file to the VPN-1 Pro Gateway with the offending content removed (if the CVP server is allowed to modify content), or
• Drop the file (if the CVP server is not allowed to modify content).

CVP uses TCP port 18181, by default.

How a connection is handled by the HTTP Security Server

The following discussion describes how the HTTP Security Server handles a connection on which CVP checking is performed. The VPN-1 Pro Gateway that runs the HTTP Security Server acts as a proxy, and so is not an active participant in the connection.

The connection request/response process without a CVP server is:

1. HTTP client to HTTP server (request)
2. HTTP server to HTTP client (response)

The data which needs to be checked is carried in the response which comes from the Web server, so when a CVP server is used the response is always checked. In that case, the connection request/response process is:

1. HTTP client to HTTP server (request)
2. HTTP server to CVP server (response)
3. CVP server to HTTP client (response)
Normally, only the HTTP responses, which come from the Web server, are sent to the CVP Server for checking. However, you also may wish to protect against undesirable content in the HTTP request, for example, when inspecting peer-to-peer connections. In this case, the connection request/response process is

1. HTTP client to CVP server (request)
2. CVP server to HTTP server (request)
3. HTTP server to CVP server (response)
4. CVP server to HTTP client (response)

The HTTP Security Server can be configured to send HTTP headers to the CVP server, as well as the HTTP message data.

**Improving CVP Performance for Web Traffic**

HTTP Security Server performance can be significantly improved by ensuring that safe traffic is not sent to the CVP server. This reduces the amount of traffic sent to the CVP server, and reduce the number of connections opened with the CVP server.

However, sending all content for CVP checking gives more certain protection.

VPN-1 Pro considers safe, picture and video files that are non-executable, because they do not normally contain viruses.

The HTTP Security Server identifies safe content by actually examining the contents of a file. It does not rely on examining the URL (for file extensions such as *.GIF) nor does it rely on checking the MIME type (such as image/gif) in the server response.

For configuration details, see “Configuring CVP Checking for Web Traffic with Improved Performance” on page 230.

**Virus checking an FTP connection using CVP**

Virus scanning on FTP connections can be performed by transferring the file to a third party anti-virus application using the CVP protocol.

**FIGURE 13-3** illustrates how VPN-1 Pro implements CVP for virus checking in an FTP connection.
The relevant rule for the connection specifies a resource that includes Content Vectoring Protocol (CVP) for anti-virus checking.

1. The FTP client establishes a connection via port 21 to the FTP server.
2. The Inspection Module monitors port 21 for GET and PUT commands, and determines that the CVP Server must be invoked.
3. When the client initiates a data transfer over port 20, the Inspection Module folds the connection into the FTP Security Server.
4. The FTP Security Server sends the file to be inspected to the CVP Server.
5. The CVP Server scans the FTP files and returns a Validation Result message, notifying the FTP Security Server of the result of the scan.
6. The CVP Server returns a clean version of the file to the FTP Security Server.
7. The FTP Security Server determines whether to transfer the file, based on the Validation Result message, and takes the action defined for the resource, either allowing or disallowing the file transfer.
8. If allowed, the FTP Security Server relays the FTP file on to the FTP server.
Using URL Filtering (UFP) to Limit Web Surfers

In This Section

Understanding URL Filtering ........................ page 223
URL Filtering Using the HTTP Security Server  ...... page 224
Enhanced UFP Performance Mode .................. page 224
Choosing the URL Filtering Mode ................... page 225

Understanding URL Filtering

The security administrator can choose to prevent access to specific destinations on the Internet in order to allow access only to appropriate Web page information, and make it impossible to access particular Web sites, or download certain file types.

This is done with the help of third party, OPSEC certified URL SmartCenter applications. The security administrator can define a corporate Security Policy that includes URL screening, in order to block undesirable Web pages, and record the types of URLs accessed for internal analysis and reporting needs.

A URL Filtering Protocol (UFP) server is used to maintain a list of URLs and their categories. As a user requests a URL, VPN-1 Pro checks that URL against a UFP Server, which returns the category under which the URL falls. In SmartDashboard, permitted categories can be selected. Access to the Web page is allowed if the URL is in a permitted category.

UFP uses TCP port 18182 by default.

Note - A basic URL filtering capability is built in to VPN-1 Pro. It can be used to block a specific list of URLs without a UFP server. For details, see “Basic URL Filtering” on page 257.

VPN-1 Pro can integrate with OPSEC certified solutions in two ways:

- Enhanced UFP Performance mode (called Enhanced UFP Performance in the URI Resource) uses VPN-1 Pro kernel inspection together with a dedicated UFP daemon (aufpd). However, in this mode it is not possible to use CVP and UFP checking on the same connection.

- The ordinary UFP checking mode uses the VPN-1 Pro HTTP Security Server to mediate UFP connections. This can add significantly to the response time seen by clients that browse web sites, in comparison to the Enhanced UFP Performance mode.
For configuration details, see “Configuring URL Filtering with a UFP Server” on page 230. An explanation follows that describes how these two modes work.

**URL Filtering Using the HTTP Security Server**

**FIGURE 13-4** illustrates how VPN-1 Pro performs URL Filtering of an HTTP connection using the HTTP Security Server and a UFP server.

**FIGURE 13-4** URL Filtering (UFP) Process for an HTTP Connection

1. Client invokes a connection through the VPN-1 Pro Inspection Module.
2. The HTTP Security Server uses UFP to send the URL to be categorized to the third-party UFP Server.
3. The UFP Server inspects the file and returns a Validation Result message, notifying the security server of the result of the inspection.
4. Based on the Validation Result message, the Inspection Module either allows or disallows the viewing of that particular Web page.

**Enhanced UFP Performance Mode**

**FIGURE 13-5** illustrates how enhanced URL Filtering (UFP) performance of an HTTP connection works.
FIGURE 13-5 Enhanced URL Filtering (UFP) process, using kernel inspection

1. Web client invokes a connection through the VPN-1 Pro Inspection Module.
2. The kernel Inspection Module puts up a barrier that prevents the web clients receiving a response from the Web Server before a confirmation is received from the UFP server.
3. HTTP requests destined for the Web Server go through VPN-1 Pro uninterrupted.
4. At the same time as step 3, the Inspection Module extracts the URL, and the AUFPD daemon establishes a UFP session with the UFP server to categorize the URL.
5. Based on the Validation Result message, AUFPD tells the Inspection Module whether or not to block the URL.
6. If the URL is permitted, the barrier is removed, and the HTTP response from the Web Server is allowed through VPN-1 Pro.
7. If the URL is blocked, the HTTP response is rejected.

**Choosing the URL Filtering Mode**

Enhanced UFP Performance Mode and URL Filtering Using the HTTP Security Server are different ways of doing UFP Filtering. When deciding the method to employ, you must balance performance against security.
When the Enhanced UFP Performance mode is used, users browsing Web sites experience significantly improved response times, as compared to UFP checking using the VPN-1 Pro HTTP Security Server. However, in this mode (called Enhanced UFP Performance in the URI Resource), it is not possible to use CVP and UFP checking on the same connection.

The TCP Security Server

Malicious content can potentially be carried in any TCP service, not only SMTP, HTTP and FTP.

The TCP Security Server is used to perform CVP or UFP Content Security by a third party OPSEC compliant application, on any TCP Service.

For configuration details, see “Performing CVP or UFP Inspection on any TCP Service” on page 233.

Configuring Content Security

In This Section

- Resources: What They Are and How to Use Them  page 226
- Creating a Resource and Using it in the Rule Base  page 227
- Configuring Anti-Virus Checking for Incoming Email  page 228
- Configuring CVP Checking for Web Traffic with Improved Performance  page 230
- Configuring URL Filtering with a UFP Server  page 230
- Performing CVP or UFP Inspection on any TCP Service  page 233
- Advanced CVP Configuration: CVP Chaining and Load Sharing  page 234

Resources: What They Are and How to Use Them

To perform Content Security via the Security Rule Base, an object called a Resource is defined in SmartDashboard (FIGURE 13-6). Resources are used to match a specific kind of application layer content, in other words, to specify what content you are looking for, and to perform some action on the content.
Using a Resource turns on either kernel inspection or the security servers, depending on what the resource is used for.

For instance, a rule can be created that will drop the connection and generate an alert if there are GETs or PUTs in an FTP transfer or if a specifically named file is part of the transfer. Another rule can drop email addresses or attachments while allowing the rest of the content through.

To specify the content you are looking for, regular expressions and wildcards can be used in the Resource.

The Resource is triggered when a Rule includes the Resource, and a packet matching that rule is encountered. A Resource is applied per Service. If a connection matches the source and destination of the rule and the match parameters of the Resource, then both the Action in the Rule and the Action in the Resource are applied.

**Creating a Resource and Using it in the Rule Base**

1. To create a resource, select the Resources branch of the objects tree. Select the Resource Type, right click, select a resource type, such as New URL... or New SMTP....
2. Define the resource parameters in the General tab, and in the other tabs as required.
3. To use service with a resource in a rule, right click in the Service column of the rule, right click, and select Add with Resource.... In the Service with Resource window, select the service, and then select the Resource that will operate on the service. Click OK.
If a connection matches the source and destination of the rule and the match parameters of the Resource, then both the Action in the Rule and the Action in the Resource are applied.

**Configuring Anti-Virus Checking for Incoming Email**

The goal is to check incoming mail for viruses, as illustrated in FIGURE 13-7. SMTP mail arrives from the Internet to a mail relay server (Mail_relay) in a DMZ segment. Before the mail is forwarded to the internal mail server (Mail_server), it undergoes virus checking in the anti virus server (Anti_virus_server). Outgoing mail is sent from the mail server towards the internet.

**FIGURE 13-7** Sample Configuration - illustrating Anti-Virus Checking for Incoming Email

---

**General Procedure**

1. Create a host object for the machine on which the third-party OPSEC Server application is installed.

2. Create an OPSEC Application object to represent the OPSEC application server, and associate it with the host object created in step 1.

3. Define an SMTP resource that uses the OPSEC Application object, and associate it with the OPSEC Application object created in step 2. Specify the matching, and the content checking to be done.

4. Define rules that use the resource.

**Implementation**

1. Create a host object (e.g. Anti_virus_server) for the machine on which the third-party OPSEC Server application is installed.
2. Create an OPSEC Application object to represent the OPSEC application server, and associate it with the host object created in step 1. Initialize Secure Internal Communication between the OPSEC Application and the SmartCenter Server. In the CVP Options tab, verify that FW1_cv p is selected, and click OK.

3. Define an SMTP resource that uses the OPSEC object, and associate it with the OPSEC Application object created in step 2. Specify the matching, and the content checking to be done.

   In the General Tab, give the Resource a Name (such as virus_check). Choose the Mail Delivery and the Error Mail Delivery options, and the Exception Tracking.

   In the Match tab, for the Sender put *, and for the Recipient put *@your_domain, (for example *@company.com).

   In the Action1 tab, define the Rewriting Rules, if any.

   In the Action2 tab, define the Attachment handling, if any. Define the largest allowed email attachment.

4. In the CVP tab, check Use CVP (Content Vectoring Protocol), select the CVP Server defined in step 1, and define the CVP Server Options and Reply Order.

   Click OK. A message may appear regarding stripping MIME of type “message/partial”. Accepting the MIME strip of type “message/partial” will result in a configuration change to the Action2 tab. The Strip MIME of Type field will contain message/partial. Stripping the Multipurpose Internet Mail Extension (MIME) type of message/partial will not allow multiple-part messages to be accepted for scanning.

5. Define a pair of rules that will perform virus checking on incoming mail, and a rule to allow outbound email. The rules should look similar to the ones in FIGURE 13-8.

6. Install the Security Policy.

**FIGURE 13-8 Example Rules for SMTP Virus Scanning**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>mail_relay</td>
<td>smtp</td>
<td>Accept</td>
<td>Log</td>
<td>Corporate_gw</td>
<td>Incoming email to mail relay</td>
</tr>
<tr>
<td>mail_relay</td>
<td>mail_server</td>
<td>smtp-&gt; virus_check</td>
<td>Accept</td>
<td>Log</td>
<td>Corporate_gw</td>
<td>Incoming email virus scan</td>
</tr>
<tr>
<td>mail_server</td>
<td>Any</td>
<td>smtp</td>
<td>Accept</td>
<td>Log</td>
<td>Corporate_gw</td>
<td>Outgoing email</td>
</tr>
</tbody>
</table>
Configuring CVP Checking for Web Traffic with Improved Performance

The performance of the CVP server when inspecting HTTP connections can be enhanced by ensuring that only unsafe file types are sent to the CVP server for inspection. For background information, see “Improving CVP Performance for Web Traffic” on page 221.

Proceed as follows:

1. Create a host object for the machine on which the CVP Server application is installed.
2. Create an OPSEC Application object to represent the CVP server, and associate it with the host object created in step 1.
3. Define a URI resource that uses the OPSEC Application object, and associate it with the OPSEC Application object created in step 2. Give it a name (such as Internal.HTTP.CVP), specify the matching, and the content checking to be done.
4. In the CVP tab, select **Send only unsafe file types to the CVP server**, and the other required CVP options.
5. Associate the Resource with the HTTP Service, and place it in a Rule in the Security Rule Base. See the sample rule shown in TABLE 13-1.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal_LAN</td>
<td>Any</td>
<td>http-&gt;Internal.HTTP.CVP</td>
<td>Accept</td>
</tr>
</tbody>
</table>

Configuring URL Filtering with a UFP Server

VPN-1 Pro 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 Pro and the URL Filtering server uses the URL Filtering Protocol.

**Rule Match in UFP Modes**

There are differences in rule matching behavior between UFP rules in **Enforce URI Capabilities** mode (that use the kernel) and rules in **Enhance UFP Performance** mode (that use the HTTP Security server). For background information about these two modes, see “Using URL Filtering (UFP) to Limit Web Surfers” on page 223.
In **Enforce URI Capabilities** mode, the connection is matched to the Source, Destination, Service, and UFP category of the Resource in the rule.

If the connection does not match to all these, the connection is compared to successive rules in the Rule Base until a match is found.

In **Enhance UFP Performance** mode, the connection is matched only to the Source, Destination, and Service in the rule. The connection is *not* matched to the UFP category. If the connection matches the Source, Destination, and Service in the rule, it is *not* matched to any other rule further down the Rule Base.

In this mode, if connection matches the UFP category, the Action in the rule is performed. If the connection does not match the UFP category, the opposite of the Action specified in the Rule is performed.

What this means is that you may only have one rule with an **Enhance UFP Performance** resource, for a given Source/Destination/Service. In the **Match** tab of the resource, you must include all UFP categories. The Action in the rule takes place if *any* of the selected categories match the connection.

If using **Enforce URI Capabilities** mode in a UFP resource, you may have more than one rule with a resource using this mode, for a given Source/Destination/Service. However, in order to have a simpler and less error-prone Rule Base, it is recommended to use only one resource, as for the **Enhance UFP Performance**.

For example, consider the following rules:

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
<td>Resource with UFP Category “Drugs”</td>
<td>Drop</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Any</td>
<td>Resource with UFP Category “Alcohol”</td>
<td>Drop</td>
</tr>
</tbody>
</table>

If a connection fits the UFP category of “Alcohol”:

- In **Enhance UFP Performance** mode, the connection matches on Rule 1 and the connection is Accepted — which is not the desired behavior.
- In **Enforce URI Capabilities** mode, the connection matches on Rule 2 and the connection is Dropped.

The correct way to build this rule in a way that will work in all modes, and for greater simplicity, is as follows:

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
<td>Resource with UFP Categories “Drugs” and “Alcohol”</td>
<td>Drop</td>
</tr>
</tbody>
</table>
Configuring URL Filtering

This procedure describes how to configure a URL Filtering using the VPN-1 Pro kernel or using the Security Server. For background information, see “Using URL Filtering (UFP) to Limit Web Surfers” on page 223.

1. Create a host object for the machine on which the third-party OPSEC Server application is installed.

2. Create an OPSEC Application object (Alaska_HTTP_UFP) to represent the OPSEC application server, and associate it with the host object created in step 1.

3. Create a new URI resource that uses the OPSEC Application object, and associate it with the OPSEC Application object created in step 2.

4. To perform URL Filtering using the VPN-1 Pro kernel, select **Enhance UFP Performance**.

   To perform URL Filtering using the Security Server, select **Enforce URI capabilities**, and select **URI Match Specification Type: UFP**.

   In the **Match** tab, select the **UFP server** object that was created in step 2. Check the appropriate **Categories**. Some UFP Servers show just two categories: **Blocked** and **Not Blocked**. Others show many categories.

   **FIGURE 13-9** shows a restrictive resource that matches one of the many categories.

**FIGURE 13-9** Match tab for a URI Resource for UFP
Performing CVP or UFP Inspection on any TCP Service

5. Associate the Resource with the HTTP Service, and place it in a Rule in the Security Rule Base. See the sample rules shown in TABLE 13-2.

The Action in Rule 1 is Drop because the resource matches on Blocked categories. If the resource were to match on Not Blocked categories, the Actions in Rules 1 and 2 would be reversed: Allow in Rule 1, and Drop in Rule 2.

Rule 2 is required for the Enforce URI Capabilities mode. For the Enhance UFP Performance mode it is recommended to avoid problems in cases where more than one URI resource is used in the Rule Base.

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
<td>http-&gt;Alaska_HTTP_UFP</td>
<td>Drop</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Any</td>
<td>http</td>
<td>Accept</td>
</tr>
</tbody>
</table>

Performing CVP or UFP Inspection on any TCP Service

To configure CVP or UFP inspection on any TCP service:

1. In the TCP Service Properties, Advanced tab, check Enable for TCP Resource.

2. Create a TCP Resource. In the General tab, choose CVP or UFP, and the Exception Track method.

3. Configure settings in the CVP or UFP tab.

4. Add a Rule to the Rule Base, and in the Service column, select Add with Resource.

5. In the Service with Resource window, select the TCP service configured in step 1. under Resource, select the resource created in step 2.

6. Install the Security Policy.

For background information, see “The TCP Security Server” on page 226.

To configure CVP inspection for email, see “Configuring Anti-Virus Checking for Incoming Email” on page 228.

To configure CVP and UFP inspection for Web traffic, see “Configuring Web Content Protection” on page 264.
Advanced CVP Configuration: CVP Chaining and Load Sharing

In This Section

Introduction to CVP Chaining and Load Sharing  page 234
CVP Chaining  page 234
CVP Load Sharing  page 235
Combining CVP Chaining and Load Sharing  page 236
Configuring CVP Chaining and Load Sharing  page 237

Introduction to CVP Chaining and Load Sharing

Traffic that crosses the FireWall-1 enforcement point can be checked using CVP servers. CVP checking is available for Web, Mail, FTP and TCP traffic. For detailed explanations, see:

- “CVP and Anti-Virus Protection for SMTP and HTTP Traffic” on page 220.
- “Virus checking an FTP connection using CVP” on page 221.

It is possible to chain CVP servers in order to combine functionality, and to perform load sharing between CVP servers, in order to speed up CVP checking.

CVP Chaining

CVP servers can be chained for the purpose of combining functionality. Chaining is useful when each of the CVP servers performs a different task, such as scanning for viruses, or blocking large email attachments. In the configuration shown in FIGURE 13-10, the FireWall-1 Security Server invokes the first, second, and third CVP servers in turn.
Chained CVP servers are invoked in the order chosen by the administrator in the CVP Group object. When choosing a chaining order, consider whether there are any security or connectivity issues. For example, in FIGURE 13-10, you may wish the virus scanning to take place first.

The order in which the chained servers are called, is relative to the response of the server. This is the case whether the server is on the unprotected (external interface) side of the FireWall-1 enforcement point or on the protected (internal interface) side.

For example, in FIGURE 13-10, consider a user at an internal FTP client who is downloading a file from an external FTP server. CVP checking is done on the response from the FTP server (that is, on the downloaded file) in the order defined in the CVP group object.

There is one exception to this order. The HTTP Security server allows CVP checking to be done on the HTTP request. CVP checking of HTTP requests is performed by the CVP servers in the reverse of the order specified in the CVP Group object.

CVP chaining works only if all servers in the chain are available. If one or more of the servers is unavailable, the whole CVP session is dropped. This is because skipping one of the servers may contradict the security policy. For example, the security policy may specify that both virus scanning and blocking of large attachments are mandatory.

**CVP Load Sharing**

Identical CVP servers can be configured to share the load among themselves. Load sharing can speed up CVP checking by allowing many CVP sessions to run simultaneously on more than one CVP server.
Two load sharing methods are available:

- In the *round robin* method, the FireWall-1 Security Server sends each new CVP session to a different CVP server in turn.
- In the *random* method, the FireWall-1 Security Server sends each new CVP session to a randomly chosen CVP server.

It is possible to configure a load sharing suspension period for a CVP server that does not respond. During that period of time, that CVP server does not take part in the load sharing group.

CVP load sharing is implemented by defining a Resource that invokes a group of CVP servers. The order in round robin mode is configured in the CVP Group object.

**FIGURE 13-11** shows two CVP servers that share the load among themselves.

**FIGURE 13-11** Load sharing between CVP servers

---

**Combining CVP Chaining and Load Sharing**

It is possible to combine CVP chaining and load sharing. **FIGURE 13-12** shows three CVP servers. Two perform load sharing between themselves, and the load sharing group is chained with another CVP server.

It is possible to put a load sharing group into a CVP chain, but it is not possible to perform load sharing between chained CVP groups.
Configuring CVP Chaining and Load Sharing

1. For each CVP server, define a CVP Server object. To define a CVP Server object, right click in the Servers and OPSEC Application tree, and select New > OPSEC Application... In the OPSEC Application Properties window, General tab, make sure that the selected Server Entities include CVP.

2. Define a CVP Group object. A CVP Group object contains CVP server objects, and is used in the same way as an OPSEC Application object for a CVP server. To define a CVP Group object, right click the Servers and OPSEC Application tree, and select New > CVP Group.

3. In the CVP Group Properties window, add the CVP servers to the group.

4. Choose the Work distribution method: Either Load sharing or Chaining.

5. If you chose Load sharing, define the Load sharing method, and the Load sharing suspend timeout, if any.

6. Create a Resource object. In the Resources tree, right click and select one of the following: New > URI..., New > SMTP..., New > FTP..., or New > TCP... Define the content security capabilities.

7. In the CVP Server field in the CVP tab of the Resource object, select the CVP Group defined in step 2.

8. In the Security Rule Base, define a rule that uses the Resource.

9. Save and install the Security Policy.
Section 5: Web Security

This section describes the VPN-1 Pro Web Content capabilities, and the Web Intelligence add-on for VPN-1 Pro that provides high performance attack protection for web servers and applications.
CHAPTER 14

Web Intelligence

In This Chapter

The Need for Web Attack Protection  page 241
The Web Intelligence Solution for Web Attack Protection  page 242
Web Intelligence Technologies  page 243
Web Intelligence Online Updates  page 243
Web Intelligence Security and Usability  page 244
Web Intelligence Protections  page 247
Web Content Protections  page 248
Understanding HTTP Sessions, Connections and URLs  page 249
Connectivity Versus Security Considerations  page 251
Web Security Performance Considerations  page 252
Backward Compatibility Options for HTTP Protocol Inspection  page 254

The Need for Web Attack Protection

Web servers and web applications have evolved from their origins as serving simple static content. Today, web servers and applications can create dynamic pages, invoke applications, and communicate with databases to produce useful content for users. With most web server platforms bundling applications with the server, even the simplest web sites interact with web applications.
With almost all organizations allowing web traffic (TCP port 80) through their perimeter firewall, hackers are increasingly focusing their attacks on web servers and applications. Many attacks today exploit security weaknesses in the different layers of the modern web architecture, often termed as the N-tier web architecture. These attacks range from defacing the primary web interface, getting an embedded web application on a server to do unintended functions, installing malicious applications, to tricking the backend database to send information back to the user.

Similar to network security, web security is only as strong as the weakest link. To build secure web applications, web developers must design security in every aspect of the web application. Unfortunately, many enterprise web applications were not designed with holistic security in mind. Worse, an organization may only design web security into only some of the web servers that are made accessible to the outside world.

**The Web Intelligence Solution for Web Attack Protection**

Check Point Web Intelligence enables customers to configure, enforce and update attack protections for web servers and applications. Web Intelligence protections are designed specifically for web-based attacks, and complement the network and application level protections offered by SmartDefense. In addition, Web Intelligence Advisories published online by Check Point provide information and add new attack defenses.

Web Intelligence not only protects against a range of known attacks, varying from attacks on the web server itself to databases used by web applications, but also incorporates intelligent security technologies that protect against entire categories of emerging, or unknown, attacks.

Unlike web firewalls and traditional intrusion protection systems, Web Intelligence provides proactive attack protections. It ensures that communications between clients and web servers comply with published standards and security best practices, restricts hackers from executing irrelevant system commands, and inspects traffic passing to web
servers to ensure that they don't contain dangerous malicious code. Web Intelligence allows organizations to permit access to their web servers and applications without sacrificing either security or performance.

**Web Intelligence Technologies**

Web Intelligence is based on Check Point's *Stateful Inspection*, *Application Intelligence*, and *Malicious Code Protector* technologies, so that it is possible to block not only specific attacks, but also entire categories of attacks, while allowing legitimate traffic to pass.

- **Malicious Code Protector** is a Check Point patent-pending technology that blocks hackers from sending malicious code to target web servers and applications. It can detect malicious executable code within web communications by identifying not only the existence of executable code in a data stream but its potential for malicious behavior. Malicious Code Protector is a kernel-based protection delivering almost wire-speed performance.

- **Application Intelligence** is a set of technologies that detect and prevent application-level attacks by integrating a deeper understanding of application behavior into network security defenses.

- **Stateful Inspection** analyzes information flow into and out of a network so that real-time security decisions can be based on communication session information as well as on application information. It accomplishes this by tracking the state and context of all communications traversing the firewall gateway, even when the connection involves complex protocols.

**Web Intelligence Online Updates**

Web intelligence is an add-on for VPN-1 Pro. Customers who purchase the SmartDefense Subscription service can automatically update both SmartDefense and Web Intelligence with a single click. Updates are released frequently, and are obtained from the Check Point SmartDefense site:

http://www.checkpoint.com/techsupport/documentation/smartdefense/index.html

Customers with a valid subscription license also receive special SmartDefense Advisories that provide updated SmartDefense and Web Intelligence attack protections, as well as information, tools and best practice methods to mitigate different attacks.

**Tip** - It is recommended to keep your gateway version up-to-date, as the newest defenses are incorporated into the latest version of Check Point software.
Web Intelligence Security and Usability

Web Intelligence provides a number of Security and Usability enhancements that make it a very effective tool for configuring, enforcing and updating attack protections for web servers and applications.

Web Server Focused Security

Web Intelligence focuses on protecting web servers against attacks. As such, web server objects are defined, and protections are applied either to all web servers, or to selected web servers. Any gateway or host object can be defined as a web server.

Enforcement Granularity

It is possible to vary the scope of the protection. A protection can be applied to selected web servers, or to all web servers.

![FIGURE 14-2 Protection Scope and Action Settings](image)

Configuration Flexibility

The Web Server View page in SmartDashboard gives a convenient global view of every Web Intelligence protection. The configuration state of every protection on every web server can be viewed and changed.

Protections can be also be enabled/disabled from the individual protection page in Web Intelligence, and via the web server object. The protections can be applied via the web server object if the protection scope in Web Intelligence is set to apply to specific web servers.
Variable Security Levels

To provide good protection with a minimum number of false positives, a number of advanced defenses (Malicious Code Protector, Cross Site Scripting, SQL Injection and Command Injection) have three possible security levels. By moving a slider, you can choose the appropriate trade-off between a high detection rate on the one hand and a low level of false positives on the other.

FIGURE 14-4 Variable protection level slider
Monitor Only Mode

All Web Intelligence protections have a monitor-only option, which detects and tracks unauthorized traffic without blocking it (see FIGURE 14-2). Intrusions are logged in SmartView Tracker.

The monitor-only option is helpful when deploying a Web Intelligence protection for the first time, to evaluate the effectiveness of the protection without interrupting connectivity. Monitor-only mode also makes it possible to have an audit-only deployment.

Customizable Error Page

Many Web Intelligence protections give the administrator the ability to define an error page that can be sent back to the user whose browsing was blocked (see FIGURE 14-5). This page (in conjunction with SmartView Tracker) can be used to pinpoint the exact reason that caused the connection to be closed.

FIGURE 14-5 HTML Error Page Configuration
This makes it possible to quickly nail down and eliminate the attack, before it can spread. The security administrator can fix the problem even before users know about it, or if the users notice the problem first, they can call the Help Desk about it. Alternatively, users can be given information in the web page about how to fix the problem themselves, which is of great benefit to overworked support staff.

The administrator can customize the page with text and a logo. To help pinpoint the reason that caused the connection to be closed, the page shows two IDs: a Reject ID and an Error ID.

**Note** - Activating the Error Page decreases performance for Web traffic to which this feature is applied.

### Reject ID

The Reject ID that appears on the Error page is intended to deliver information to the administrator without exposing it to a potential attacker.

The Reject ID is unique for each rejected connection. The Reject ID also appears in the SmartView Tracker, and allows the administrator to correlate between an error and a log record of a specific connection. The log record contains attack information, such as “Cross site scripting detected”.

### Error Description ID

The Error description ID is a standard ID that is used to identify the attack. It appears in the SmartView Tracker log, and corresponds to a SecureKnowledge solution about the attack. For example, the following could appear in the Information column of the SmartTracker log: “WSE0030002 cross site scripting detected in request”. The WSE0030002 is the Error description ID, and a SecureKnowledge search for that ID will locate information about the attack.

The administrator can choose whether or not to display the Error Description ID on the error page. It is not recommended to display it because the information could be misused by an attacker.

### Web Intelligence Protections

Web Intelligence protections are organized into a number of protection classes.

**Note** - Details about individual protections can be found in the Web Intelligence GUI, and in the online help.
Web Content Protections

TABLE 14-1 Web Intelligence Protection Classes

<table>
<thead>
<tr>
<th>Protection Class</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious Code</td>
<td>These protections allow you to prevent attacks that run malicious code on Web Servers (or clients).</td>
</tr>
<tr>
<td>Application Layer</td>
<td>This class of protections prevents hackers from introducing text, tags, commands, or other characters that a web application will interpret as special instructions. Introducing them in forms or URLs can allow a hacker to steal private data, redirect a communication session to a malicious web site, steal information from a database, gain unauthorized access, or execute restricted commands.</td>
</tr>
<tr>
<td>Information Disclosure</td>
<td>These protections prevent an attacker gathering information about a web site. The goal of the attacker is to get the web server to reveal information that can be used to tailor an attack.</td>
</tr>
<tr>
<td>HTTP Protocol Inspection</td>
<td>HTTP Protocol Inspection provides strict enforcement of the HTTP protocol, ensuring these sessions comply with RFC standards and common security practices.</td>
</tr>
</tbody>
</table>

Web Intelligence and ClusterXL Gateway Clusters

Web Intelligence features on a ClusterXL gateway cluster do not survive failover. This means that if ClusterXL is providing Web Intelligence protections, and a cluster member fails, HTTP connections through the failed member are lost.

Web Content Protections

It is possible to scan HTTP connections for viruses and malicious content using the antivirus scanning capabilities that are integrated into Express CI R.57. For details, see “Anti Virus Protection” on page 143.

VPN-1 Pro provides Web Content Security via its OPSEC partners. This allows URL filtering and Network Virus Protection using Check Point best-of-breed partners. For details, see “CVP and UFP Content Security” on page 215.

VPN-1 Pro also provides a number of integrated web security capabilities that are configured via the Security Rule Base. These include a number of URL-based protections, and the ability to secure XML Web Services (SOAP) on Web Servers. For details, see Chapter 15, “Web Content Protection”.

248
Understanding HTTP Sessions, Connections and URLs

To understand how to best use VPN-1 Pro web security and Web Intelligence protections, it is important to understand some basic terms and concepts regarding HTTP sessions, HTTP connections, and URLs.

An HTTP session is made up of an HTTP request and an HTTP response. In other words:

\[
\text{HTTP Session} = \text{HTTP Request} + \text{HTTP Response}
\]

Both the HTTP request and the HTTP response have a header section and a body section.

**HTTP Request Example**

**Header section**

The URL is marked in **bold** for clarity.

```plaintext
GET http://www.site.com/path/file.html?param1=val1&param2=value2 HTTP/1.1
Host: www.site.com
Range: 1000-2000
Cookie: cookiename=A172653987651987361BDEF
```
Understanding HTTP Sessions, Connections and URLs

**Body section**

<Some content (usually a filled form which will be submitted)>

**HTTP Response Example**

**Header section**

HTTP 200 OK  
Content-Encoding: gzip  
Content-Type: text/html  
Transfer-Encoding: chunked  
Content-Disposition: http://alternative.url.com

**Body section**

<Some content (usually an HTML page or a binary file)>

**HTTP Connections**

HTTP/1.1 encourages the transmission of multiple requests over a single TCP connection. Each request must still be sent in one contiguous message, and a server must send responses (on a given connection) in the order that it received the corresponding requests.

The following is an example of an HTTP request connection:

<table>
<thead>
<tr>
<th>Request # 1</th>
<th>Header section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post /Hello/ HTTP/1.1</td>
<td></td>
</tr>
<tr>
<td>Host: <a href="http://www.walla.co.il">www.walla.co.il</a></td>
<td></td>
</tr>
<tr>
<td>User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT5.0)</td>
<td></td>
</tr>
<tr>
<td>Pragma: no-cache</td>
<td></td>
</tr>
<tr>
<td>Content-length: 20</td>
<td></td>
</tr>
<tr>
<td>Connection: Keep-alive</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Request # 1 - Body</th>
</tr>
</thead>
<tbody>
<tr>
<td>This my example body</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Request # 2</th>
<th>Header section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get /scripts/ HTTP/1.1</td>
<td></td>
</tr>
<tr>
<td>Host: <a href="http://www.walla.co.il">www.walla.co.il</a></td>
<td></td>
</tr>
<tr>
<td>User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT5.0)</td>
<td></td>
</tr>
<tr>
<td>Pragma: no-cache</td>
<td></td>
</tr>
<tr>
<td>Content-length: 0</td>
<td></td>
</tr>
<tr>
<td>Connection: Keep-alive</td>
<td></td>
</tr>
</tbody>
</table>

250
Understanding URLs

A URL is made up of the Host, Path and Query parameters. In the URL in FIGURE 14-6, the Host is http://www.elvis.com, the Path is /alive/qc.html, and the Query is everything else. VPN-1 Pro and Web intelligence can filter the URL on these parameters and decide whether to allow the HTTP request containing a particular URL.

FIGURE 14-6 Example URL showing Host, Path and Query components

Connectivity Versus Security Considerations

Web Intelligence can be tuned for greater web server security at the expense of connectivity, or vice versa.

Monitor Only Mode

All Web Intelligence protections have a monitor-only mode which makes it possible to evaluate how the protection will affect connectivity, by examining logs to spot traffic that Web Intelligence has detected as being dangerous. All this, while allowing uninterrupted traffic flow.

Protection for Specific Servers

All Web Intelligence defenses can be activated for specific web servers. If the protection is problematic on a particular web server, it can be turned off for that specific web server.

Variable Security Levels

Some of the advanced defenses (Cross Site Scripting, Command Injection, SQL injection and Malicious Code Protector) have variable security level settings. If a connectivity problem arises on a specific web server the security level can be lowered for that web server.
Connectivity Implications of Specific Protections

HTTP protocol inspection settings that are too severe can affect connectivity to and from valid web servers.

- **HTTP Format sizes** protection restricts URL lengths, header lengths or the number of headers. This is good practice because these elements can be used to perform a Denial of Service attack on a web server. However, these restrictions can potentially block valid sites. Applying the protection for specific web servers can solve the connectivity problems.

- **ASCII only Request Header** protection can block connectivity to web pages that have non-ASCII characters in URLs. Applying the protection for specific web servers can solve the connectivity problems.

- **HTTP methods** – Some standard and non-standard HTTP methods are unsafe, because they can be used to exploit vulnerabilities on a web server. Microsoft WebDAV methods (used for Outlook Express access to Hotmail), for example, have certain security issues, but blocking them can prevent use of important applications. Applying the protection for specific web servers can solve the connectivity problems.

Web Security Performance Considerations

In This Section

- *Protections Implemented in the Kernel Vs. Security Server*  
  page 252
- *Protections with a Higher Performance Overhead*  
  page 253
- *Adjusting the Number of Allowed HTTP Concurrent Connections*  
  page 254

Protections Implemented in the Kernel Vs. Security Server

Web Intelligence provides a wide range of security features for web servers. All Web Intelligence features are implemented in the kernel Inspection Module, which means that users benefit from very high performance.
VPN-1 Pro provides a number of web security capabilities that do not require the Web Intelligence add-on. These capabilities make use of the HTTP Security Server. The performance provided by the HTTP Security Server is not as high as that provided by the kernel. These capabilities are available by defining a URI Resource and using it the Security Rule Base. They are listed in Table 14-2.

**Table 14-2** Web security capabilities that do not require the Web Intelligence Add-On

<table>
<thead>
<tr>
<th>Web security capability</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Integrated Anti-Virus scanning</td>
<td>“Anti-Virus Protection” on page 143.</td>
</tr>
<tr>
<td>2. Integration with third-party OPSEC-certified CVP servers</td>
<td>“CVP Servers for Anti-Virus and Malicious Content Protection” on page 220.</td>
</tr>
<tr>
<td>for Anti-Virus protection</td>
<td></td>
</tr>
<tr>
<td>3. URL filtering (via a UFP server) with enhanced security checks.</td>
<td>“Using URL Filtering (UFP) to Limit Web Surfers” on page 223.</td>
</tr>
<tr>
<td>4. Blocking URL-based attacks by source and destination</td>
<td>“Filtering URLs, Schemes and Methods by Source and Destination” on page 256.</td>
</tr>
<tr>
<td>5. Integrated URL filtering of a limited list of sites.</td>
<td>“Basic URL Filtering” on page 257.</td>
</tr>
</tbody>
</table>

**Protections with a Higher Performance Overhead**

Web Intelligence default protections are optimized to blend high security and performance.

Activating the following features decreases performance for Web traffic to which these features are applied:

- Custom HTML error pages.
- **Header Spoofing**, where headers are rewritten.
- **ASCII Only Response Headers**, where the HTTP response is inspected.
Adjusting the Number of Allowed HTTP Concurrent Connections

It is possible to adjust the resources available for HTTP connections on the VPN-1 Pro gateway. If traffic volume is greater than 1000 concurrent connections, you can increase the allowed maximum number of concurrent HTTP connections. Conversely, if there is a problem installing the Security Policy due to a lack of memory, you can decrease the allowed maximum number of concurrent connections.

From the SmartDashboard main menu, select Policy> Global Properties, and then SmartDashboard Customization > Configure. In the Advanced Configuration window, select FireWall-1 > Web Security > Tuning. Adjust the value of the parameter http_max_concurrent_connections. The default value is 1000.

Backward Compatibility Options for HTTP Protocol Inspection

Web Intelligence performs high performance kernel-level inspection of all connections passing through enforcement modules of version NG with Application Intelligence (R55W) or higher.

On enforcement modules of lower version, there is a choice. In Web Intelligence, under HTTP Protocol Inspection, it is possible to choose whether to perform HTTP protocol inspection using the kernel for optimized performance, or using the HTTP Security Server for strict protocol enforcement. The three options are:

1 Configurations apply to all connections: Perform optimized protocol enforcement
The following HTTP protocol inspection options are enforced by the kernel on all connections (if active): HTTP Format sizes, ASCII Only Request, Header Rejection, and General HTTP Worm Catcher. Note that in this option, the ASCII Only Response Headers protection is not performed. If a connection matches a rule in the Rule Base that activates the Security Server, the Security Server performs these options (if activated).

2 Configurations apply to all connections: Perform strict protocol enforcement
The HTTP protocol inspection options are enforced by the Security Server.

3 Configurations apply only to connections related to resources used in the Rule Base
For connections related to resources used in the Rule Base, the HTTP protocol inspection options are enforced by the Security Server. For all other connections, the options are not enforced.
CHAPTER 15

Web Content Protection

In This Chapter

Introduction to Web Content Protection  page 255
Web Content Security via the Security Rule Base  page 256
Securing XML Web Services (SOAP)  page 258
Understanding HTTP Sessions, Connections and URLs  page 259
Connectivity Versus Security Considerations for Web Surfers  page 261
Factors that Affect HTTP Security Server Performance  page 262
Configuring Web Content Protection  page 264

Introduction to Web Content Protection

This chapter discusses the following Web Security capabilities of VPN-1 Pro:

- Integrated web security capabilities that are configured via the Security Rule Base. These include a number of URL-based protections.
- The ability to secure XML Web Services (SOAP) on Web Servers.

Web Intelligence is an add-on for VPN-1 Pro that provides high performance attack protection for web servers and applications. It provides proactive attack protection by looking for malicious code and ensuring adherence to protocols and security best practice. For details about Web Intelligence, see “Web Intelligence” on page 241.

It is possible to scan HTTP connections for viruses and malicious content using the antivirus scanning capabilities that are integrated into Express CI R57. For details, see “Anti Virus Protection” on page 143.
Web Content Security via OPSEC partners allows network virus protection and URL filtering using best-of-breed Check Point partners. For details, see “CVP and UFP Content Security” on page 215.

Web Content Security via the Security Rule Base

In This Section

- What is a URI Resource? page 256
- Filtering URLs, Schemes and Methods by Source and Destination page 256
- Basic URL Filtering page 257
- URL Logging page 257
- Java and ActiveX Security page 257

VPN-1 Pro provides some web security capabilities that are configured via the Security Rule Base, rather than using Web Intelligence. These include a number of URL-based protections.

What is a URI Resource?

Web security via the Security Rule Base is implemented by defining a SmartDashboard object called a URI Resource, and using it in the Security Rule Base. Resource objects are explained in “Resources: What They Are and How to Use Them” on page 226.

URI stands for Uniform Resource Identifier. A URI is more-or-less identical to the familiar URL (Uniform Resource Locator).

Filtering URLs, Schemes and Methods by Source and Destination

It is possible to block URL based attacks such as Code Red and Nimda using a URI resource. Attacks from and to a specified source and destination can be blocked. HTTP methods (such as GET and POST) and schemes (such as http, ftp, and mailto) can also be blocked.

URL patterns are specified using regular expressions. The URL can be broken into filterable components using the Host, Path and Query parameters that are specified in the Match tab.

For configuration details, see “Blocking URL-based Attacks using a URI Resource” on page 264.
Basic URL Filtering

Basic URL Filtering capability is integrated into VPN-1 Pro. Use this capability to restrict user access to as many as 50 URLs, without having to define a separate resource for each URL.

This method is not recommended for large URL lists, because the list of banned sites must be defined in a file, and then manually edited and maintained, which is difficult for a large list of banned sites.

For configuration details, see “Configuring Basic URL Filtering” on page 265.

More comprehensive URL Filtering is available using third party OPSEC-certified applications.

URL Logging

Normally, a logged connection shows the source or destination Web server and domain (for example http://foo.bar.com).

It is possible to generate extra URL logging information by performing kernel inspection on the HTTP connection, rather than using a URI Resource, which gives a less detailed log. This shows in the log the full path and query of the requested URL, not just the name of the Web server (e.g. http://foo.bar.com/products/servlet/Satellite?pagename=1234). Do this by defining a URI resource and selecting Optimize URL Logging.

For configuration details about logging URLs, either by performing kernel inspection on the HTTP connection, or using a URI Resource, see “Configuring URL Logging” on page 265.

Java and ActiveX Security

VPN-1 Pro is able to protect web surfers by controlling incoming Java and ActiveX code according to specific conditions, such as host, URL, or authenticated user name.

Capabilities of Java and ActiveX screening include the following:

- Stripping ActiveX tags from HTML pages.
- Stripping Java applet tags from HTML pages.
- Blocking Java attacks by blocking suspicious back connections.

More comprehensive scanning of Java, ActiveX and other executables can be accomplished with content security applications from OPSEC certified vendors.
To screen for Java and ActiveX, you need to define a URI resource and add it to a Security Rule Base rule. See “Creating a Resource and Using it in the Rule Base” on page 227.

Securing XML Web Services (SOAP)

VPN-1 Pro provides some web security capabilities that are configured via the Security Rule Base, rather than using Web Intelligence. These include the securing of XML Web Services (SOAP).

XML Web services (using XML Schema and SOAP) allow program-to-program communication, and represent an important new way of communicating using Internet protocols and standards. This is in contrast to Web pages (using HTML and DHTML), which can be used for person-to-program communication, and email and Instant Messaging (using protocols such as SMTP and MIME) which are for person-to-person communication.

The Simple Object Access Protocol (SOAP) provides a way for applications to communicate with each other over the Internet, independent of platform. SOAP relies on XML to define the format of the information and then adds the necessary HTTP headers to send it.

XML passes information using commands called *Methods* that are intended to run on the destination computer.

VPN-1 Pro uses a Security Server to prevent potential attacks by verifying that the HTTP, XML, SOAP methods in SOAP requests conform to the RFC. VPN-1 Pro also checks that only a predefined list of acceptable methods is being passed in the SOAP packet.

The way that VPN-1 Pro treats SOAP packets is defined in a URI resource that uses HTTP. The URI specifies whether a SOAP packet passing though the enforcement point will always be accepted, or only the Methods specified in a predefined file will be accepted.

The SOAP processing defined in the URI resource is performed only if the HTTP connection carrying the SOAP message was already accepted by the rule in which the URI resource is used. In other words, the connection must match the rule, and the rule *Action* cannot be *Reject* or *Drop*.

For configuration details, see the online help in the SOAP tab of the URI Resource.
Understanding HTTP Sessions, Connections and URLs

To understand how to best use VPN-1 Pro web security and Web Intelligence protections, it is important to understand some basic terms and concepts regarding HTTP sessions, HTTP connections, and URLs.

An HTTP session is made up of an HTTP request and an HTTP response. In other words:

\[
\text{HTTP Session} = \text{HTTP Request} + \text{HTTP Response}
\]

Both the HTTP request and the HTTP response have a header section and a body section.

HTTP Request Example

**Header section**

The URL is marked in bold for clarity.

```
GET http://www.site.com/path/file.html?param1=val1&param2=value2 HTTP/1.1
Host: www.site.com
Range: 1000-2000
Cookie: cookiename=A172653987651987361BDEF
```
**HTTP Connections**

HTTP/1.1 encourages the transmission of multiple requests over a single TCP connection. Each request must still be sent in one contiguous message, and a server must send responses (on a given connection) in the order that it received the corresponding requests.

The following is an example of an HTTP request connection:

<table>
<thead>
<tr>
<th>Request # 1</th>
<th>Header section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Post /Hello/ HTTP/1.1</td>
<td>Host: <a href="http://www.walla.co.il">www.walla.co.il</a></td>
</tr>
<tr>
<td>User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT5.0)</td>
<td>Pragma: no-cache</td>
</tr>
<tr>
<td>Content-length: 20</td>
<td>Connection: Keep-alive</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Request #1 - Body</th>
</tr>
</thead>
<tbody>
<tr>
<td>This my example body</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Request # 2</th>
<th>Header section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get /scripts/ HTTP/1.1</td>
<td>Host: <a href="http://www.walla.co.il">www.walla.co.il</a></td>
</tr>
<tr>
<td>User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT5.0)</td>
<td>Pragma: no-cache</td>
</tr>
<tr>
<td>Content-length: 0</td>
<td>Connection: Keep-alive</td>
</tr>
</tbody>
</table>
Understanding URLs

A URL is made up of the **Host**, **Path** and **Query** parameters. In the URL in FIGURE 15-1, the **Host** is http://www.elvis.com, the **Path** is /alive/qc.html, and the **Query** is everything else. VPN-1 Pro and Web intelligence can filter the URL on these parameters and decide whether to allow the HTTP request containing a particular URL.

FIGURE 15-1 Example URL showing Host, Path and Query components

http://www.elvis.com/alive/qc.html?seenon=Mars

Connectivity Versus Security Considerations for Web Surfers

To tune connectivity versus security for web surfers, you need to adjust certain database properties.

Allowing or Restricting Content

**The Content Disposition Header**

The Content-Disposition header in the HTTP Response header suggests to the client a location where the client should save content (such as a file) carried in the HTTP response. This location can potentially point to a crucial OS file on the client. Some clients may take up this suggestion without question and save the content to that location.

By default, the Content-Disposition header is not allowed. To allow it, from the SmartDashboard main menu, select **Policy > Global Properties**, and then **SmartDashboard Customization > Configure**. In the **Advanced Configuration** window, select **FireWall-1 > Web Security > Security**. To allow the Content-Disposition header, check **http_allow_content_disposition**.
Partial Range Requests

Partial range requests allow the content in an HTTP response to be split over more than one response. However, content security checks are only completely effective if the responses are not split in this way.

Adobe Acrobat® uses HTTP ranges to allow pages of Acrobat PDF files to be viewed as soon as they are downloaded. Not allowing ranges means that the whole file must be downloaded before it can be viewed. Some download managers also use HTTP ranges.

Range requests in HTTP requests, and range responses in HTTP responses are not allowed by default. To allow ranges, from the SmartDashboard main menu, select Policy > Global Properties, and then SmartDashboard Customization > Configure. In the Advanced Configuration window, select FireWall-1 > Web Security > Security > Content Security. To allow range request, check http_allow_ranges.

Content Compression

Compressing content in HTTP responses is a way of increasing the speed of the connection. However, content security checks such as HTML weeding and CVP checking cannot be performed on compressed content.

The Content-Encoding and Content-Type headers in the HTTP response indicate whether or not the content is compressed, for example: Content-Encoding: gzip, Content-Type: application/gzip.

The http_disable_content_enc and http_disable_content_type database properties control whether or not to allow data in the HTTP response to be compressed. If these properties are false (the default value), compression of content in an HTTP response is not allowed. Both these properties can be either true or false. One may be true when the other is false. Each one affects it own header.

These properties only affect content on which one or more of the following content security checks are performed: HTML weeding, blocking Java code, CVP, SOAP.

To change the value of this property, in SmartDashboard, edit the Global Properties in the SmartDashboard Customization > Advanced Configuration page, under Web Security.

Factors that Affect HTTP Security Server Performance

On multiple CPU machines, running more than one instance of the HTTP Security Server increases the performance seen by users. This is because each Security Server uses a different CPU. Run at least one Security Server instance for each CPU (see “How To Run Multiple Instances of the HTTP Security Server” on page 263).
It may well be worthwhile to run more than one Security Server even in a single CPU machine, in order to allow more concurrent connections. However, this will increase the memory usage.

**The Number of Simultaneous Security Server Connections**

Each Security Server allows up to 1024 file descriptors, which limits the number of simultaneous connections. In an ordinary connection, packets pass in both directions through the VPN-1 Pro enforcement module, as follows:

1. Web client to VPN-1 Pro to web server (request).
2. Web server to VPN-1 Pro to web client (response).

512 descriptors are available for use in each direction, so that a total of 512 simultaneous connections are possible.

Where a CVP or UFP server is used, packets in each connection pass through VPN-1 Pro three times:

1. Web client to VPN-1 Pro to web server (request).
2. Web server to VPN-1 Pro to CVP/UFP server (response).
3. CVP/UFP server to VPN-1 Pro to web client (response).

Therefore the available file descriptors are split three ways, so that a total of 341 simultaneous connections are possible.

**How To Run Multiple Instances of the HTTP Security Server**

To run multiple instances of the HTTP Security Server:

1. Edit `$FWDIR/conf/fwauthd.conf`, and include the line
   
   ```
   80    in.ahttpd    wait    -2
   ```
   
   The last digit on the line is the number of instances of the Security Server. In this example, there are two instances of the HTTP Security Server.

2. Restart the VPN-1 Pro enforcement module (`cpstart`).
Configuring Web Content Protection

In This Section

- Blocking URL-based Attacks using a URI Resource  page 264
- Configuring URL Logging  page 265
- Configuring Basic URL Filtering  page 265

Blocking URL-based Attacks using a URI Resource

All URL-based attacks such as Code Red and Nimda can be blocked using a URI resource in SmartDashboard. Each resource can block one attack. For background information, see “Securing XML Web Services (SOAP)” on page 258.

Proceed as follows:

1  Create a new URI Resource, and give it a name (such as Alaska.Web.Protection)

2  In the General tab, select
   • Use this resource to: Enforce URI capabilities
   • Connection Methods: Normally Transparent and Proxy are selected
   • URI Match Specification Type: Wild Cards

3  Specify the URL pattern, using regular expressions in the Match tab. For example, to block Code Red, use the following values:
   • Host: *
   • Path: \.ida\?
   • Query: *

4  If you wish to specify a replacement URL to redirect the connection if the pattern is found, specify a Replacement URI in the Action tab.
5 Associate the Resource with the HTTP Service, and place it in a Rule in the Security Rule Base. See the sample rules shown in TABLE 15-1.

**TABLE 15-1 Sample URI Resource in a Rule Base**

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Any</td>
<td>Any</td>
<td>http-&gt;Alaska.Web.Protection</td>
<td>Drop</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Any</td>
<td>http</td>
<td>Accept</td>
</tr>
</tbody>
</table>

The Action in Rule 2 is the opposite of the Action in Rule 1. Rule 2 is required for the **Enforce URI Capabilities** mode. For the **Enhance UFP Performance** mode it is recommended to avoid problems in cases where more than one URI resource is used in the Rule Base.

### Configuring URL Logging

1 Create a URI Resource.

2 Log URL in the connection in one of the following ways:
   - To log the URLs including the URL paths and query, by performing kernel inspection: In the **General** tab of the **URI Resource Properties** window, select **Optimize URL Logging**.
   - For basic URL logging using the Security Server: In the **General** tab of the **URI Resource Properties** window, select **Enforce URI Capabilities**.
     The **Exception Track** option specifies how to track connections that match this rule but fail the content security checks. An example of an exception is a connection with an unsupported scheme or method.

3 Place the URI Resource in a rule with the **Action** **Accept**.

4 Select **Log** in the **Track** column. This logs the URL of all connections that match this rule.

For background information, see “URL Logging” on page 257.

### Configuring Basic URL Filtering

To prevent access to selected forbidden Web sites, proceed as follows:

1 Specify a list of forbidden sites in a file that lists the site URIs. The URI specification file is an ASCII file consisting of a list of lines. Each line has the format:

```
ip-address /path category
```


Configuring Web Content Protection

- **ip-address** is the IP address of the Web server to be matched. Host names can be used, but DNS must be enabled and configured on the VPN-2 Pro gateway.
- **/path** is optional. Use it to restrict a particular directory in a site.
- **category** is an optional parameter that can be any Hex number. It is not currently used.

Make sure there is no white space after the category. The last line in the file must be blank. For example:

```
192.168.56.78   /games
192.168.25.58
```

The file should contain no more than a thousand records.

2. Define a Resource that uses this file.
3. Use this Resource in a Rule, for all HTTP Traffic.
4. Define the Action as **Reject**.

For background information, see “Basic URL Filtering” on page 257.
Appendices

This section describes how the FireWall-1 machine protects itself and the networks behind it upon activation, and the command line interface.
In This Appendix

Achieving Security Before VPN-1 Pro Activation  page 269
Boot Security  page 269
The Initial Policy  page 271
Default Filter and Initial Policy Configuration  page 273

Achieving Security Before VPN-1 Pro Activation

There are several scenarios in which a computer does not yet have a VPN-1 Pro Security Policy installed, and is vulnerable. Two features provide security during these situations: Boot Security, which secures communication during the boot period, and Initial Policy, which provides security before a Security Policy is installed for the first time. As an outcome, there is no instant of time when the computer is left unprotected.

Boot Security

During the boot process, there is a short period of time (measured in seconds) between the point when the computer is capable of receiving communication (and can be attacked) and the point when the Security Policy is loaded and is enforced. During this time, VPN-1 Pro Boot Security feature protects both the internal networks behind the VPN-1 Pro Gateway, and the computer itself. Boot Security is provided by two elements working together:

• Control of IP Forwarding on boot
• The Default Filter
The Default Filter also provides protection in a scenario where VPN-1 Pro processes are stopped for maintenance.

**Control of IP Forwarding on Boot**

For networks protected by a VPN-1 Pro enforcement module, protection is available at boot by disabling IP forwarding in the OS kernel. This ensures that there will never be a time when IP Forwarding is active at a time when no Security Policy is enforced. This ensures that networks behind the gateway are safe.

Disabling IP Forwarding protects networks behind the VPN-1 Pro computer, but it does not protect the VPN-1 Pro computer itself. For this purpose, VPN-1 Pro implements a Default Filter during the period of vulnerability.

**The Default Filter**

The sequence of actions for a VPN-1 Pro Gateway when booting with the Default Filter, is illustrated in **FIGURE A-1:**

- Computer boots up.
- Boot security takes effect (Default Filter loads and IP Forwarding is disabled).
- Interfaces are configured.
- FireWall-1 services start.

The computer is protected as soon as the Default Filter loads.

**FIGURE A-1**  How a Default Filter Protects the VPN-1 Pro Gateway computer

There are five Default Filters:
• General - accepts no inbound communication (this is the default option).
• Drop Filter - accepts no inbound or outbound communication. This filter drops all communications into and out of the gateway during a period of vulnerability. Note, however, that if the boot process requires that the gateway communicate with other hosts, then the Drop Filter should not be used.
• Default Filter for IPSO allowing SSH incoming communication to support remote Administration.
• Default Filter for IPSO allowing HTTPS incoming communication to support remote Administration.
• Default Filter for IPSO allowing SSH and HTTPS incoming communication to support remote Administration.

The appropriate Default Filter should be selected based on platform and communication needs. The general filter is selected by default.

The Default Filter also provides anti-spoofing protection for the VPN-1 Pro Gateway. It makes sure that packets whose source are the VPN-1 Pro Gateway computer itself have not come from one of its interfaces.

**Using the Default Filter for Maintenance**

It is possible to stop VPN-1 Pro processes for maintenance while at the same time protecting the VPN-1 Pro Gateway and the internal network.

During maintenance, the Default Filter allows open connections to the Gateway to remain open, without dropping them.

**The Initial Policy**

Until the VPN-1 Pro administrator installs the Security Policy on the Gateway for the first time, security is enforced by an Initial Policy. The Initial Policy operates by adding “implied rules” to the Default Filter. These rules forbid most of the communication but allows the communication needed for the installation of the Security Policy. The Initial Policy also protects a Gateway during Check Point product upgrades, or when a SIC certificate is reset on the module, or in the case of a Check Point product license expiration.

**Note** - During a Check Point upgrade, a SIC certificate reset, or license expiration, the Initial Policy overwrites the user-defined policy.

The sequence of actions during boot of the VPN-1 Pro Gateway computer until a Security Policy is loaded for the first time, is illustrated in **FIGURE A-2**.
• Computer 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.
• SmartConsole clients connect or Trust is established, and the Security Policy is installed.

**FIGURE A-2** Initial Policy- Until the First Policy Installation

The Initial Policy 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.

There are different Initial Policies for stand-alone and distributed setups. In a stand-alone configuration, where the SmartCenter Server and VPN-1 Pro module are on the same computer, the Initial Policy allows CPMI communication only. This permits SmartConsole clients to connect to the SmartCenter Server.

In a distributed configuration, where the Primary SmartCenter Server is on one computer and the VPN-1 Pro module is on a different computer, the Initial Policy allows the following:
• Primary SmartCenter Server computer — allows CPMI communication for SmartConsole clients.
VPN-1 Pro Gateway — allows cpd and fwd communication for SIC communication (to establish trust) and for Policy installation.

In a distributed configuration, the Initial Policy on the VPN-1 Pro module does not allow CPMI connections. The SmartConsole will not be able to connect to the SmartCenter Server, if the SmartConsole must access the SmartCenter Server through a Gateway running the Initial Policy.

There is also an Initial Policy for a Secondary SmartCenter Server (Management High Availability). This Initial Policy allows CPMI communication for SmartConsole clients and allows cpd and fwd communication for SIC communication (to establish trust) and for Policy installation.

### Default Filter and Initial Policy Configuration

In This Section

- Verifying the Default Filter or Initial Policy is Loaded
- Change the Default Filter to a Drop Filter
- User-Defined Default Filter
- Using the Default Filter for Maintenance
- To Unload a Default Filter or an Initial Policy
- If You Cannot Complete Reboot After Installation
- Command Line Reference for Default Filter and Initial Policy

#### Verifying the Default Filter or Initial Policy is Loaded

You can verify that the Default Filter and/or Initial Policy are indeed loaded as follows:

1. Boot the system.
2. Before installing another Security Policy, type the following command:

   ```bash
   $FWDIR/bin/fw stat
   ```

   The command’s output should show that defaultfilter is installed for the Default Filter status. It should show that InitialPolicy is installed for the Initial Policy.

#### Change the Default Filter to a Drop Filter

For a typical setup there are two Default Filters: defaultfilter.boot and defaultfilter.drop. They are located in $FWDIR/lib.
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 `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.

**User-Defined Default Filter**

For administrators with Inspect knowledge, it is possible to define your own Default Filter as follows:

1 Create an Inspect script named `defaultfilter.pf` in $FWDIR/conf:

   **Warning** - Ensure that the script does not perform any of the following functions:
   - Logging
   - Authentication
   - Encryption
   - Content security

2 Continue as from step 2 of “Change the Default Filter to a Drop Filter” on page 273.”

   You must ensure that your Security Policy does not interfere with the boot process.

**Using the Default Filter for Maintenance**

It is sometimes necessary to stop VPN-1 Pro processes for maintenance, and it is impractical to disconnect the VPN-1 Pro Gateway computer from the network (for example, the computer may be at a remote location). The `cpstop -fwflag -default` and `cpstop -fwflag -proc` commands allow VPN-1 Pro processes to be temporarily stopped for remote maintenance without exposing the computer to attack.
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 an Initial Policy from a remote SmartCenter machine, run the following command on the SmartCenter Server:
  
  ```
  fwm unload <hostname>
  ```

  where `hostname` is the SIC_name of the Module.

If You Cannot Complete Reboot After Installation

In certain configurations the Default Filter may prevent the VPN-1 Pro Gateway computer from completing the reboot following installation.

First, examine the Default Filter and verify that the Default Filter allows traffic that the computer need to boot.

If the boot process cannot complete successfully, 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.

Command Line Reference for Default Filter and Initial Policy

`control_bootsec`

Enables or disables Boot Security. The command affects both the Default Filter and the Initial Policy.
Usage

$FWDIR/bin/control_bootsec [-r] [-g]

TABLE A-1  options control_bootsec

<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>

fwboot bootconf

Use the `fwboot bootconf` command to configure boot security options. This command is located in $FWDIR/boot.

Usage

$FWDIR/bin/fwboot bootconf <command> [value]

TABLE A-2  options fwboot bootconf

<table>
<thead>
<tr>
<th>Options</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| Get_ipf     | Reports whether VPN-1 Pro controls IP Forwarding.
|             | • Returns 1 if IP Forwarding control is enabled on boot. |
|             | • Returns 0 if IP Forwarding is not controlled on boot. |
| Set_ipf 0/1 | Turns off/on control of IP forwarding for the next boot. |
|             | 0 - Turns off |
|             | 1 - Turns on |
| Get_def     | Returns the full path to the Default Filter that will be used on boot. |
| Set_def <filename> | Will load <filename> as the Default Filter in the next boot. The only safe, and recommended, place to put the default.bin file is $FWDIR\boot. (The default.bin filename is a default name.) |
|             | Note - Do NOT move these files |

comp_init_policy

Use the `comp_init_policy` command to generate and load, or to remove, the Initial Policy.
This command generates the Initial Policy. It ensures that it will be loaded when the computer is booted, or any other time that a Policy is fetched, which would also occur at cpstart, or with the fw fetch localhost command. After running this command, cpconfig will add an Initial Policy if there is no previous Policy installed.

**Usage**

```
$FWDIR/bin/comp_init_policy [-u | -g]
```

<table>
<thead>
<tr>
<th>Options</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-u</td>
<td>Removes the current Initial Policy, and ensures that it will not be generated in future when cpconfig is run.</td>
</tr>
<tr>
<td>-g</td>
<td>(Can be used if there is no Initial Policy. If there is, make sure that after removing the policy, you delete the $FWDIR\state\local\FW1\ folder.) Generates the Initial Policy and ensures that it will be loaded the next time a policy is fetched (at cpstart, 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>

The `comp_init_policy -g` command will only work if there is no previous Policy. If there is, make sure that after removing the policy, you delete the folder $FWDIR\state\local\FW1\. The $FWDIR/\state/\local/\FW1/ folder contains the policy that will be fetched when fw fetch localhost is run.

The `fw fetch localhost` command is the command that installs the local policy in cpstart. `comp_init_policy` creates the initial policy, but has a safeguard such that the initial policy will not overwrite a regular user policy (since initial policy is only used for fresh installations or upgrade). For this reason, you must delete the $FWDIR\state\local\FW1\ directory if there is a previous policy, otherwise `comp_init_policy` will detect that there is already a user policy there, and will not overwrite it.

If you do not delete the previous policy, yet perform the following commands ...

```
comp_init_policy -g + fw fetch localhost
comp_init_policy -g + cpstart
comp_init_policy -g + reboot
```

... the original policy will still be loaded.
**cpstop -fwflag -default and cpstop -fwflag -proc**

To stop all VPN-1 Pro processes but leave the Default Filter running, use `cpstop -fwflag -default`. To stop all VPN-1 Pro processes but leave the Security Policy running, use `cpstop -fwflag -proc`.

To stop and start all Check Point processes, use `cpstop` and `cpstart`. These commands should be used with caution.

On Win32 platforms, use the **Services** applet in the **Control Panel** to stop and start Check Point Services.

**Usage**

```
cpstop -fwflag [-default | -proc]
```

**TABLE A-4 Options for fwflag**

<table>
<thead>
<tr>
<th>Options</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-default</td>
<td>Kills VPN-1 Pro processes (fwd, fwm, vpnd, smtpd etc.). Logs, kernel traps, resources, and all security server connections stop working. The Security Policy in the kernel is replaced with the Default Filter.</td>
</tr>
<tr>
<td>-proc</td>
<td>Kills VPN-1 Pro processes (fwd, fwm, vpnd etc.). Logs, kernel traps, resources, and all security server connections stop working. The Security Policy remains loaded in the kernel. Therefore allow/reject/drop rules that do not use resources, but only service, continue working.</td>
</tr>
</tbody>
</table>
FireWall-1 Command Line Interface

The following command line commands relate to FireWall-1 and are documented in the Command Line Interface (CLI) Guide.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>comp_init_policy</td>
<td>Generates and loads (or removes) the Initial Policy.</td>
</tr>
<tr>
<td>fw</td>
<td>The fw commands are used for working with various aspects of FireWall-1. All fw commands are executed on the FireWall-1 enforcement module.</td>
</tr>
<tr>
<td>fw isp_link</td>
<td>Takes down (or up) one of the redundant ISP links.</td>
</tr>
<tr>
<td>fw monitor</td>
<td>A powerful built-in tool to simplify the task of capturing network packets at multiple capture points within the FireWall-1 chain.</td>
</tr>
<tr>
<td>fw tab</td>
<td>View kernel table contents and change the contents of dynamic tables. Static tables cannot be changed.</td>
</tr>
<tr>
<td>fw stat</td>
<td>Displays the content of state tables on the target hosts in various formats. For each host, the default format displays the host name and a list of all tables with their elements.</td>
</tr>
<tr>
<td>fw ver</td>
<td>Displays the VPN-1 and FireWall-1 major and minor version number and build number.</td>
</tr>
<tr>
<td>svr_webupload_config</td>
<td>This utility is used to configure the SmartView Reporter web upload script.</td>
</tr>
</tbody>
</table>
Index

A
Access Control 18
ActiveX 257
Address Translation Rule Base 68
Anti Virus 143
Anti-spoofing
and NAT 72
configuring 30
definition 21
planning considerations 26
SmartDefense
configuration 127
Anti-virus protection
for HTTP 220
for SMTP 228
understanding CVP 220
Architecture of FireWall-1 18

B
Boot Security 269
boot security
default filter 269
IP Forwarding 269, 270, 276

C
CIFS
Configuring protection 210
inspection 209
Code Red 256
Content Security
FTP configuration 213
Performed by Services 25
Content security
Connectivity versus security 261
CVP
chaining 234
for any TCP service 233
for FTP 221
for HTTP 220
for SMTP
configuring 228
Improving performance 230
CVP Load Sharing 234

D
Default Filter 269
Default Security Policy
verifying that it is loaded 273

E
enable_propfind_method 261

F
Fingerprint scrambling
definition 128
FireWall-1
security servers 217
FTP Commands
limiting using resource 212
fw isp_link 94
FW1_clntauth 45
fwauthd.conf 45

H
Hide NAT 66
http_allow_content_disposition 261
http_allow_ranges 261
http_disable_content_enc 262
http_disable_content_type 262

I
Implied Rules
definition 20
when to edit 27
Instant Messaging
SIP-based 156
Internet Service Provider. See ISP
Redundancy
IP addresses, private and public 64
IP Forwarding 270
ISP Redundancy
ClusterXL support 96
configuring 101
deployment, choosing 100
deployments 95
dialup support 96
DNS configuration 102
how it works 92
incoming connections 92
link monitoring 92
link status 94
modes, choosing 100
modes, understanding 91
NAT, Hide 92, 104
NAT, Static 92, 104
need 89
outgoing connections 92
overview 90
script 94
script for DNS server 107
SmartView Status 92
VPN 106

J
Java 257

L
Load agents port property 116
M

Malicious Activity Detection (MAD) 128

N

NAT
anti-spoofing 72
arp commands 73
automatic and manual 68
bidirectional 69
definition 65
disabling in VPNs 75
Hide address 76
Hide NAT 66
Hide, planning for 75
IP pools 74
port translation configuring 80
understanding 71
private and public addresses 64
Rule Base 68
rule match 69
Static NAT 65
static routes 72
Static, planning for 75
understanding automatic 69
Nimda 256

Q

QuickUFP. See UFP
enhancing performance

R

Resource
creating 227
Resources
definition 226
URI resource definition 256
RFC 1918 64
RFC 3261 156
RTP/RTCP 157
Rule Base. See Security Rule Base

S

Security Before VPN-1 Pro Activation 269
Security Rule Base
basic rules 26
elements 20
using X11 in 27
Security Server
FTP 212
how it works 217
HTTP
CVP 220
Improving CVP
performance 221
Sequence verifier 122
Services
DNS 24
SSHv2 23
SSLv3 23
TCPT 24
X11 27
SIP
and NAT 165
logging 160
SIP and SIP_Any services 164
Stateful inspection 156
supported elements 162
supported topologies 162
SmartDefense
architecture 125
DoS attack protection 127
Malicious Activity Detection (MAD) 128
sequence verifier 122
subscription service 124
updating 132
SOAP 258
Stateful Inspection 18
Static NAT 65

U

UFP
enhancing performance-concept 223
enhancing performance-configuration 230
for any TCP service 233
How it works 223
rule match behavior 230
URL Filtering

V

version number
displaying 279
Visitor Mode 24
VoIP
H.323 configuration 185
Handover 157
VPN-1 and FireWall-1 version number
displaying 279

X

X11 service, using in Rule Base 27