

# Firewall

Administration Guide  
Version R70



**© 2003-2009 Check Point Software Technologies Ltd.**

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

**RESTRICTED RIGHTS LEGEND:**

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

**TRADEMARKS:**

Please refer to <http://www.checkpoint.com/copyright.html> for a list of our trademarks

For third party notices, see [http://www.checkpoint.com/3rd\\_party\\_copyright.html](http://www.checkpoint.com/3rd_party_copyright.html).



# Contents

---

Preface	Who Should Use This Guide.....	14
	Summary of Contents.....	15
	Section 1: Network Access .....	15
	Section 2: Connectivity .....	15
	Section 3: CoreXL .....	16
	Section 4: Application Intelligence.....	16
	Section 5: Web Security .....	17
	Section 6: Appendix.....	17
	Related Documentation .....	18
	More Information .....	20
	Feedback .....	21

## Network Access

Chapter 1	<b>Access Control</b>	
	The Need for Access Control .....	26
	Solution for Secure Access Control .....	26
	Access Control at the Network Boundary .....	26
	The Rule Base .....	28
	Example Access Control Rule.....	29
	Rule Base Elements .....	29
	Implied Rules.....	30
	Preventing IP Spoofing .....	31
	Multicast Access Control .....	38
	Cooperative Enforcement.....	42
	End Point Quarantine (EPQ) - Intel(r) AMT .....	44
	Special Considerations for Access Control .....	45
	Spoofing Protection.....	45
	Simplicity .....	45
	Basic Rules .....	46
	Rule Order .....	46
	Topology Considerations: DMZ .....	46
	X11 Service.....	47
	Editing Implied Rules.....	47
	Configuring Access Control .....	48
	Defining Access Control Rules.....	48
	Defining a Basic Access Control Policy.....	49
	Configuring Multicast Access Control .....	50
	Configuring Cooperative Enforcement.....	51

Configuring End Point Quarantine (EPQ) .....	52
Activating EPQ .....	52
Connection Authentication Data .....	53
Quarantine Policy Data .....	54
Encrypting the Password.....	55
Malicious Activity Script and Alert.....	55
Logging Activity .....	57

## Chapter 2

### **Authentication**

The Need for Authentication .....	60
Solution for Authentication .....	60
Introduction to Check Point Authentication .....	60
Authentication Schemes.....	61
Authentication Methods.....	64
Configuring Authentication .....	73
Creating Users and Groups.....	73
Configuring User Authentication.....	76
Configuring Session Authentication .....	77
Configuring Client Authentication .....	80
Configuring Authentication Tracking .....	86
Configuring a Security Gateway to use RADIUS..	87
Granting User Access Using RADIUS Server Groups .....	89
Associating a RADIUS Server with Security Gateway.....	90
Configuring Security Gateway to use SecurID.....	91
Configuring Security Gateway to use TACACS+ .....	92
Configuring Policy for Groups of Windows Users.....	93

# **Connectivity**

## Chapter 3

### **Network Address Translation**

The Need to Conceal IP Addresses .....	98
Check Point Solution for Network Address Translation .....	99
Public and Private IP addresses .....	99
NAT in Check Point Security Gateway .....	100
Static NAT .....	101
Hide NAT .....	102
Automatic and Manual NAT Rules .....	104
Automatic Hide NAT for Internal Networks .....	105
NAT Rule Base .....	106
Bidirectional NAT .....	107
Understanding Automatically Generated Rules.....	108
Port Translation .....	110
NAT and Anti-Spoofing.....	110
Routing Issues.....	110

Disabling NAT in a VPN Tunnel .....	113
Planning Considerations for NAT .....	114
Hide Versus Static .....	114
Automatic Versus Manual Rules .....	114
Choosing the Hide Address in Hide NAT.....	115
Configuring NAT .....	116
General Steps for Configuring NAT .....	116
Basic Configuration (Network Node with Hide NAT) .....	117
Sample Configuration (Static and Hide NAT) .....	119
Sample Configuration (Using Manual Rules for Port Translation) .....	121
Configuring Automatic Hide NAT for Internal Networks.....	122
Advanced NAT Configuration .....	123
Connecting Translated Objects on Different Interfaces.....	123
Internal Communication with Overlapping Addresses.....	123
Security Management Behind NAT .....	128
IP Pool NAT .....	132

## Chapter 4

### **ISP Redundancy**

The Need for ISP Link Redundancy .....	140
Solution for ISP Link Redundancy .....	141
ISP Redundancy Overview .....	141
ISP Redundancy Operational Modes .....	142
Monitoring the ISP Links .....	143
How ISP Redundancy Works .....	143
ISP Redundancy Script .....	146
Manually Changing the Link Status (fw isp_link) .....	146
ISP Redundancy Deployments.....	147
ISP Redundancy and VPNs .....	151
Considerations for ISP Link Redundancy .....	154
Choosing the Deployment .....	154
Choosing the Redundancy Mode.....	154
Configuring ISP Link Redundancy .....	155
Introduction to ISP Link Redundancy Configuration .....	155
Registering the Domain and Obtaining IP Addresses.....	155
DNS Server Configuration for Incoming Connections .....	156
Dialup Link Setup for Incoming Connections .....	157
SmartDashboard Configuration .....	157
Configuring Default Route for ISP Redundancy Gateway .....	160

## Chapter 5

### **ConnectControl - Server Load Balancing**

The Need for Server Load Balancing .....	162
ConnectControl Solution for Server Load Balancing .....	163
Introduction to ConnectControl.....	163
Load-Balancing Methods .....	164
ConnectControl Packet Flow.....	165
Logical Server Types .....	166
Persistent Server Mode.....	169
Server Availability .....	171

Load Measuring .....	171
Configuring ConnectControl .....	172

## Chapter 6

### **Bridge Mode**

Introduction to Bridge Mode .....	176
Limitations in Bridge Mode.....	177
Configuring Bridge Mode .....	178
Bridging Interfaces .....	178
Configuring Anti-Spoofing.....	178
Displaying the Bridge Configuration.....	179

# **CoreXL**

## Chapter 7

### **CoreXL Administration**

Introduction to CoreXL .....	184
Supported Platforms and Features.....	185
Default Configuration .....	185
Performance Tuning.....	186
Processing Core Allocation.....	186
Allocating Processing Cores .....	187
Configuring CoreXL .....	192
Command Line Reference.....	193
Affinity Settings.....	193
fwaffinity.conf .....	194
fwaffinity_apply .....	195
fw ctl affinity.....	195
fw ctl multik stat .....	198

# **Application Intelligence**

## Chapter 8

### **Anti-Virus and URL Filtering**

Anti-Virus Protection .....	202
Introduction to Integrated Anti-Virus Protection .....	202
Architecture .....	203
Configuring Integrated Anti-Virus Scanning .....	203
Database Updates.....	204
Understanding Scan By Direction and Scan By IP .....	205
Scanning by Direction: Selecting Data to Scan .....	209
File Type Recognition.....	211

	Continuous Download .....	212
	Logging and Monitoring .....	213
	File Size Limitations and Scanning.....	214
	UTM-1 Edge Anti-Virus.....	216
	URL Filtering .....	217
	Introduction to URL Filtering .....	217
	Terminology .....	218
	Architecture .....	218
	Configuring URL Filtering .....	219
Chapter 9	<b>Anti-Spam and Mail</b>	
	Introduction to Anti-Spam and Mail Security .....	222
	Mail Management .....	224
	Mail Security Overview .....	224
	Configuring Anti-Spam .....	228
	Configuring Anti-Virus .....	234
	Logging and Monitoring .....	237
	Reporting False Positives to Check Point.....	237
	Tracking and Reporting Options .....	239
	SmartView Tracker .....	239
	SmartView Monitor.....	239
	Eventia Reporter .....	239
	MIB .....	239
Chapter 10	<b>Securing Voice Over IP</b>	
	The Need to Secure Voice Over IP .....	242
	Introduction to the Check Point Solution for Secure VoIP.....	243
	Control Signalling and Media Protocols .....	244
	VoIP Handover.....	245
	VoIP Application Intelligence .....	247
	Introduction to VoIP Application Intelligence .....	247
	Restricting Handover Locations Using a VoIP Domain.....	248
	Controlling Signalling and Media Connections .....	249
	Preventing Denial of Service Attacks.....	249
	Protocol-Specific Application Intelligence .....	250
	VoIP Logging .....	251
	Protocol-Specific Security.....	252
	Securing SIP-Based VoIP .....	252
	Securing H.323-Based VoIP .....	270
	Configuring H.323-Based VoIP .....	278
	Securing MGCP-Based VoIP .....	294
	Securing SCCP-Based VoIP.....	302
Chapter 11	<b>Securing Instant Messaging Applications</b>	
	The Need to Secure Instant Messenger Applications.....	310
	Introduction to Instant Messenger Security.....	311
	Understanding Instant Messenger Security .....	312

	NAT Support for MSN Messenger over SIP .....	313
	NAT Support for MSN Messenger over MSNMS .....	314
	Logging Instant Messenger Applications.....	314
	Configuring SIP-based Instant Messengers .....	315
	Configuring MSN Messenger over MSNMS .....	317
	Configuring Skype, Yahoo, ICQ and More .....	318
<b>Chapter 12</b>	<b>Microsoft Networking Services Security</b>	
	Securing Microsoft Networking Services (CIFS).....	320
	Restricting Access to Servers and Shares (CIFS Resource) .....	321
<b>Chapter 13</b>	<b>FTP Security</b>	
	Introduction to FTP Content Security .....	324
	FTP Enforcement by the Firewall Kernel .....	324
	FTP Enforcement by the FTP Security Server.....	325
	Control Allowed Protocol Commands.....	325
	Maintaining Integrity of Other Protected Services.....	325
	Avoiding Vulnerabilities in FTP Applications .....	325
	Content Security via the FTP Resource.....	325
	Configuring Restricted Access to Specific Directories .....	326
<b>Chapter 14</b>	<b>Content Security</b>	
	The Need for Content Security .....	330
	Check Point Solution for Content Security.....	331
	Introduction to Content Security.....	331
	Security Servers.....	332
	Deploying OPSEC Servers .....	333
	CVP Servers for Anti-Virus and Malicious Content Protection .....	335
	Using URL Filtering to Limit Web Surfers.....	338
	TCP Security Server .....	342
	Configuring Content Security .....	343
	Resources: What They Are and How to Use Them.....	343
	Creating a Resource and Using it in the Rule Base.....	344
	Configuring Anti-Virus Checking for Incoming Email.....	345
	Configuring CVP for Web Traffic Performance .....	347
	Configuring URL Filtering with a UFP Server .....	348
	Performing CVP/UFP Inspection on any TCP Service.....	351
	Advanced CVP Configuration: CVP Chaining and Load Sharing .....	352
	Introduction to CVP Chaining and Load Sharing.....	352
	CVP Chaining .....	352
	CVP Load Sharing .....	354
	Combining CVP Chaining and Load Sharing.....	355
	Configuring CVP Chaining and Load Sharing.....	355
<b>Chapter 15</b>	<b>Services with Application Intelligence</b>	
	Introduction to Services with Application Intelligence.....	358
	DCE-RPC .....	358

SSLv3 Service .....	359
SSHv2 Service .....	359
FTP_BASIC Protocol Type.....	359
Domain_UDP Service .....	360
Point-to-Point Tunneling Protocol (PPTP).....	361
Configuring PPTP .....	361
Blocking Visitor Mode (TCPT).....	363
Introduction to TCPT .....	363
Why Block Visitor Mode and Outgoing TCPT?.....	363
How the Firewall Identifies TCPT.....	363
When to Block Outgoing TCPT.....	363
Blocking Visitor Mode (Blocking Outgoing TCPT).....	364
Changing the Port Used to Block Outgoing TCPT.....	364

# Web Security

## Chapter 16

### Web Content Protection

Introduction to Web Content Protection.....	368
Web Content Security in the Rule Base.....	369
What is a URI Resource? .....	369
Filtering URLs .....	369
Basic URL Filtering.....	370
URL Logging .....	370
Java and ActiveX Security .....	371
Securing XML Web Services (SOAP) .....	372
Understanding HTTP Sessions, Connections and URLs.....	373
HTTP Request Example.....	373
HTTP Response Example.....	374
HTTP Connections .....	374
Understanding URLs .....	375
Connectivity or Security: Web Surfers .....	376
Allowing or Restricting Content .....	376
Content Compression .....	377
HTTP Security Server Performance .....	378
Simultaneous Security Server Connections .....	378
Running Multiple Instances of HTTP Security Server.....	379
Configuring Web Content Protection .....	380
Blocking URL-Based Attacks Using URI Resources .....	380
Configuring URL Logging.....	381
Configuring Basic URL Filtering .....	381

# **Appendices**

## **Appendix A**

### **Security Before Firewall Activation**

Achieving Security Before Firewall Activation .....	386
Boot Security .....	386
Control of IP Forwarding on Boot .....	386
The Default Filter .....	387
Changing the Default Filter to a Drop Filter .....	388
Defining a Custom Default Filter .....	389
Using the Default Filter for Maintenance.....	389
The Initial Policy .....	390
Managing Default Filter and Initial Policy.....	393
Verifying Default Filter or Initial Policy Loading .....	393
Unloading Default Filter or Initial Policy.....	393
Troubleshooting: Cannot Complete Reboot .....	394
Command Line Reference.....	394

## **Appendix B**

### **Command Line Interface**

# Preface

---

## In This Chapter

Who Should Use This Guide	page 14
Summary of Contents	page 15
Related Documentation	page 18
More Information	page 20
Feedback	page 21

---

# Who Should Use This Guide

This guide is intended for administrators responsible for maintaining network security within an enterprise, including policy management and user support.

This guide assumes a basic understanding of the following:

- System administration
- The underlying operating system
- Internet protocols (for example, IP, TCP and UDP)

---

# Summary of Contents

This guide describes the firewall components of Check Point Security Gateway. It contains the following sections and chapters.

## Section 1: Network Access

This section describes how to secure the networks behind the Check Point Security Gateway by allowing only permitted users and resources to access protected networks.

Chapter	Description
<a href="#">Chapter 1, “Access Control”</a>	Describes how to set up a security policy to fit organizational requirements.
<a href="#">Chapter 2, “Authentication”</a>	Describes authentication schemes and methods.

## Section 2: Connectivity

This section describes how to give internal users and resources unrestricted yet secure connectivity across the gateway.

Chapter	Description
<a href="#">Chapter 3, “Network Address Translation”</a>	Describes the Network Address Translation (NAT) process, used for both security and administrative.
<a href="#">Chapter 4, “ISP Redundancy”</a>	Describes the ISP Redundancy feature, for reliable Internet connectivity by allowing a Check Point Security Gateway to connect with redundant Internet Service Provider (ISP) links.
<a href="#">Chapter 5, “ConnectControl - Server Load Balancing”</a>	Describes the ConnectControl server load balancing solution to reduce loads on each machine, improve network response time and ensure high availability.
<a href="#">Chapter 6, “Bridge Mode”</a>	Describes the Firewall Bridge Mode, for the placement of a firewall without changing the existing IP routing.

---

## Section 3: CoreXL

This section provides an overview of CoreXL, a firewall component which enables customers to take advantage of multi-core processors.

Chapter	Description
<a href="#">Chapter 7, "CoreXL Administration"</a>	Describes configuration and management of CoreXL.

## Section 4: Application Intelligence

This section describes Check Point Application Intelligence features that detect and prevent application-level attacks. The chapters in this section describe how to protect against application-level attacks for each application protocol, and how to work with Anti-Virus (CVP) and URL filtering (UFP) applications.

Chapter	Description
<a href="#">Chapter 8, "Anti-Virus and URL Filtering"</a>	Describes Check Point Security Gateway Content Inspection gateways with integrated Anti-Virus technology.
<a href="#">Chapter 9, "Anti-Spam and Mail"</a>	Describes how to manage Anti-Spam and other email features.
<a href="#">Chapter 10, "Securing Voice Over IP"</a>	Describes how to secure VoIP traffic in H.323, SIP, MGCP and SCCP environments.
<a href="#">Chapter 11, "Securing Instant Messaging Applications"</a>	Describes how to secure SIP-based Instant Messenger and MSN Messenger applications.
<a href="#">Chapter 12, "Microsoft Networking Services Security"</a>	Describes how to secure Microsoft Networking (CIFS) Services.
<a href="#">Chapter 13, "FTP Security"</a>	Describes FTP content security and restricted access to specific directories.
<a href="#">Chapter 14, "Content Security"</a>	Describes how to integrate with third party OPSEC-certified antivirus and URL filtering applications.
<a href="#">Chapter 15, "Services with Application Intelligence"</a>	Describes how to configure protection for predefined TCP services that perform content inspection.

---

## Section 5: Web Security

This section describes the firewall web inspection and content security features, which provide high performance attack protection for Web servers, applications, and content.

Chapter	Description
<a href="#">Chapter 16, "Web Content Protection"</a>	Describes the Web security capabilities and how to secure XML Web Services (SOAP) on Web servers.

## Section 6: Appendix

This section describes how a Check Point Security Gateway protects itself and its networks during activation and provides a summary of its command line interface commands.

Appendix	Description
<a href="#">Appendix A, "Security Before Firewall Activation"</a>	Describes the Boot Security and Initial Policy features, used when a computer does not yet have a Security Gateway policy installed.
<a href="#">Appendix B, "Command Line Interface"</a>	Describes command line interface of Security Gateway firewall components.

---

# Related Documentation

This release includes the following related documentation:

**TABLE P-1** Check Point Documentation

Title	Description
<b>Internet Security Installation and Upgrade Guide</b>	Contains detailed installation instructions for Check Point network security products. Explains the available upgrade paths from versions R60 to the current version.
<b>High-End Installation and Upgrade Guide</b>	Contains detailed installation instructions for the Provider-1 and VSX products, including hardware and software requirements and licensing requirements. Explains all upgrade paths for Check Point products specifically geared towards upgrading to the current version.
<b>Security Management Administration Guide</b>	Explains Security Management solutions. This guide provides solutions for control over configuring, managing, and monitoring security deployments.
<b>Firewall Administration Guide</b>	Describes how to control and secure network access and VoIP traffic; how to use integrated web security capabilities; and how to optimize Application Intelligence with capabilities such as Content Vectoring Protocol (CVP) applications, URL Filtering (UFP) applications.
<b>IPS Administration Guide</b>	Describes how to use IPS to protect against attacks.
<b>Virtual Private Networks Administration Guide</b>	Describes the basic components of a VPN and provides the background for the technology that comprises the VPN infrastructure.

---

**TABLE P-1** Check Point Documentation (Continued)

Title	Description
<b>Eventia Reporter Administration Guide</b>	Explains how to monitor and audit traffic, and generate detailed or summarized reports in the format of your choice (list, vertical bar, pie chart etc.) for all events logged by Check Point Security Gateways, SecureClient and IPS.
<b>SecurePlatform/ SecurePlatform Pro Administration Guide</b>	Explains how to install and configure SecurePlatform. This guide will also teach you how to manage your SecurePlatform machine and explains Dynamic Routing (Unicast and Multicast) protocols.
<b>Provider-1/SiteManager-1 Administration Guide</b>	Explains the Provider-1 security management solution. This guide provides details about a three-tier, multi-policy management architecture and a host of Network Operating Center oriented features that automate time-consuming repetitive tasks common in Network Operating Center environments.

---

## More Information

- For additional technical information about Check Point products, consult Check Point's SecureKnowledge at <http://support.checkpoint.com>.
- To view the latest version of this document in the Check Point User Center, go to: <http://support.checkpoint.com>.

---

# **Feedback**

Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments to:

[cp\\_techpub\\_feedback@checkpoint.com](mailto:cp_techpub_feedback@checkpoint.com)



# **Network Access**

This section describes how to secure the networks behind the Check Point Security Gateway by allowing only permitted users and resources to access protected networks.



# Chapter

# Access Control

## In This Chapter

The Need for Access Control	page 26
Solution for Secure Access Control	page 26
Special Considerations for Access Control	page 45
Configuring Access Control	page 48

# The Need for Access Control

Network administrators 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 responsibility of authorization, or Access Control. Determining who can access these resources is the responsibility of User Authentication.

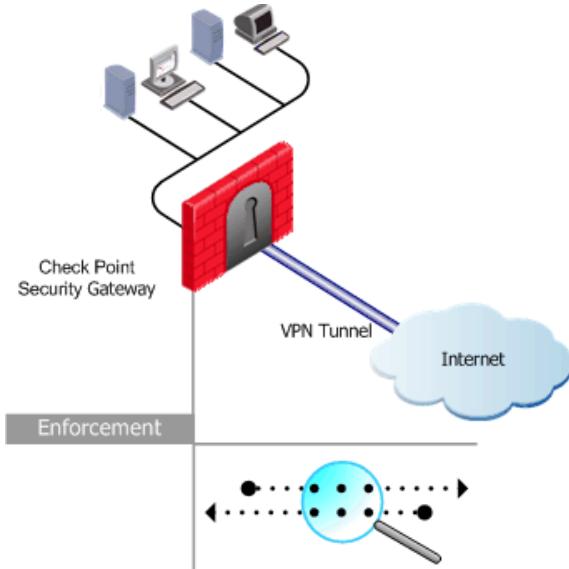
# Solution for Secure Access Control

## In This Section

Access Control at the Network Boundary	page 26
The Rule Base	page 28
Example Access Control Rule	page 29
Rule Base Elements	page 29
Implied Rules	page 30
Preventing IP Spoofing	page 31
Multicast Access Control	page 38
Cooperative Enforcement	page 42
End Point Quarantine (EPQ) - Intel(r) AMT	page 44

## Access Control at the Network Boundary

A Check Point Security Gateway at the network boundary inspects and provides access control for all gateway traffic. Traffic that does not pass through the gateway is not controlled.

**Figure 1-1** Security Gateway Traffic Inspection at the Network Boundary

A security administrator is responsible for implementing company security policy. Check Point Security Gateway allows administrators to enforce security policies consistently across multiple gateways. To do this, the administrator defines a company-wide security policy Rule Base using SmartDashboard and installs it to the Security Management server. SmartDashboard is a SmartConsole client application that administrators use to define and apply security policies to gateways. Granular security policy control is possible by applying specific rules to specific gateways.

Check Point Security Gateway provides secure access control because of its granular understanding of all underlying services and applications traveling on the network. Stateful Inspection technology provides full application level awareness and comprehensive access control for more than 150 predefined 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 levels and maintains this information in dynamic state tables that are used to evaluate subsequent connection attempts. For additional technical information on Stateful Inspection, refer to the Check Point Technical Note at: [http://www.checkpoint.com/products/downloads/firewall-1\\_statefulinspection.pdf](http://www.checkpoint.com/products/downloads/firewall-1_statefulinspection.pdf)

## The Rule Base

A security policy is implemented by means of ordered set of rules in the security Rule Base. A well defined security policy is essential to an effective security solution.

The fundamental principle of the Rule Base is that all actions that are not explicitly permitted are prohibited. The Rule Base is a collection of rules that determine which communication traffic is permitted and which is blocked. Rule parameters include the source and destination of the communication, the services and protocols that can be used and at what times, and tracking options. Reviewing SmartView Tracker traffic logs and alerts is an crucial aspect of security management.

Check Point Security Gateway inspects packets in a sequential manner. After the Security Gateway receives a packet from a connection, the gateway inspects the packet according to the first rule in the Rule Base, and then the second and so on. When the gateway finds an applicable rule, it stops inspecting and applies that rule to the packet. If no applicable rule is found in the Rule Base, the packet is blocked. It is important to understand that the **first** matching rule applies to the packet, not necessarily the rule that best applies.

## Example Access Control Rule

[Figure 1-2](#) displays a typical access control rule, as seen in the Firewall tab of SmartDashboard. This rule states that HTTP connections that originate from any of the Alaska\_LAN group hosts, and directed to any destination, will be accepted and logged.

**Figure 1-2** Example Access Control Rule

SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
Alaska_LAN	* Any	Any Traffic	http	accept	Log	* Policy Targets	* Any

## Rule Base Elements

A rule is made up of the following Rule Base elements (not all fields are relevant in a given rule):

**Table 1-1** Rule Base Elements

<b>Source and Destination</b>	Refers to the originator and recipient of the connection. For applications that work in the client server model, the source is the client and the destination is the server. Once a connection is allowed, packets in the connection pass freely in both directions.  You can negate source and destination parameters, which means that a given rule applies to all connection sources/destinations <b>except</b> the specified location. You may, for example, find it more convenient to specify that the a rule applies to any source that is <b>not</b> in a given network To negate a connection source or destination, right click on the appropriate rule cell and select Negate Cell from the options menu.
<b>VPN</b>	Allows you to configure whether the rule applies to any connection (encrypted or clear) or only to VPN connections. To limit a rule to VPN connections, double-click on the rule and select one of the two VPN options.
<b>Service</b>	Allows you to apply a rule to specific predefined protocols or services or applications. You can define new, custom services.
<b>Action</b>	Determines whether a packet is accepted, rejected, or dropped. If a connection is rejected, the firewall sends an RST packet to the originator of the connection and the connection is closed. If a packet is dropped, no response is sent and the connection eventually times out. (For information on actions that relate to authentication, see <a href="#">Chapter 2, “Authentication”</a> .)

**Table 1-1** Rule Base Elements (Continued)

<b>Track</b>	Provides various logging options (see the <i>Security Management Server Administration Guide</i> ).
<b>Install-On</b>	Specifies the Security Gateway on which the rule is installed. There may be no need to enforce certain rules on every Security Gateway. For example, a rule may allow certain network services to cross only one particular gateway. In this case, the specific rule need not be installed on other gateways (see the <i>Security Management Server Administration Guide</i> .)
<b>Time</b>	Specifies the days and the time of day to enforce this rule.

## Implied Rules

Apart from those rules defined by an administrator, the Security Gateway also creates implied rules, which are derived from the Policy > Global Properties definitions. Implied rules enable certain connections to occur to and from the gateway using a variety of different services. Examples of implied rules include rules that enable Security Gateway control connections and outgoing packets originating from the Security Gateway.

Firewall implied rules are placed first, last, or before last in the Rule Base and can be logged. Implied rules are processed in the following order:

1. **First:** This rule cannot be modified or overwritten in the Rule Base because the first rule that matches is always applied to the packet and no rules can be placed before it.
2. **Explicit:** These are the administrator-defined rules, which may be located between the first and the before last rules.
3. **Before Last:** These are more specific rules that are enforced before the last rule is applied.
4. **Rule n:** The last defined rule.
5. **Last:** A rule that is enforced after the last rule in the Rule Base, which normally rejects all packets and has no effect.
6. **Implicit Drop Rule:** No logging occurs.

To see implied rules:

1. Add at least one rule to the rule base.
2. Click **View > Implied Rules**.

The Firewall tab displays the Implied Rules in addition to the user-defined rules.

## Preventing IP Spoofing

IP spoofing occurs when an intruder attempts to gain unauthorized access by changing a packet's IP address to appear as though it originated from network node with higher access privileges.

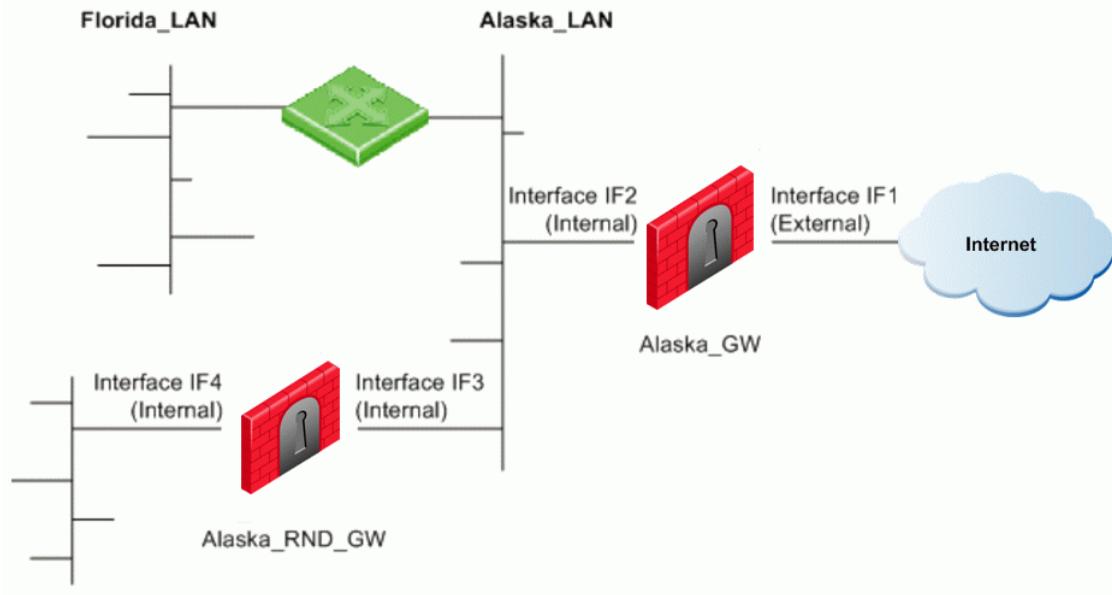


**Note** - It is important to ensure that all communication originates from its apparent source.

Anti-spoofing protection verifies that packets originate from and are destined to the correct interfaces on the gateway. It confirms which packets actually come from the specified internal network interface. It also verifies that once a packet is routed, it goes through the proper interface.

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

**Figure 1-3** Anti-Spoofing Process



#### **Alaska\_RND\_LAN**

On Alaska\_GW, the firewall ensures 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, the firewall ensures that:

- All incoming packets to interface IF3 come from Alaska\_LAN, Florida\_LAN or the Internet.
- All incoming packets to interface IF4 come from Alaska\_RND\_LAN.

When configuring anti-spoofing, you need to specify in the interface topology definitions whether the interfaces lead to the Internet (defined as External) or an internal network (defined as Internal).

## ***Excluding Specific Internal Addresses***

In some cases, it may be necessary to allow packets with source addresses that belong to an internal network to enter the gateway through an external interface. This may be useful if an external application assigns internal IP addresses to external clients. In this case, you can specify that anti-spoofing checks are not made on packets from specified internal networks.

## ***Legal Addresses***

Legal addresses are those addresses that are permitted to enter a Security Gateway interface. Legal addresses are determined by the network topology. When configuring the firewall anti-spoofing protection, the administrator specifies the legal IP addresses behind the interface. The **Get Interfaces with Topology** option automatically defines the interface and its topology and creates network objects. the firewall obtains this information by reading routing table entries.

## ***Configuring Anti-Spoofing***

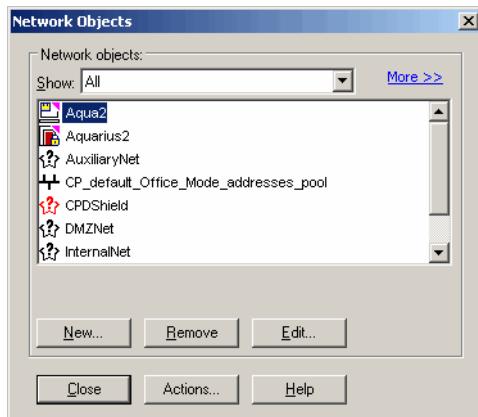
It is important to configure anti-spoofing protection on every interface of every Security Gateway, including internal interfaces.

### **Configuring Anti-Spoofing for External Interfaces**

To define a valid address for external interfaces:

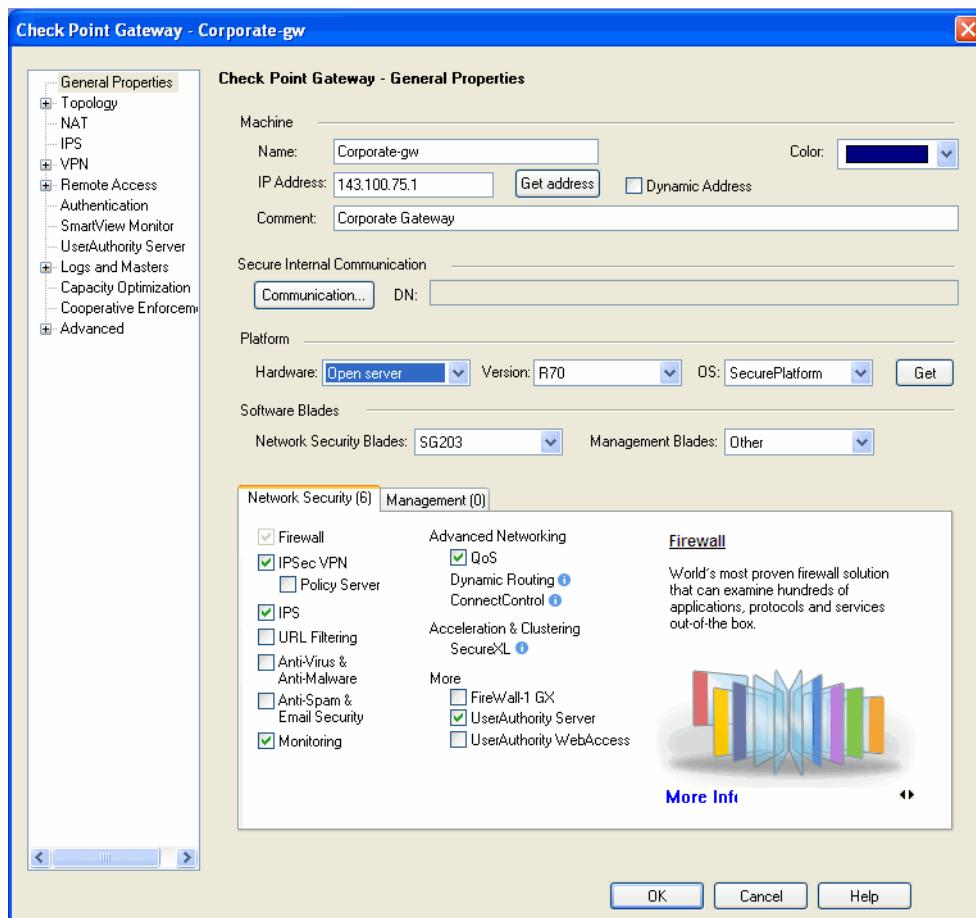
1. In SmartDashboard, select **Manage > Network Objects**.

**Figure 1-4** Network Objects Window



2. Select a gateway and click **Edit**.

Figure 1-5 Check Point Gateway General Properties



3. From the list of pages, click **Topology**.

**Figure 1-6** Check Point Gateway Topology Page in Gateway Window

Name	IP Address	Network Mask	Topology
eth0	143.100.75.1	255.255.255.0	External
eth1	172.16.2.1	255.255.255.0	This Network
eth2	172.16.1.1	255.255.255.0	Undefined
eth3	10.1.0.1	255.255.255.0	This Network
eth4	10.2.0.1	255.255.255.0	This Network
eth5	10.3.0.1	255.255.255.0	This Network

Note: IPv6 address configuration is available in each interface's edit dialog box.

Add... Edit... Remove Show...

**VPN Domain**

All IP Addresses behind Gateway based on Topology information.

Manually defined

Show VPN Domain

Set domain for Remote Access Community ...

4. Click **Get > Interfaces** to obtain interface information of the gateway machine.

**Figure 1-7** Get Topology Results

Name	IP Address	Network Mask
eth0	192.168.1.166	255.255.255.0

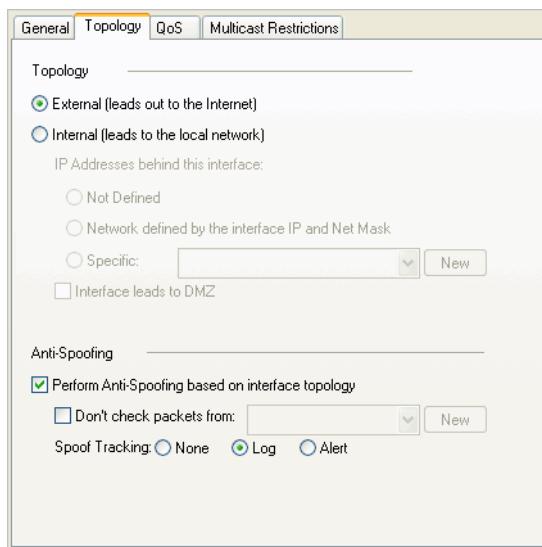
Accept Cancel Help

5. Click **Accept**.

If SmartDashboard could not retrieve the topology information, check that the General Properties of the gateway are listed correctly and that the gateway, the Security Management server, and the SmartDashboard all have functioning communications.

6. In the **Topology** page, select the interface to the Internet and click **Edit**.

**Figure 1-8** Internet Properties Window



7. In the **Interface Properties** window, open the **Topology** tab.
8. Select **External (leads out to the Internet)**.
9. Select **Perform Anti-Spoofing based on interface topology**.  
To ensure that anti-spoofing verification does not occur for addresses coming from internal networks into the external interface, in the next step, define a network object that represents those internal networks.
10. Select **Don't check packets from** and then select the network object from the drop-down list.  
If the network object that you need is not in the list, click **New** and define the Internal Network object that you need.
11. In the **Spoof Tracking** option, select **Log** and then click **OK**.

## Configuring Anti-Spoofing for Internal Interfaces

To define a valid address for internal interfaces:

1. In SmartDashboard, select **Manage > Network Objects**.
2. Select the Check Point gateway and click **Edit**.
3. In the gateway window, select **Topology**.
4. In the Topology window, click **Get > Interfaces** to obtain interface information of the gateway machine.
5. Under the **Name** column, select the internal interface and click **Edit**.
6. In the **Interface Properties** window, click **Topology**, and then select **Internal (leads to the local network)**.
7. Under **IP Addresses behind this interface**, do one of the following:
  - If there is only one network behind the interface, select **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 consists of all the networks behind the interface by selecting **Specific** and the group.
8. To verify **Perform Anti-Spoofing based on interface topology**, under **Spoof Tracking**, select **Log** and click **OK**.
9. Repeat [step 1](#) to [step 8](#) for all internal interfaces.
10. Install the security policy: **Policy > Install**.

For additional information on anti-spoofing protection planning, refer to “[Spoofing Protection](#)” on page 45.

# Multicast Access Control

## In This Section

<a href="#">Introduction to Multicast IP</a>	page 38
<a href="#">Multicast Routing Protocols</a>	page 38
<a href="#">Dynamic Registration Using IGMP</a>	page 39
<a href="#">IP Multicast Group Addressing</a>	page 39
<a href="#">Per-Interface Multicast Restrictions</a>	page 40

## ***Introduction to Multicast IP***

Multicast IP transmits a single message to a predefined group of recipients. an example of this is distributing real-time audio and video to a set of hosts that have joined a distributed conference.

Multicast is similar to radio and TV where only those people who have tuned their tuners to a selected frequency receive the information. With multicast you hear the channel you are interested in, but not the others.

IP multicasting applications send one copy of each datagram (IP packet) and address it to a group of computers that want to receive it. This technique sends datagrams to a group of recipients (at the multicast address) rather than to a single recipient (at a unicast address). The routers in the network forward the datagrams to only those routers and hosts that want to receive them.

The Internet Engineering Task Force (IETF) has developed multicast communication standards that define:

- Multicast routing protocols
- Dynamic registration
- IP multicast group addressing

## ***Multicast Routing Protocols***

Multicast routing protocols communicate information between multicast groups. Examples of multicast routing protocols include Protocol-Independent Multicast (PIM), Distance Vector Multicast Routing Protocol (DVMRP), and Multicast Extensions to OSPF (MOSPF).

## Dynamic Registration Using IGMP

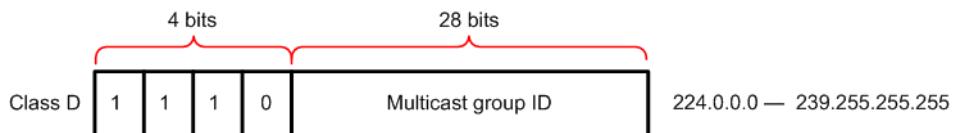
Hosts use the Internet Group Management Protocol (IGMP) to let the nearest multicast router know if they want to belong to a particular multicast group. Hosts can leave or join the group at any time. IGMP is defined in RFC 1112.

## IP Multicast Group Addressing

The IP address area has four sections: Class A, Class B, Class C, and Class D. Class A, B, and C addresses are used for unicast traffic. Class D addresses are reserved for multicast traffic and are allocated dynamically.

The multicast address range 224.0.0.0 through 239.255.255.255 is used only for the group address or destination address of IP multicast traffic. Every IP datagram whose destination address starts with 1110 is an IP multicast datagram ([Figure 1-9](#)).

**Figure 1-9** Multicast Address Range



Just as a radio is tuned to receive a program that is transmitted at a certain frequency, a host interface can be tuned to receive datagrams sent to a specific multicast group. This process is called joining a multicast group.

The remaining 28 bits of the multi-case address range identify the multicast group to which the datagram is sent. Membership in a multicast group is dynamic (hosts can join and leave multicast groups). The source address for multicast datagrams is always the unicast source address.

## Reserved Local Addresses

Multicast group addresses in the 224.0.0.0 through 224.0.0.255 range are assigned by the Internet Assigned Numbers Authority (IANA) for applications that are never forwarded by a router (they remain local on a particular LAN segment).

These addresses are called permanent host groups. [Table 1-2](#) provides examples of reserved Local Network Multicast Groups.

**Table 1-2** Local Network Multicast Groups Examples

Multicast Address	Purpose
224.0.0.1	All hosts. An ICMP Request (ping) sent to this group should be answered by all multicast capable hosts on the network. Every multicast capable host must join this group at start up on all of its multicast capable interfaces.
224.0.0.2	All routers. All multicast routers must join this group on all of its multicast capable interfaces.
224.0.0.4	All DVMRP routers.
224.0.0.5	All OSPF routers.
224.0.0.13	All PIM routers.

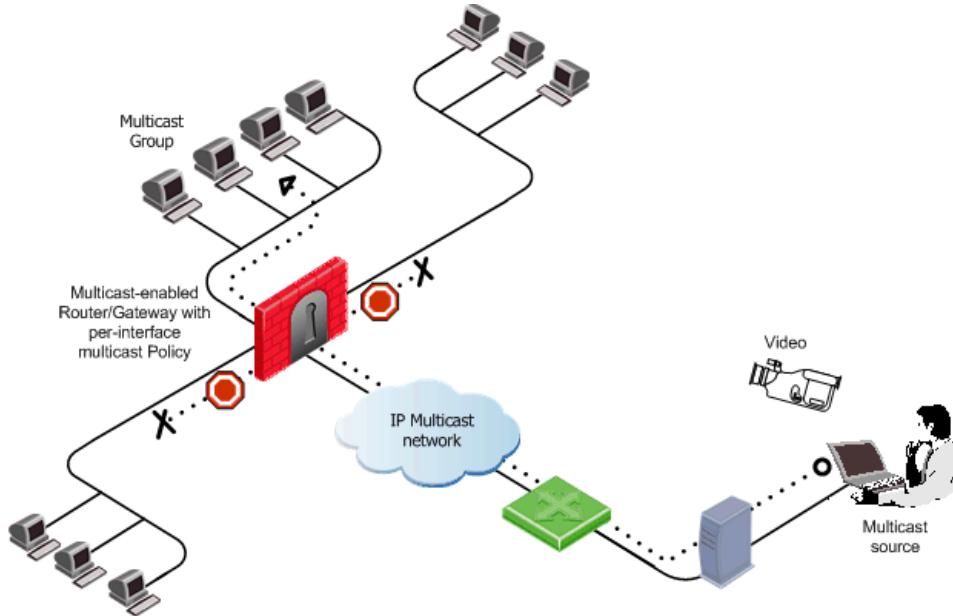
For additional information on reserved multicast addresses, refer to:

<http://www.iana.org/assignments/multicast-addresses>.

## ***Per-Interface Multicast Restrictions***

A multicast enabled router forwards multicast datagrams from one interface to another. When you enable multicast on a Security Gateway running on SecurePlatform, you can define multicast access restrictions on each interface. These restrictions specify which multicast groups (addresses or address ranges) to allow or to block. Enforcement is performed on outbound multicast datagrams.

When access is denied to a multicast group on an interface for outbound IGMP packets, inbound packets are also denied.

**Figure 1-10** Gateway with Per Interface Multicast Restrictions

When access restrictions for multicast datagrams are not defined, inbound multicast datagrams entering a gateway from one interface are allowed out of all other interfaces.

In addition to defining per interface access restrictions, you must define a rule in the Rule Base that allows multicast traffic and services, and the destination defined in this rule must allow the required multicast groups.

See also “[Configuring Multicast Access Control](#)” on page 50.

## VPN Connections

Multicast traffic can be encrypted and sent across VPN links defined using multiple VPN tunnel interfaces (virtual interfaces associated with the same physical interface).

## Cooperative Enforcement

Cooperative Enforcement works with Check Point Endpoint Security servers. This feature utilizes the Endpoint Security server compliance capability to verify connections arriving from various hosts across the internal network.

Endpoint Security server is a centrally managed, multi-layered endpoint security solution that employs policy-based security enforcement for internal and remote PCs. Easily deployed and managed, the Endpoint Security server mitigates the risk of hackers, worms, spyware, and other security threats.

Features such as predefined policy templates, an intuitive Web-based management interface, and PC firewall and application privilege controls, enable administrators to develop, manage, and enforce Cooperative Enforcement quickly and easily.

Using Cooperative Enforcement, any host initiating a connection through a gateway is tested for compliance. This increases the integrity of the network because it prevents hosts with malicious software components from accessing the network.

This feature acts as a middle-man between hosts managed by an Endpoint Security server and the Endpoint Security server itself. It relies on the Endpoint Security server compliance feature, which defines whether a host is secure and can block connections that do not meet the defined prerequisites of software components.

The following is a typical Cooperative Enforcement workflow:

1. A host opens a connection to the network through a firewall gateway. The first packet from the client to the server is allowed. It is only on the first server's reply to the client that the Cooperative Enforcement feature begins to perform.
2. The firewall checks for host compliance in its tables and queries the Endpoint Security server, if required.
3. Upon receiving a reply, connections from compliant hosts are allowed and connections from non-compliant hosts are blocked.

When activating the cooperative enforcement feature on a gateway, the following implied rules are automatically enabled:

1. Allow all firewall GUI clients to connect to the Endpoint Security server via HTTP or HTTPS (port 80 or 443).
2. Allow all internal clients to access the Endpoint Security server via the firewall for heartbeats.
3. Allow the firewall to communicate with the Endpoint Security server on port 5054.

If additional access permissions are required (such as allow external clients to connect to the Endpoint Security server, or for other machines to access the administration portion of the Endpoint Security server), explicit rules should be defined.

If additional access permissions are required (such as allow external clients to connect to the Endpoint Security server, or for other machines to access the administration portion of the Endpoint Security server), explicit rules should be defined.

## ***Enforcement Mode***

When in enforcement mode, noncompliant host connections are blocked by the firewall endpoint security feature. For HTTP connections, the host is notified that it is noncompliant. The user can then perform appropriate actions to achieve compliance. For example, the user may upgrade the version of the Endpoint Security client.

## ***NAT Environments***

Cooperative Enforcement feature is not supported by all the NAT configurations.

For Cooperative Enforcement to work in a NAT environment, the gateway and the Endpoint Security Server must relate to the same IP address of a specific client. Therefore, when NAT is used, if NAT is causing the Client IP received by gateway to be different than the Client IP received by the Endpoint Security Server, Cooperative Enforcement will not work properly.

## ***Monitor Only Deployment Mode***

In the *Monitor Only* deployment mode, the firewall requests authorization statuses from the Endpoint Security server but, regardless of the received statuses, connections are not dropped. In addition (if configured by the administrator) the Cooperative Enforcement feature generates logs regardless of the deployment mode.

For configuration details, see “[Configuring Cooperative Enforcement](#)” on page 51.

## End Point Quarantine (EPQ) - Intel(r) AMT

End Point Quarantine (using Intel® AMT) gives the administrator the ability to place a malicious user's machine under quarantine whenever malicious activity takes place according to the security policy configuration.

EPQ isolates the malicious machine by installing a security policy on the machine where the malicious activity originated. The policy restricts both inbound and outbound traffic flowing from that machine. As a result, the machine is isolated from the rest of the network and is prevented from causing any further problems.

It is recommended to enable anti-spoofing to maximize the security protection. Even with anti-spoofing enabled, the following protections will not work properly with EPQ and may cause hosts to be put into quarantine:

- All DOS protections
- Packet sanity
- Max ping size
- IP fragment
- Network quota
- Small pmtu

EPQ is supported on SecurePlatform and Linux platforms.

For configuration details, see “[Configuring End Point Quarantine \(EPQ\)](#)” on [page 52](#).

# Special Considerations for Access Control

## In This Section

Spoofing Protection	page 45
Simplicity	page 45
Basic Rules	page 46
Rule Order	page 46
Topology Considerations: DMZ	page 46
Editing Implied Rules	page 47
Defining Access Control Rules	page 48

## Spoofing Protection

If your network is not protected against IP address spoofing, your access control rules are ineffective and it is easy for attackers to gain access by changing the source address of the packet. For this reason, ensure that you configure anti-spoofing protection on every interface of the Security Gateway, including internal interfaces. See “[Configuring Access Control](#)” on page 48.

## Simplicity

The key to effective firewall protection is a simple Rule Base. One of the greatest dangers to the security of your organization is misconfiguration. For example, a user may try to sneak spoofed, fragmented packets past your firewall if you have accidentally allowed unrestricted messaging protocols. To keep your Rule Base simple, ensure that it is concise and therefore easy to understand and maintain. The more rules you have, the more likely you are to make a mistake.

## Basic Rules

When creating rules, ensure that you allow only traffic that you want. Consider traffic initiated and crossing the firewall from both the protected and unprotected sides of the firewall.

The following basic access control rules are recommended for every Rule Base:

- A Stealth Rule to prevent direct access to the Security 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 such access attempts.

Remember that the fundamental concept behind the Rule Base is that actions that are not explicitly permitted are prohibited.

## Rule Order

Rule order is a critical aspect of an effective Rule Base. Having the same rules, but putting them in a different order, can radically alter the effectiveness of your firewall. It is best to place more specific rules first and more general rules last. This order prevents a general rule from being applied 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, it is recommended to create a demilitarized zone (DMZ). The DMZ isolates all servers that are accessible from untrusted sources, such as the Internet, so that if one of those servers is compromised, the intruder only has limited access to other externally accessible servers. Servers in the DMZ are accessible from any network, and all externally accessible servers should be located in the DMZ. 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.

## X11 Service

The X11 (X Window System Version 11) graphics display system is the standard graphics system for the Unix environment. To enable X11, you must create a specific rule using the X11 service. If you select **Any** as the **Source** or **Destination**, the X11 service is not included because when using the X11 service, the GUI application acts as the server rather than the client.

## Editing Implied Rules

Implied rules are defined in the **Global Properties** window > **Firewall Implied Rules** page. In general, there is no need to change predefined implied rules. It is often best to leave some of the rules unselected so that the property can be controlled with greater granularity through the Rule Base. For example, you may want to allow ICMP pings across certain gateways only.

The following are the recommended settings for implied rules:

**Table 1-3** Recommended Settings for Firewall Implied Rules

Implied Rule	Recommended Setting
Accept control connections	First
Accept Remote Access control connections	First
Accept SmartUpdate connections	First
Accept outbound packets originating from the gateway	Unselected
Accept RIP	Unselected
Accept Domain Name Over UDP (Queries)	Unselected
Accept Domain Name over TCP (Zone transfer)	Unselected
Accept ICMP requests	Unselected
Accept dynamic address DHCP traffic	First
Accept VRRP packets originating from cluster members (VSX Nokia VRRP)	First

# Configuring Access Control

## In This Section

Defining Access Control Rules	page 48
Defining a Basic Access Control Policy	page 49
Configuring Multicast Access Control	page 50
Configuring Cooperative Enforcement	page 51
Configuring End Point Quarantine (EPQ)	page 52

## Defining Access Control Rules

To define access control rules, perform the following steps using SmartDashboard (see the *Security Management Server Administration Guide*):

1. Define network objects for each network and host using SmartDashboard.
2. Click the **Firewall** tab in SmartDashboard.
3. From the SmartDashboard menu, select **Rules > Add Rule** and then select either **Bottom**, **Top**, **Below**, or **Above**.
4. Right-click in the **Source** column and select **Add**.
5. Select a network object and click **OK**.
6. Right-click in the **Destination** column and select **Add**.
7. Select a network object and click **OK**.
8. Right-click in the **Service** column and select **Add**.
9. Select a service or a service group and click **OK**.
10. Right-click in the **Action** column and select **Accept**, **Drop**, or **Reject**.
11. Right-click in the **Track** column and select **Add**.
12. Select one of the tracking options.

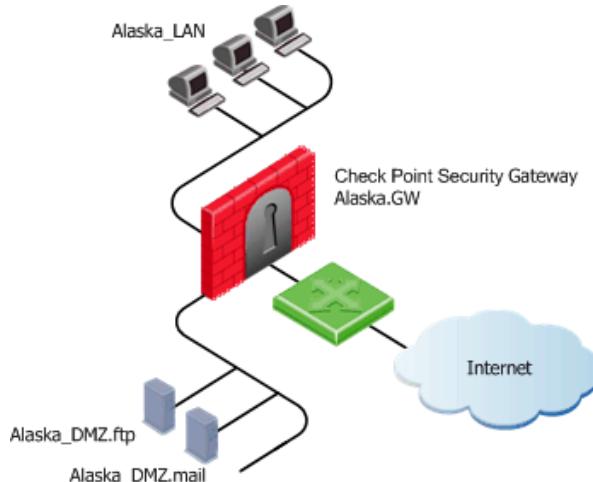
# Defining a Basic Access Control Policy

The Access Control policy is required to:

- Allow internal users access to the Internet.
- Allow all users access to the servers on the DMZ network.
- Protect the network from outsiders.

The policy also requires two basic rules: a Stealth rule and a Cleanup rule.

**Figure 1-11** Sample Network Requiring an Access Control Policy



To create an Access Control Policy:

- Add rules in SmartDashboard using the **Rules > Add Rules** menu options.

**Figure 1-12** Sample Access Control Rule Base

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	* Any	Alaska_GW	* Any	* Any	drop	Log	* Policy Target	* Any	Stealth Rule
2	* Any	Alaska_DMZ.LAN	* Any	TCP smtp TCP ftp	accept	Log	* Policy Target	* Any	DMZ Access Rule
3	Alaska_LAN	* Any	* Any	TCP http	accept	Log	* Policy Target	* Any	Web Traffic Rule
4	* Any	* Any	* Any	* Any	drop	Log	* Policy Target	* Any	Cleanup Rule

See also “[Defining a Basic Access Control Policy](#)” on page 49.

# Configuring Multicast Access Control

To configure multicast access control:

1. In the gateway **General Properties** page, ensure that the gateway version is specified correctly. (A per-interface multicast policy can be defined for gateways of versions R60 or higher.)
2. In the **Topology** page, select an interface and click **Edit**.
3. In the **Multicast Restrictions** tab of the **Interface Properties** window, select **Drop Multicast packets by the following conditions**.
4. Select a multicast policy for the interface:
  - **Drop multicast packets whose destination is in the list**
  - **Drop all multicast packets except those whose destination is in the list**
5. Click **Add** to add a multicast address range. The **Add Object** window opens, with the **Multicast Address Ranges** object selected in the list.
6. Click **New > Multicast Address Range**. The **Multicast Address Range Properties** window opens.
7. Provide a name for this range.
8. Define either an **IP address Range** or a **Single IP Address** that are in the 224.0.0.0 to 239.255.255.255 range.
9. Click **OK**. The named Multicast Range appears in the **Add Object** window.
10. Click **OK**. The named Multicast Range appears in the **Interface Properties > Multicast Restrictions** window.
11. Click **OK** to close the **Interface Properties** window and again to close the gateway window.
12. In the Rule Base, add a rule that allows the multicast address range. As the **Destination** of the rule, specify the range defined in [step 5](#).
13. Save and install the security policy: **Policy > Install**.

See also: “[Multicast Access Control](#)” on page 38.

# Configuring Cooperative Enforcement

To configure Cooperative Enforcement:

From the gateway's **Cooperative Enforcement** page, select **Authorize clients using Endpoint Security Server** to enable Cooperative Enforcement.

1. Select **Monitor Only** for traffic to pass successfully and to track only connections that would otherwise have been dropped.
2. **Track unauthorized client status** allows you to set the appropriate track or alert option. The default setting is **Log**.
3. In the **Endpoint Security Server Selection** section, select which Endpoint Security server will be used:
  - To use this machine, select **Use Endpoint Security Server installed on this machine**.
  - To use another machine, select a server from the **Select Endpoint Security Server** drop down menu. Click **New** to create a new server.
4. In the **Client Authorization** section, select one of the following methods:
  - **Check authorization of all clients**: Inspects all clients.
  - **Bypass authorization of the following clients**: Permits all clients in the selected groups drop-down list to pass without inspection.
  - **Check authorization only of the following clients**: Verifies the authorization of clients from the selected groups drop-down list.

# Configuring End Point Quarantine (EPQ)

Configuring EPQ is done using CLI. The `AMT.conf` file, which is located in the `$FWDIR/conf` folder, is used to define all actions taken on the machine initiating any malicious action.

## Activating EPQ

By default, EPQ is disabled. To enable, proceed in the `AMT.conf` file:

1. On the Security Management server, open `$FWDIR/conf/AMT.conf`
2. On the `enable_amt` line, change `false` to `true`.

See [Figure 1-13](#), [Figure 1-14](#), and [Figure 1-15](#) for further configuration samples.

3. Install policy.

**Figure 1-13** Configuration sample

```
----- Activate the feature by changing the flag to true and define
the subnets the feature is enabled on.
:enable_amt (false)
----- AMT Quarantine can be activated on a host, on a network, or
both
:apply_on (
    :(host
        :ipaddr (192.168.10.1)
    )
    :(network
        :ipaddr_from (192.168.10.1)
        :ipaddr_to (192.168.10.100)
    )
)
:track (log)
```

# Connection Authentication Data

Figure 1-14 Defining the Authentication Method

```
:authentication (
    ----- Define the authentication method using one of the following:
        no_tls - clear text
        tls - only server authentication
        mutual_tls - client and server authentication
    :method (no_tls)
    ----- Username and password are required for all methods
        :user_name ("admin")
        :user_pass ("Myadmin1!")
    ----- Server Certificate is only required when tls is the chosen
    authentication method
        :server_certificate (
            :server_cert_name ("server certificate name")
            :server_cert_path ("server certificate path")
        )
    ----- Client certificate is only relevant on Linux when mutual_tls
    is the chosen authentication method
        :client_certificate (
            :cert_name ("certificate name")
            :cert_pass ("certificate pass")
        )
)
```

# Quarantine Policy Data

Figure 1-15 Policy Name and Rules

```
:quarantine_policy_data (
    :policy_name ("CP_Qua")
----- Format for policy version is MMDDHHmm (month/day/hour/minutes)
    :policy_ver ("23121917")
-- Define rules for traffic directed to machine initiating malicious activity
    :incoming (
        :1 (
            :name ("dns")
            :service (
                :protocol (udp) # tcp / udp
                :port (53)
            )
            :address ("10.16.70.5")
            :address_mask ("255.255.255.0")
        )
        :2 (
            :name ("ftp")
            :service (
                :protocol (tcp)
                :port (21)
            )
            :address ("10.16.70.5")
            :address_mask ("255.255.255.0")
        )
    )
-- Define rules for traffic from machine initiating malicious acitivty
    :outgoing (
        :1 (
            :name ("dns")
            :service (
                :protocol (tcp) # udp / tcp
                :port (53)
            )
            :address ("10.16.70.5")
            :address_mask ("255.255.255.0")
        )
        :2 (
            :name ("ftp")
            :service (
                :protocol (tcp)
                :port (21)
            )
            :address ("10.16.70.5")
            :address_mask ("255.255.255.0")
        )
    )
)
```

You can configure up to 29 rules for incoming traffic and up to 29 rules outgoing traffic.

The policy name must begin with “CP\_” and cannot exceed six letters. Numbers and other characters are not permitted.



**Note** - It is recommended not to change the default policy name.

## Encrypting the Password

After the `AMT.conf` file is configured and saved, run the following command:

```
epq -o set_password
```

This command will not change the password but will encrypt the password so it is not in the clear. Running this command a second time however, will change the password. It is recommended to save and store your password in a safe place since there is no undo option.

## Malicious Activity Script and Alert

The `sam_alert` tool executes FW-1 SAM actions according to information received through Standard input (the log mechanism). This tool is to be used for executing FW-1 SAMv2 actions with the user defined alerts mechanism.

### ***sam\_alert Usage***

```
sam_alert [-O] [-S] [-t timeout] [-f target] [-n name] [-c comment] [-o originator] [-rla] -a dirlnlblqli [-C] -ip -eth -src -dst -srv -any
```

[Table 1-4](#) describes the arguments for this command.

**Table 1-4** sam\_alert Options

Argument	Description
-O	print the input of this tool to Standard output (for pipes).
-S	Match the SAM server to be contacted. Default is localhost.
-t timeout	The time period (in seconds) for which the action will be enforced. The default is forever.
-f target	The firewalls on which to run the operation. Default is All.
-n name	Fill in the SAM name field. Default is empty.

**Table 1-4** sam\_alert Options (Continued)

Argument	Description
-c comment	Fill in the SAM comment field. Default is empty.
-o originator	Fill in the SAM originator field. Default is "sam_alert".
-l	Logs to issue for connections matching the specified criteria. Either r/egular, a/lert. Default is None.
-a	Action to apply on connections matching specified criteria. Either d/rop, r/eject, n/otify, b/ypass, q/uarantine, i/nspect.
-C	Close all existing connections that match the criteria.
-ip	Use IP addresses as criteria parameters.
-eth	Use MAC addresses as criteria parameters.
-src	Match the source address of connections.
-dst	Match the destination address of connections.
-srv	Match specific source, destination, protocol and service.
-any	Match either the source or destination address of connections.

## ***sam\_alert Configuration***

In SmartDashboard:

1. Click **Policy > Global Properties > Log and Alert > Alert Commands**.
2. In one of the unused **Run UserDefined script** fields, enter the following script command:

```
 sam_alert -v2 -a r -t 60 -ip -src
```

This is a sample script. Keep in mind the following points:

- The feature will only work if the action (-a) is r (reject) or d (drop).
- -t 60 can be changed.
- -ip and -src represent that we only want to block an attacker that sends something malicious.

3. Install policy.

## Logging Activity

The script is run when a malicious action is logged.



**Note** - Actions are not logged by default. The User Defined alert must be enabled for each threat for the sam\_alert script to be activated.

The log as it appears in SmartView Tracker.

		feature_name: End Point Quarantine - Intel(r) AMT; host: broadwater.amt.intel.com
		feature_name: End Point Quarantine - Intel(r) AMT; host: broadwater.amt.intel.com

The first log entry represents that the end point host, *Broadwater*, has been quarantined. The second log represents that the end point host, *broadwater*, has been released from quarantine and authorized to be part of the network.

To quarantine a machine manually, use the following command:

```
epq -o < status | list | is_amt | enable | disable [-l  
lastPolicyHandle] > -i AMTdeviceIP [policyFileName]
```

**Table 1-5** Arguments of epq

Argument	Description
status	Display the status of the policies and rules.
list	List the quarantined end-point computers.
is_amt	Allows the user to check if there is AMT on the machine.
enable	Activates the policy.
disable	Deactivates the policy being enforced.
-l lastPolicyHandle	This is the last known policy to be activated.
-i AMTdeviceIP	The IP address of the end-point computer you want to quarantine.
policyFileName	The file name of the file containing the policy you want to enforce. (default location is \$FWDIR/conf/AMT.conf)



# Chapter

# Authentication

## In This Chapter

- The Need for Authentication
- Solution for Authentication
- Configuring Authentication

page 60  
page 60  
page 73

# The Need for Authentication

Authentication confirms the identity of valid users authorized to access your company network. Staff from different departments are assigned access permissions based on their level of responsibility and role within the organization. Authentication ensures that all users trying to access the system are valid users, but does not define their access rights.

# Solution for Authentication

## In This Section

<a href="#">Introduction to Check Point Authentication</a>	page 60
<a href="#">Authentication Schemes</a>	page 61
<a href="#">Authentication Methods</a>	page 64

## Introduction to Check Point Authentication

Check Point Security Gateway authenticates individual users using credentials and manages them using different authentication schemes. All of the authentication schemes require the provision of a user name and password. While some schemes involve storing the passwords on the gateway, others are stored on external servers.

There are different ways to access a network resource and authenticate using Check Point Security Gateway:

**User Authentication:** Enables administrators to permit users who have temporarily left their desk to work on the local network without extending access to all users on the same host. User authentication is available only for the Telnet, FTP, HTTP and RLOGIN services.

**Session Authentication:** Provides an authentication mechanism for any service and requires users to supply their credentials for each authentication session. A session authentication agent must be installed on every authenticating client, therefore this method is not suitable for authenticating HTTP services as they open multiple connections per session. Similar to client authentication, it is best used on single user machines, where only one user can authenticate from a given IP at any one time.

**Client Authentication:** Permits multiple users and connections from the authorized IP address or host. Authorization is performed per machine. For example, if FINGER is authorized for a client machine, then all users on the client are authorized to use FINGER and are not asked to supply a password during the authorization process. Client authentication is best enabled on single-user machines.

The main advantage of client authentication is that it can be used on any number of connections for any service and authentication can be set to valid for a specified time period.

These authentication methods can also be used for unencrypted communication.

Authentication is required for Remote Access communication using SecuRemote/SecureClient.

## Authentication Schemes

Authentication schemes employ usernames and passwords to identify valid users. Some schemes are maintained locally and store usernames and passwords on the Check Point Security Gateway, while others are maintained externally and store user authentication information on an external authentication server. Certain schemes, such as SecurID, are based on providing a one-time password. All of the schemes can be used with users defined on an LDAP server. For additional information on configuring the firewall to integrate with an LDAP server, see the *SmartDirectory (LDAP) and User Management* section in the *Security Management Server Administration Guide*.

### ***Check Point Password***

The Check Point Security Gateway can store a static password in the local user database of each user configured in Security Management server. No additional software is required.

### ***Operating System Password***

Check Point Security Gateway can authenticate using the user name and password that is stored on the operating system of the machine on which Check Point Security Gateway is installed. You can also use passwords that are stored in a Windows domain. No additional software is required.

## **RADIUS**

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.

Using RADIUS, Check Point Security Gateway 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 to communicate with the gateway. RADIUS servers and RADIUS server group objects are defined in SmartDashboard. See also “[Configuring a Security Gateway to use RADIUS](#)” on page 87.

## **SecurID**

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 approximately every minute. When a user attempts to authenticate to a protected resource, the one-time use code must be validated by the ACE/server.

Using SecurID, Check Point Security Gateway 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 gateway acts as an ACE/Agent 5.0 and directs all access requests to the RSA ACE/server for authentication. For additional information on agent configuration, refer to ACE/server documentation.

There are no specific parameters required for the SecurID authentication scheme. For additional information on configuring SecurID, refer to “[Configuring Security Gateway to use SecurID](#)” on page 91.

## **TACACS**

Terminal Access Controller Access Control System (TACACS) provides access control for routers, network access servers and other networked devices through one or more centralized servers.

TACACS is an external authentication scheme that provides verification services. Using TACACS, Check Point Security Gateway 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 Kerberos secret key authentication. TACACS encrypts the user name, password, authentication services and accounting information of all authentication requests to ensure secure communication.

For additional information on configuring TACACS, refer to: “[Configuring Security Gateway to use TACACS+](#)” on page 92.

## ***Undefined***

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

# Authentication Methods

## In This Section

<a href="#">Introduction to Authentication Methods</a>	page 64
<a href="#">User Authentication</a>	page 64
<a href="#">Session Authentication</a>	page 67
<a href="#">Client Authentication</a>	page 68

## ***Introduction to Authentication Methods***

Instead of creating a security rule that simply allows or denies connections, the firewall administrator can request that clients authenticate when they try to access specific network resources.

There are three authentication methods available: user, client and session. These methods differ in the services provided, the logon mechanism, and the overall user experience. Each method can be configured to connect and authenticate clients to the gateway before the connection is passed to the desired resource (a process known as nontransparent authentication). Alternatively, each method can be configured to connect clients directly to the target server (a process known as transparent authentication).

This section describes how users authenticate using each authentication method. For additional information on configuring authentication methods, refer to “[Configuring Authentication](#)” on page 73.

## ***User Authentication***

User Authentication provides authentication for the Telnet, FTP, HTTP, and rlogin services. By default, User Authentication is transparent. The user does not connect directly to the gateway, but initiates a connection to the target server.

The following is a typical User Authentication method workflow:

1. Check Point Security Gateway intercepts the communication between the client and server.
2. Check Point Security Gateway prompts the user for a username and password.
3. If the user successfully authenticates, the gateway passes the connection to the remote host. If incorrect authentication information is provided during the allowed number of connection attempts, the connection is dropped.

- 
4. The remote host prompts the user for a username and password.



**Note** - When configuring user objects, you can set the locations that they are allowed to access, however, this can lead to a conflict with security rules that require some form of authentication. See also: “[Resolving Access Conflicts](#)” on page 81.

The following sections provide Telnet and FTP authentication scheme examples using the User Authentication method.

## Telnet Session Authentication

The following is an example of a Telnet session to 10.11.12.13 authentication attempt using the User Authentication method and the Operating System Password authentication scheme (Rlogin works in a similar manner):

```
# 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:
```

## FTP Session Authentication

To authenticate an FTP session to 10.11.12.13 using the user authentication method and the Operating System Password authentication scheme:

1. Open an FTP session to 10.11.12.13:

```
# ftp 10.11.12.13
Connected to 10.11.12.13.
220 Check Point FireWall-1 Secure FTP server running on tower Name
(10.11.12.13:fbloggs):
```

2. Enter the username in the following format:

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

For example:

```
ftpuser@fbloggs@10.11.12.13
331 password: you can use password@password
```

3. Enter the FTP password followed by the Check Point password, for example:

**Password: ftppass@xyz987**

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



**Note** - Escape the **at** sign (@) in a username by using @@. For example, if the FTP username uses the user@domain format, provide:  
user@@domain@FirewallUser@Destination Host

4. Log in using the following 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 HTTP User Authentication

In HTTP user authentication, the Web browser automatically provides the password to the server for each connection, which raises special security considerations when using User Authentication for HTTP with one-time passwords.

To avoid forcing users with 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 by the **User Authentication session timeout** option in the **Authentication** page of the **Check Point Gateway** window. This ensures that users of one-time passwords do not have to reauthenticate for each request during this time period.

To enhance security, you may want to require 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, redefine the **Reauthentication** options in the **HTTP Server** definition of the **Global Properties > Firewall > Security Server** page.

For additional information on configuring User Authentication, refer to “[Configuring User Authentication](#)” on page 76.

## **Session Authentication**

Session Authentication can be used for any service, however, a Session Authentication agent is required to retrieve a user's identity. The Session Authentication agent is normally installed on the authenticating client, whereby the person who initiates the connection to the destination host, supplies the authentication credentials. Session authentication 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, thereby allowing the user at that machine to provide the username and password.

The following is a typical Session Authentication workflow:

1. The user initiates a connection directly to the server.
2. Check Point Security Gateway intercepts the connection.
3. The Session Authentication agent challenges the user for authentication data and returns this information to the gateway.
4. If the authentication is successful, Check Point Security Gateway allows the connection to pass through the gateway and continue to the target server.

For information on configuring Session Authentication and the Session Authentication agent, see “[Configuring Session Authentication](#)” on page 77.



**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 also “[Resolving Access Conflicts](#)” on page 81.

## **Client Authentication**

### In This Section

<a href="#">Client Authentication and Sign On Overview</a>	page 68
<a href="#">Manual Sign On</a>	page 69
<a href="#">Wait Mode</a>	page 71
<a href="#">Partially Automatic Sign On</a>	page 71
<a href="#">Fully Automatic Sign On</a>	page 71
<a href="#">Agent Automatic Sign On</a>	page 72
<a href="#">Single Sign On</a>	page 72

### **Client Authentication and Sign On Overview**

Client Authentication can be used to authenticate any service. It enables access from a specific IP address for an unlimited number of connections. The client user performs the authentication process, but it is the client machine that is granted access. Client Authentication is less secure than user authentication because it permits access for multiple users and connections from authorized IP addresses or hosts. Authorization is performed on a per machine basis for services that do not have an initial login procedure. The advantages of Client Authentication are that it can be used for an unlimited number of connections, for any service, and is valid for any length of time.



**Note** - When configuring user objects, you can set the locations that users can access, however, this can cause problems with security rules that require some form of authentication. See also "[Resolving Access Conflicts](#)" on page 81.

Client Authentication works with all sign on methods. [Table 2-1](#) shows how different sign on methods provide choice when selecting an authentication method for authenticated and other services. For sign on methods other than Manual Client Authentication, the gateway is transparent to the users and they authenticate directly to the destination host.

**Table 2-1** Client Authentication Sign On Methods

<b>Client Authentication Sign On Method</b>	<b>Authentication Method for authenticated services: Telnet, FTP, HTTP, RLOGIN</b>	<b>Authentication Method for other services</b>
Manual	Telnet to port 259 on gateway HTTP to port 900 on gateway	Telnet to port 259 on gateway HTTP to port 900 on gateway
Partially automatic	User Authentication	Not available
Fully automatic	User Authentication	Session Authentication
Agent automatic	Session Authentication	Session Authentication
Single Sign on	UserAuthority	UserAuthority

The following are the two Client Authentication sign on options:

- **Standard Sign on:** Enables users to access all services permitted by the rule without authenticating for each service.
- **Specific Sign on:** Enables users to access only the services that they specify when they authenticate, even if the rule allows more than one service. If the user wants to use another service, they must reauthenticate for that specific service.

At the end of an authentication session, the user can sign off. When a user signs off, they are disconnected from all services and the remote host.

## Manual Sign On

Manual Sign On is available for any service that is specified in the Client Authentication rule. The user must first connect to the gateway and authenticate in one of the following two ways:

1. Through a Telnet session to the gateway on port 259.
2. Through an HTTP connection to the gateway on port 900 and a Web browser. The requested URL must include the gateway name and the port number, for example, `http://Gateway:900`.

The following example shows Client Authentication using a Standard Manual Sign On method. In this example, before opening a connection to the destination host, the user **fbloggs** first authenticates to **london**, the Check Point Security 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 Client Authentication using a Specific Manual Sign On method. In this 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

Wait mode is a Client Authentication feature for Manual Sign On when the user initiates a client authenticated connection with a Telnet session on port 259 on the gateway.

Wait mode eliminates the need to open a new Telnet session in order to sign off and withdraw client authentication privileges. In Wait mode, the initial Telnet session connection remains open so long as client authentication privileges remain valid. Client authentication privileges are withdrawn when the Telnet session is closed.

Check Point Security Gateway keeps the Telnet session open by pinging the authenticating client. If for some reason the client machine stops running, the gateway closes the Telnet session and client authentication privileges from the connected IP address are withdrawn.

Enable Wait mode works only with client authentication rules that specify Standard Sign On. In Enable Wait mode, client authentication rules that require Specific Sign On are not applied.

## Partially Automatic Sign On

Partially Automatic Sign On is available for authenticated services (Telnet, FTP, HTTP and RLOGIN) only if they are specified in the client authentication rule. If the user attempts to connect to a remote host using one of the authenticated services, they must authenticate with User Authentication. When using Partially Automatic Client Authentication, ensure that port 80 is accessible on the gateway machine.

## Fully Automatic Sign On

Fully Automatic Sign On is available for any service only if the required service is specified in the client authentication rule. If the user attempts to connect to a remote host using an authenticated service (Telnet, FTP, HTTP, and RLOGIN), they must authenticate with User Authentication. If the user attempts to connect to a remote host using any other service, they must authenticate through a properly installed Session Authentication agent. When using Fully Automatic Client Authentication, ensure that port 80 is accessible on the gateway machine.

## **Agent Automatic Sign On**

Agent Automatic Sign On is available only if the required service is specified in the Client Authentication rule, and the Session Authentication agent is properly installed.

If a user attempts to connect to a remote host using any service, they must authenticate through a Session Authentication agent.

## **Single Sign On**

Single Sign On is available for any service only if the required service is specified in the Client Authentication rule and UserAuthority is installed.

Single Sign On is a Check Point address management feature that provides transparent network access. Check Point Security Gateway consults the user IP address records to determine which users are logged on to any given IP address. When a connection matches a Single Sign On enabled rule, the gateway 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.

# Configuring Authentication

## In This Section

<a href="#">Creating Users and Groups</a>	page 73
<a href="#">Configuring User Authentication</a>	page 76
<a href="#">Configuring Session Authentication</a>	page 77
<a href="#">Configuring Client Authentication</a>	page 80
<a href="#">Configuring Authentication Tracking</a>	page 86
<a href="#">Configuring a Security Gateway to use RADIUS</a>	page 87
<a href="#">Granting User Access Using RADIUS Server Groups</a>	page 89
<a href="#">Associating a RADIUS Server with Security Gateway</a>	page 90
<a href="#">Configuring Security Gateway to use SecurID</a>	page 91
<a href="#">Configuring Security Gateway to use TACACS+</a>	page 92
<a href="#">Configuring Policy for Groups of Windows Users</a>	page 93

## Creating Users and Groups

Authentication rules are defined by user groups rather than individual users. Therefore, you must first define users and then add them to groups in order to define authentication rules. You can define users with the Check Point Security Gateway proprietary user database or with an LDAP server. For details on incorporating LDAP, refer to *SmartDirectory (LDAP) and User Management* in the *Security Management Server Administration Guide*.

The following procedure describes how to create a group, create Check Point Security Gateway user accounts from a template, add users to the group and install user information in the database. For additional information on creating users and groups, refer to the *Security Management Overview* in the *Security Management Server Administration Guide*.

## ***Creating User Groups***

To create a user group:

1. In the SmartDashboard, select **User Groups** from the **Users and Administrators** tab of the **Objects** tree.
2. Right-click and select **New Group**. The **Group Properties** window opens.
3. Assign the group a name.

## ***Creating a User Template***

To create a user template:

1. In the SmartDashboard **Objects** tree, select the **Users and Administrators** tab.
2. Right-click **Templates** and select **New Template**. The **User Template Properties** window opens.
3. Assign the template a name.
4. In the **Groups** tab, add user groups. All users in these groups will get the properties of this template.
5. In the **Authentication** tab, select the appropriate authentication scheme for the user.
6. In the remaining tabs, enter the required properties of the user template.

After you create a template, any user that you create based on a given template inherits that template's properties, including membership in groups. If you modify a template's properties, those changes will only affect future users created using that template. Users previously created using that template are not affected.

## ***Creating Users***

To create users:

1. In the **Users** branch of the objects tree, right-click and select **Edit**. The **User Properties** window opens.
2. Enter the user data. You can change the properties that the user inherited from the template for that user only without changing the template.

## ***Installing User Information in the Database***

Users and groups can be installed separately from the Rule Base, meaning that you can update users and groups without reinstalling the Rule Base.

To install the user database:

- From the SmartDashboard menu, select **Policy > Install Database**.

# Configuring User Authentication

To configure user authentication:

1. Configure authentication for required users and groups and install the user database (see also: “[Creating Users and Groups](#)” on page 73).
2. Define a user authentication access rule as follows:
  - a. Right-click in the **Source** column, select **Add User Access** and then select the group.
  - b. To restrict the location of authenticating users, select **Restrict To** and the host, group of hosts, network or group of networks that users can access in the **Location** section of the same window.
  - c. In the **Service** field, select the services you wish to authenticate.
  - d. In the **Action** column, select **User Auth**.

**Table 2-2** User Authentication Rule for HTTP and FTP

SOURCE	DESTINATION	VPN	SERVICE	ACTION
Alaska_Users@Any	Alaska_LAN	Any Traffic	HTTP FTP	User Auth

3. Double-click the **Action** column to edit the **User Authentication Action Properties**.
4. If required, adjust the **User Authentication session timeout** from the **Authentication** page of the Security Gateway object.
5. Install the security policy: **Policy > Install**.

## ***Importance of Rule Order in User Authentication***

When defining user authentication rules for Telnet, FTP, HTTP, and RLOGIN services, if there are other non-authentication rules that use these services, ensure that the user authentication rule is located last amongst these rules.

# Configuring Session Authentication

To configure session authentication:

1. If using the Session Authentication Agent, install and configure it for all machine desktops with Session Authentication enabled (see “[Installing and Configuring Session Authentication Agent](#)” on page 78).
2. Configure the required users and groups for authentication, and install the user database (see “[Creating Users and Groups](#)” on page 73).
3. From the **Authentication** page, edit the **Check Point Gateway** object that represents the gateway and enable the required authentication schemes. The gateway must support all of the user defined authentication schemes. For example, if some users must provide a Check Point password, and others RADIUS authentication, select both schemes.
4. Define a Session Authentication access rule by doing the following:
  - a. Right-click in the **Source** column, select **Add User Access** and then the group. Do not close the window.
  - b. To restrict the location of authenticating users, in the **Location** section of the same window, select **Restrict To** and the host, group of hosts, network or group of networks that users can access.
  - c. In the **Service** field, select the services you want to authenticate.
  - d. In the **Action** column, select **Session Auth**. [Table 2-3](#) shows a typical Session Authentication Rule.

**Table 2-3** Session User Authentication Rule for HTTP and FTP

SOURCE	DESTINATION	VPN	SERVICE	ACTION
Alaska_Users@Any	Alaska_LAN	Any Traffic	HTTP FTP	Session Auth

5. Double-click the **Action** column to edit the **User Authentication Action Properties**.
6. If required, adjust the **Failed Authentication Attempts** settings for Session Authentication in the **Authentication** page of the **Global Properties**.
7. Install the security policy: **Policy > Install**.

## ***Installing and Configuring Session Authentication Agent***

To install and configure the Session Authentication Agent:

1. Install the Session Authentication agent from the CD-ROM.
  - If the Session Authentication agent is installed on the authenticating client, users who want to connect to the destination host provide the authentication credentials.
  - If Session Authentication agent is installed on the destination machine or on some other machine in the network, the user at the machine on which the Agent is installed is prompted to provide authentication credentials.
2. On Windows machines, double-click the Session Authentication agent icon in the system tray. The **Session Authentication** window.
3. Click **Configure**. The **Configuration** window opens and displays the **Passwords** tab. Specify how often the user is prompted to provide their password. One-time passwords (such as SecurID) cannot be cached.
4. Select one of the following options:
  - **Every request**: The user is prompted for a password each time that the Check Point Security Gateway requests authentication. Each time that the user initiates a session for which a Session Authentication Rule applies, the user is prompted for the password. No password caching occurs.
  - **Once per session**: The user is prompted for the password once per Session Authentication Agent session. Once the user provides the password, the Session Authentication agent caches the password indefinitely. This option cannot be used with one-time passwords. If the Session Authentication Agent session is closed and then restarted, the user must provide the password again.
  - **After minutes of inactivity**: Similar to the **Once per session** option, however, the user is prompted again for the password if there has been no authentication request over a specified time interval.
5. In the **Configuration** window, select the **Allowed FireWall-1** tab and specify the Security Gateways for which the Session Authentication agent can provide authentication services.

6. Select one of the following options:
  - **Any IP Address:** The Session Authentication agent can provide authentication services for any Security Gateway.
  - **IP Address:** The Session Authentication agent can provide authentication services for only a Security Gateway running on a user-specified IP address (you can specify up to three IP addresses).
7. In the **Configuration** window, select the **Options** tab and specify whether to allow clear passwords and to resolve addresses.
8. Select the appropriate option and click **OK**.

### ***Starting the Session Authentication Agent***

To start the Session Authentication Agent:

- From the Windows system tray, select the minimized Session Authentication Agent icon. The user can now configure the Session Authentication Agent and/or receive authentication requests from a Security Gateway.

# Configuring Client Authentication

## In This Section

Performing Basic Client Authentication Configuration	page 80
Enabling Client Authentication Wait Mode	page 81
Resolving Access Conflicts	page 81
Authorizing All Standard Sign On Rules	page 82
Changing the Client Authentication Port Number	page 83
Allowing Encrypted Client Authentication	page 84

## ***Performing Basic Client Authentication Configuration***

To perform basic client authentication configuration:

1. Configure the required users and groups for authentication and install the user database (see also “[Creating Users and Groups](#)” on page 73).
2. From the **Authentication** page, edit the **Check Point Gateway** object that represents the Security Gateway and enable the required authentication schemes. The gateway must support all of the user defined authentication schemes. For example, if some users must provide a Check Point password, and others RADIUS authentication, select both schemes.
3. Define a Client Authentication access rule as follows:
  - a. Right-click in the **Source** column, select **Add User Access** and then the group. Do not close the window.
  - b. To restrict the location of authenticating users, in the **Location** section of the same window, select **Restrict To** and the host, group of hosts, network or group of networks that users can access.
  - c. In the **Service** field, select the services you want to authenticate.
  - d. In the **Action** column, select **Client Auth**. [Table 2-4](#) shows a Client Authentication Rule for HTTP and FTP.

**Table 2-4** Client Authentication Rule for HTTP and FTP

SOURCE	DESTINATION	VPN	SERVICE	ACTION
Alaska_Users@Any	Alaska_LAN	Any Traffic	HTTP FTP	Client Auth

4. For Partially or Fully Automatic Client Authentication, ensure that port 80 is accessible on the gateway machine.
5. Double-click in the **Action** column to edit the **Client Authentication Action Properties**. The settings for Requires Sign On and Sign On Method are described in “[Client Authentication](#)” on page 68.
6. Place all Client Authentication Rules above the rule that prevents direct connections to the Security Gateway (the Stealth Rule) to ensure that they have access to the Security Gateway.
7. If required, adjust the **Failed Authentication Attempts** settings for Client Authentication in the **Authentication** page of the **Global Properties** window.
8. Install the security policy: **Policy > Install**.

## ***Enabling 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 eliminates the need to open a new Telnet session in order to sign off and withdraw client authentication privileges.

To enable Wait mode:

1. From the **Authentication** page, edit the **Check Point Gateway** object that represents the Security Gateway and select **Enable Wait Mode for Client Authentication**. In Client Authentication Wait mode, the Check Point Security Gateway monitors the Telnet connection to port 259 of the gateway by pinging the user's host.
2. Define rules to enable pinging as follows:
  - Enable the echo-request service from the Security Gateway to the user's host.
  - Enable the echo-reply service from the user's host to the Security Gateway.

## ***Resolving Access Conflicts***

When configuring users, you can define those locations that they can access. However, by doing so, you disallow access to all unspecified locations, which can cause conflicts with security rules that require authentication. For example, if a rule grants authenticated access to users from Mktg\_net to Finance\_net, but in the user's **Location** tab connections are only permitted within Mktg\_net, the firewall can not know whether to allow the authentication request when the user tries to connect to Finance\_net.

You can specify how to resolve this conflict by editing the **Authentication Action Property** of the rule. You can define this property for both the **Source** and **Destination** of the rule.

To resolve access conflicts:

1. Right-click the **Action** field of a rule using some form of authentication and select **Edit Properties**.
2. Do one of the following:
  - To apply the more restrictive access privileges specified in the rule and in the **Location** tab of each user's **User Properties** window, select **Intersect with User Database**.
  - To allow access according to the location specified in the rule, select **Ignore User Database**.

## ***Authorizing All Standard Sign On Rules***

By default, the Partially or Fully Automatic sign on methods open one rule following successful authentication (the rule for which the sign on was initiated). For example, if a user successfully authenticates according an automatic sign on rule, the user can work with the services and destinations permitted only by that rule.

You can configure Check Point Security Gateway to automatically open all Standard Sign On rules following successful authentication using Partially or Fully Automatic Sign On. If a user successfully authenticates according to an automatic sign on rule, then all Standard Sign On rules that define that user and source are available. The user can then work with all of the services and destinations permitted by the relevant rules; the Security Gateway knows which user is at the client, and additional authentication is not necessary.

To authorize all relevant Standard Sign On Rules following successful .

Partially or Fully Automatic authentication, use the GUILdbedit Database Tool to change a setting in the database.

To authorize all standard sign on rules:

1. Access the GUILdbedit Database Tool from the same directory on your local drive as where SmartConsole is installed.
2. Open GUILdbedit.
3. Search for the **automatically\_open\_ca\_rules** field.
4. Set the value to *true*. The new value takes effect after you install the security policy.

## Changing the Client Authentication Port Number

To change the Client Authentication port number:

1. Stop Check Point services by running the `cpstop` command.
2. Modify the port number in the **Manage > Service > Show > TCP Services** window for the following services:
  - To modify the port number for Telnet sign on, change the port number of the `FW1_clntauth_telnet` service.
  - To modify the port number for HTTP sign on, change the port number of the `FW1_clntauth_http` service.

These are special Check Point services provided as part of the Client Authentication feature.

3. Use a simple text editor to edit the `$FWDIR/conf/fwauthd.conf` file. Change the port number of the Client Authentication application to the same port number defined in [step 2](#).
4. Do one of the following:
  - 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.

**Figure 2-1**    \$FWDIR/conf/fwauthd.conf File

```
21fwssd in.aftpd wait 0
80 fwssd in.ahttpd wait 0
513 fwssd in.arlogindwait 0
25 fwssd in.asmtpd wait 0
23 fwssd in.atelnetd wait 0
259 fwssd in.aclientd wait 259
10081 fwssd in.lhttpd wait 0
900 fwssd in.ahclientdwait 900
0 fwssd in.pingd respawn 0
0 fwssd in.asessiond respawn 0
0 fwssd in.aufpd respawn 0
0 vpn vpnd respawn 0
0 fwssd mdq respawn 0
0 xrm xrmdrespawn0-pr
```



**Warning** - Do not change anything else in these lines.

5. Ensure that there is no rule that blocks the connection to the new port.
6. Restart Check Point services by running the `cpstart` command.

For additional information on configuring Client Authentication, see “[Configuring Client Authentication](#)” on page 80.

## ***Allowing Encrypted Client Authentication***

To configure Encrypted Client Authentication for HTTPS Connections:

1. Run the `cpstop` command on the Security Gateway.
2. Edit the `fwauthd.conf` file in the `$FWDIR/conf` directory by changing the line:

```
900 fwssd     in.ahclientd wait 900
```

to:

```
900 fwssd     in.ahclientd wait 900 ssl:defaultCert
```



**Note** - `defaultCert` is a nickname on the Certificate List on the Security Gateway. To check the nickname of your gateway, open the **VPN** page of the **Gateway Properties** window and see the **Certificates List**.

3. Save and close the file.
4. Run `cpstart`.
5. Open SmartDashboard.
6. Create the following Rule

**Table 2-5**

<b>Source</b>	<b>Destination</b>	<b>Service</b>	<b>Action</b>
User_group@Any	Internal server	https	Client Auth (Partially automatic or Manual mode)



**Note** - This Rule also permits HTTPS traffic between the client and the Web server following successful authentication.

7. Install the policy.

Continue with the following procedure in the client's browser.

1. Type the URL address `https://<Firewall_name_or_IP_address>:900`.
2. Click **Yes** to trust the Security Gateway certificate.
3. Type the Check Point Security Gateway user name.
4. Click **OK**.
5. Click **Yes**.
6. Type the Check Point Security Gateway password.
7. Click **Submit**.
8. Type the URL address: `https://<Internal_Web_Server_IP_address>`.
9. Click Yes.

You are now authenticated both to the Security Gateway and to your internal Web server.

# Configuring Authentication Tracking

Successful and unsuccessful authentication attempts can be monitored in SmartView Tracker or using other tracking options, for example, email and alerts. Authentication tracking can be configured for the following types of authentication attempts:

- **Failed authentication attempts:** Can be tracked for all forms of authentication.

To track failed authentication attempts:

- In the **Authentication** page of a gateway object, set the **Authentication Failure Track** property to define the tracking option when authentication failures occur.

- **Successful authentication attempts:** Can be tracked for Client Authentication.

To track successful authentication attempts:

1. In the **Client Authentication Action Properties** window, set the **Successful Authentication Tracking** property to define the tracking option for all successful Client Authentication attempts.
2. To set this option, right-click in the **Action** column of the Client Authentication rule. The default setting is **Log**.

- **All Authentication attempts:** Can be tracked for all forms of authentication.

To track all authentication attempts:

- Select an option in the **Track** column of any rule that uses some form of authentication. The **Set by Rule** tracking option can only be added to the tracking policy set in the gateway object.

For example, if the gateway object is set to log all failed authentication attempts, setting a rule to None has no effect and failed authentication attempts are still logged in SmartView Tracker. However, setting the rule to Alert causes an Alert to be sent for each failed authentication attempt.



**Note** - Authentication failure tracking for Check Point firewall versions prior to NG is defined by the **Authentication Failure Track** property in the **Authentication** page of the **Global Properties** window.

# Configuring a Security Gateway to use RADIUS

To configure a Security Gateway to use RADIUS authentication:

1. In SmartDashboard, create a RADIUS Host object by selecting **Manage > Network Objects > New > Node > Host**.
2. Name the Host object and assign it an IP address.
3. Create a RADIUS Server object by selecting **Manage > Server and OPSEC Applications > New > RADIUS**, and configure the following:
  - a. Name the RADIUS Server object.
  - b. Associate the RADIUS Server object with the RADIUS Host object created in [step 1](#).
  - c. Assign the **Service** by selecting either the **RADIUS** on port 1645 or **NEW-RADIUS** on port 1812 service. (The default setting is **RADIUS**, however the RADIUS standards group recommends using **NEW-RADIUS**, because port 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. Select either **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**.
4. Right-click the gateway object and select **Edit > Authentication**.
5. Enable **RADIUS** authentication.
6. Define a user group by selecting **Manage > Users & Administrators > New > User Group** (for example, **RADIUS\_Users**).
7. Enable RADIUS authentication for Check Point Security Gateway users by selecting **Manage > Users and Administrators > New > User by Template > Default**.
8. Enable RADIUS authentication for users without Check Point Security Gateway user accounts by creating an External User Profile. Select **Manage > Users and Administrators > New > External User Profile > Match all users** or **Match by domain**. To support more than one external authentication scheme, define your External User Profiles with the **Match By Domain** setting.

9. For all User Profiles and Templates, configure the following:
  - a. In the **General** tab, type 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. In the **Personal** tab, adjust the **Expiration Date**.
  - c. In the **Authentication** tab, select **RADIUS** from the drop-down list.
  - d. In the **Groups** tab, add the User Profile to the RADIUS group.
10. Verify that communication between the firewall and the RADIUS server are not NATed in the Address Translation Rule Base.
11. Save, verify, and install the policy.

# Granting User Access Using RADIUS Server Groups

Check Point Security Gateway enables you to control access for authenticated RADIUS users, based on the administrator's assignment of users to RADIUS groups. These groups are used in the Security Rule Base to restrict or grant access to users to specific resources. Users are unaware of the groups to which they belong.

To use RADIUS groups, you must define a return attribute in the RADIUS user profile of the RADIUS server. This attribute is returned to the Security Gateway and contains the group name (for example, RAD\_<group to which the RADIUS users belong>) to which the users belong. Although other RADIUS attributes can be used, by default the Class attribute is used (IETF RADIUS attribute number 25).

To grant access using RADIUS server groups:

1. On the Security Gateway, follow [step 1 to step 4](#) in “Configuring a Security Gateway to use RADIUS” on page 87.
2. Create an External User Profile by selecting **Manage > Users and Administrators > New > External User Profile > Match all users**. This is the generic\* user.
3. In the **Authentication** tab, select **RADIUS** as the Authentication Scheme and then select the created RADIUS server (not the node) from the drop-down list.
4. Define the required RADIUS user groups by selecting **Manage > Users & Administrators > New > User Group**. The name of the group must be in the format: RAD\_<group to which the RADIUS users belong>. Ensure the group is empty.
5. Create the required Rule Base rules to allow access to RADIUS users.
6. Save the changes, and exit SmartDashboard.
7. Run `cpstop` on the Security Management server.
8. On the Security Management server, use the Graphical Database Tool (GUIDbEdit) to change the value of the `add_radius_groups` attribute from false to true.
9. Run `cpstart` on the Security Management server.
10. Install the policy.
11. On the RADIUS server, modify the RADIUS users to include a class RADIUS attribute on the users **Return** list that corresponds to the user group that they access.

To use a different attribute instead of the class attribute, do one of the following:

- On the Security Gateway, use GUIdbEdit to modify the value of the firewall\_properties attribute radius\_groups\_attr to the new RADIUS attribute.
- On the RADIUS server, ensure that you use the same RADIUS attribute (on the users' Return list that corresponds to the Firewall user group that they access).

## Associating a RADIUS Server with Security Gateway

You can associate users with the Radius authentication server in the **User Properties Authentication** tab. You can also associate a gateway with a Radius server so that this overrides the User to Radius server association. This is performed by editing the database using the dbedit command.

To associate one or more Radius servers to a gateway:

1. Run the dbedit command:

```
modify network_objects <gw obj> radius_server servers:<radius obj>
```

2. To switch off the Radius to Check Point Security Gateway association so that the user always authenticates to the Radius server specified in the **User Properties Authentication** tab, switch off another attribute in the database by running the dbedit command:

```
modify users <user obj> use_fw_radius_if_exist false
```

# Configuring Security Gateway to use SecurID

To configure a Security Gateway to use SecurID:

1. Generate and copy the `sdconf.rec` file from the ACE/Server to:
  - `/var/ace/sdconf.rec` on UNIX, Linux or IPSO
  - `%SystemRoot%\System32\sdconf.rec` on Windows
2. In SmartDashboard, right-click the gateway object and select **Edit > Authentication** page.
3. Enable **SecurID** authentication.
4. Define a user group by selecting **Manage > Users & Administrators > New > User Group** (for example, `SecurID_Users`).
5. Enable SecurID authentication for Check Point Security Gateway users by selecting **Manage > Users and Administrators > New > User by Template > Default**.
6. Enable SecurID authentication for users without Check Point Security Gateway user accounts by creating an External User Profile. Select **Manage > Users and Administrators > New > External User Profile > Match all users** or **Match by domain**. If you support more than one external authentication scheme, set up your External User Profiles with the **Match By Domain** setting.
7. For all User Profiles and Templates, configure the following:
  - a. In 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. In the **Personal** tab, change the **Expiration Date**.
  - c. In the **Authentication** tab, select **SecurID** from the drop-down list.
  - d. In the **Groups** tab, add the User Profile to the SecurID group.
8. Verify that communication between the firewall and the ACE/Server are not NATed in the Address Translation Rule Base.
9. Save, verify, and install the policy.

**Note** - When a Security Gateway has multiple interfaces, the SecurID agent in Check Point Security Gateway sometimes uses the wrong interface IP to decrypt the reply from the ACE/Server, and authentication fails.



To overcome this problem, place a new text file, named `sdocts.rec`, in the same directory as `sdconf.rec`. The file should contain the `CLIENT_IP=<ip>` line, where `<ip>` is the primary IP address of the Security Gateway, as defined on the ACE/Server. This is the IP address of the interface to which the server is routed.

# Configuring Security Gateway to use TACACS+

To configure a Security Gateway to use TACACS+:

1. In SmartDashboard, create a TACACS Host object by selecting **Manage > Network Objects > New > Node > Host**
2. Name the Host object and assign it an IP address.
3. Create a TACACS server by selecting **Manage > Server and OPSEC Applications > New...> TACACS...**, and configure the following:
  - a. **Name** the TACACS server object.
  - b. Associate the TACACS server object with the TACACS **Host** object created in [step 1](#).
  - c. Select 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** selected in [step c](#).
4. Right-click the gateway object and select **Edit > Authentication**.
5. Enable **TACACS** authentication.
6. Define a user group by selecting **Manage > Users & Administrators > New > User Group** (for example, `TACACS_Users`).
7. Enable TACACS authentication for Check Point Security Gateway users by selecting **Manage > Users and Administrators > New > User by Template > Default**.
8. Enable TACACS authentication for users without Check Point Security Gateway user accounts by creating an External User Profile. Select either **Manage > Users and Administrators > New > External User Profile > Match all users** or **Match by domain**. If more than one external authentication scheme is supported, set up your External User Profiles using the **Match By Domain** setting.
9. For all User Profiles and Templates, configure the following:
  - a. In 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. In the **Personal** tab, change the **Expiration Date**.
  - c. In the **Authentication** tab, select **TACACS** from the drop-down list.
  - d. In the **Groups** tab, add the User Profile to the TACACS group.

10. Verify that communication between the firewall and the TACACS server is not NATed in the Address Translation Rule Base.
11. Save, verify, and install the policy.

## Configuring Policy for Groups of Windows Users

You can create policy rules for groups of users that are not defined on the Security Management server, but are defined either on the gateway's host (a Windows machine) or in the Windows machine's trusted domain.

To configure policy for groups of Windows users:

1. Enable this feature using the Graphical Database Tool (GUiDbEdit).
2. Change the value of the `add_nt_groups` attribute to `true`. (This attribute is located under the `firewall_properties` object in the `properties` table.)
3. Ensure that the user belongs to a Windows user group.
4. In the SmartDashboard, create a user group with the name: `Windows_<Windows user group which the user belongs to>`. The group may be empty.
5. Define a Generic User Profile for each user that uses an operating system password as its authentication scheme.



# **Connectivity**

This section describes how to give internal users and resources unrestricted yet secure connectivity across the gateway.



# Chapter

# Network Address Translation

## In This Chapter

The Need to Conceal IP Addresses	page 98
Check Point Solution for Network Address Translation	page 99
Planning Considerations for NAT	page 114
Configuring NAT	page 116
Advanced NAT Configuration	page 123

# 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 also require access to the Internet. Normally, it is impossible to give each computer an Internet-routable IP address 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. This makes available IP addresses scarce since most addresses have already been assigned. Internet Service Providers 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 a network is not practical for most companies.

Even if additional public IP addresses become available, changing the addresses of every machine in a large network would be both labor intensive and time consuming.

Whether computers have routable or non-routable addresses, the administrator may want to conceal their real addresses for security reasons, for example, to ensure that addresses cannot be seen from outside the organization or from other parts of the same organization. A network's internal addresses contains the topology of the network and, therefore, hiding this information greatly enhances security.

# Check Point Solution for Network Address Translation

## In This Section

Public and Private IP addresses	page 99
NAT in Check Point Security Gateway	page 100
Static NAT	page 101
Hide NAT	page 102
Automatic and Manual NAT Rules	page 104
Automatic Hide NAT for Internal Networks	page 105
NAT Rule Base	page 106
Bidirectional NAT	page 107
Understanding Automatically Generated Rules	page 108
Port Translation	page 110
NAT and Anti-Spoofing	page 110
Routing Issues	page 110
Disabling NAT in a VPN Tunnel	page 113

## Public and Private IP addresses

Public IP addresses are those that are routable on the Internet. RFC 1918 documents private address spaces that can be used on internal networks and do 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

When an enterprise employs an intranet using private addresses, a NAT gateway connects the intranet to the Internet. The **Global Properties > Non Unique IP Address Ranges** page specifies the address ranges that the Security Gateway considers private (non-unique).

## NAT in Check Point Security Gateway

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) side to the external (unprotected) side of the firewall appears to the destination as if it came from a different address, and the packet that is sent from the external to the internal side of the firewall arrives at the correct address.

Check Point Security Gateway supports two kinds of NAT:

- **Static NAT:** 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 Security Gateway to initiate connections, for example, so that internal servers can be made available externally.
- **Hide NAT:** A single public address is used to represent multiple computers with private addresses on the internal network. Hide NAT is a many-to-one translation. Hide NAT allows connections to be initiated only from the protected side of the Security Gateway.

NAT can be performed on Check Point network objects, nodes, networks, address ranges, and dynamic objects. NAT can be defined either automatically through the network object, by automatically adding rules to the NAT Rule Base, or manually by defining rules in the NAT Rule Base.

Manually creating NAT Rules adds extra flexibility. For example, in addition to translating IP addresses, you can translate the service or the destination port numbers. Port number translation is a type of Static NAT, in which one port number is translated to another port number.

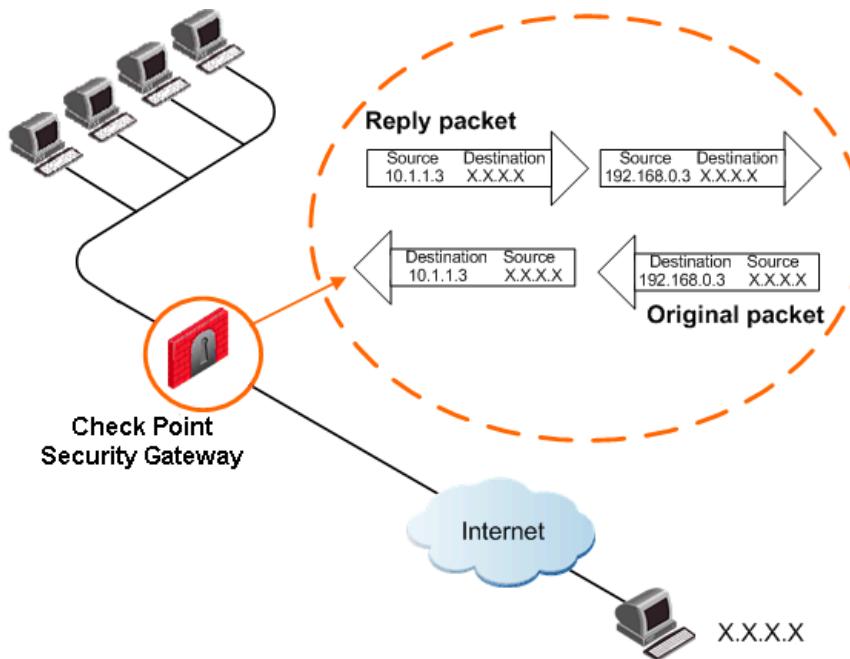
## Static NAT

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 3-1](#), the address range 10.1.1.2 to 10.1.1.10 is hidden behind the NAT range 192.168.0.2-192.168.0.11. The diagram shows a connection that originates at 10.1.1.3, and the source and destination translation of the original and reply packet.

**Figure 3-1** Static NAT on an Address Range



## Hide NAT

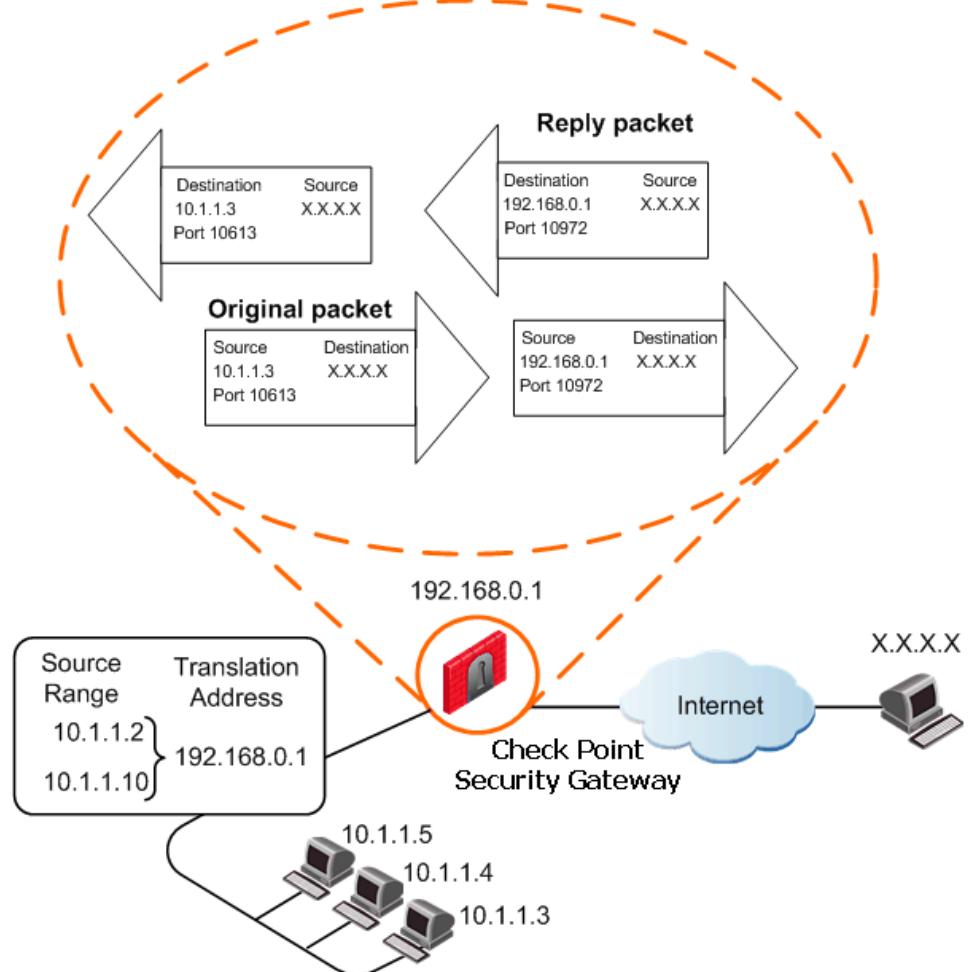
The NAT gateway makes it possible to share a single public address with multiple computers that have private addresses on your intranet. The Internet is unaware of the division you have created between the Internet and your intranet, and treats your multiple computer connection as a single connection.

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, however, 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 opt to hide the internal address(es) either:

- 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 Check Point Security Gateway interface through which the packet is routed out of (formerly known as “Hiding behind IP address 0.0.0.0”).

For example, assume the address range 10.1.1.2 to 10.1.1.10 is hidden behind the address of the external interface 192.168.0.1. A connection appears to originate from 10.1.1.3, and the source and destination original and reply packets are translated.

**Figure 3-2** 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, the Security Gateway uses the port number to determine to which internal machines the packets are destined. Port numbers are dynamically assigned from two pools of numbers: 600 to 1023 and 10,000 to 60,000.

Port numbers are normally 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 connection uses one of these services, and the original source port is less than 1024, then a port number is assigned from the first pool. This behavior is configurable.

Check Point Security Gateway keeps track of the port numbers assigned, so that the original port number is correctly restored for return packets and a port number that is currently in use is not assigned again to a new connection.

Hide NAT has a capacity of 50,000 connections per server. 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 Security Gateway—a highly unlikely scenario.

## Automatic and Manual NAT Rules

NAT can be defined automatically through the network object (node, network or address range). When you define NAT this way, rules are automatically added to the NAT Rule Base.

You can manually specify NAT rules by adding or editing NAT rules in the NAT Rule Base. The firewall validates manual NAT rules, helping to avoid mistakes in the setup process. Creating manual NAT Rules gives maximum control over the way NAT functions. You can specify the source, destination and service separately for both the original and the translated packet.

When creating Manual NAT rules, you must define the translated network objects in addition to the original objects.

## Automatic Hide NAT for Internal Networks

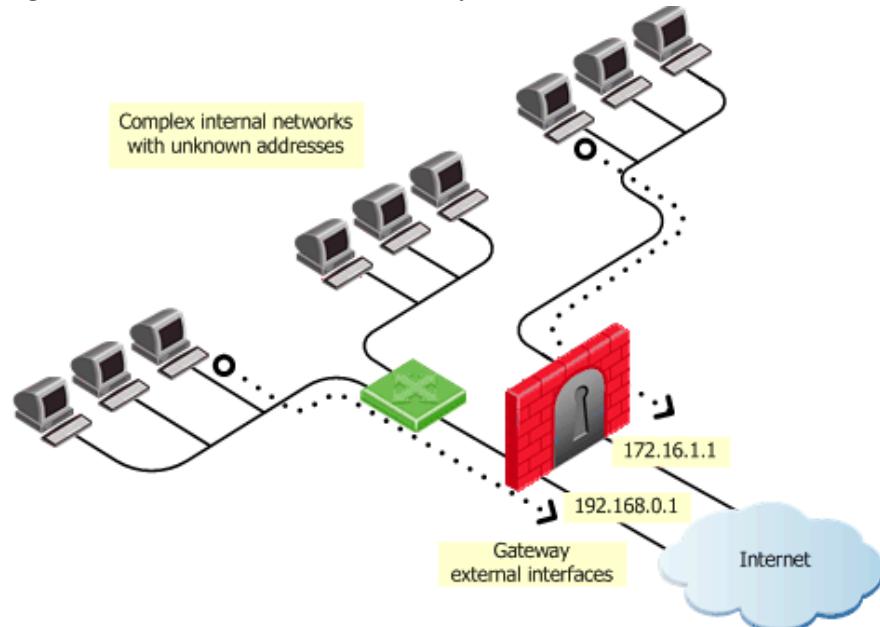
You can use Hide NAT to allow Internet access for large and complex internal networks that contain many subnets, not all of which may be known.

Regular Hide NAT requires that all internal network addresses to be NATed must be specified, even though this may be impractical.

If this is the case, you can specify automatic Hide NAT for all internal networks. Every connection entering from an internal interface and exiting through an external gateway interface (as defined in the **Topology** page of the gateway object) is NATed behind the external gateway interface address.

For example, assume clients in internal networks initiate connections to servers on the Internet. The source addresses of internal clients are NATed to the address of the external interface, either **192.168.0.1** or **172.16.1.1**, depending on the interface from which the connection emerges.

**Figure 3-3** Hide NAT Behind Gateway Interface



**Note** - Regular NAT rules take precedence over NAT-for-internal-networks rules. If a connection matches both NAT rule types, the connection is matched to the regular NAT rule.

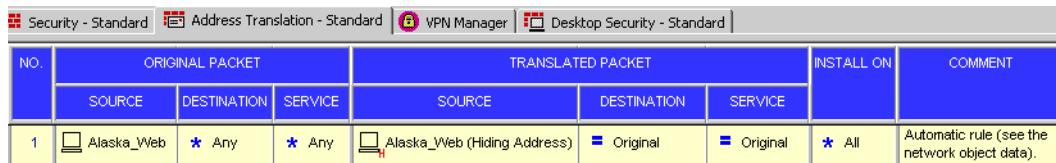
Access rules must also be defined in the Rule Base.

See also “[Configuring Automatic Hide NAT for Internal Networks](#)” on page 122.

# NAT Rule Base

[Figure 3-4](#) shows the NAT Rule Base.

**Figure 3-4** NAT Rule Base



The screenshot shows a software interface titled "Address Translation - Standard". The window has tabs at the top: "Security - Standard", "Address Translation - Standard" (which is selected), "VPN Manager", and "Desktop Security - Standard". Below the tabs is a table titled "NAT Rule Base". The table has columns: NO., ORIGINAL PACKET (with sub-columns SOURCE, DESTINATION, SERVICE), TRANSLATED PACKET (with sub-columns SOURCE, DESTINATION, SERVICE), INSTALL ON, and COMMENT. A single rule is listed:

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	<input type="checkbox"/> Alaska_Web	* Any	* Any	<input type="checkbox"/> Alaska_Web (Hiding Address)	= Original	= Original	* All	Automatic rule (see the network object data).

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 NAT Rule Base is divided into two sections:

- **Original Packet:** Specifies the conditions when the rule is applied.
- **Translated Packet:** Specifies the action taken when the rule is applied.

Each section in the NAT Rule Base Editor is divided into Source, Destination, and Service. The following actions are performed:

- 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 NAT Rule Base follows the same principle as in the Rule Base. When the firewall receives a packet belonging to a connection, it first compares it against the first rule in the Rule Base, then the second rule, and then the third rule, and so on. When it finds a rule that matches, it stops checking and applies that rule.

The exception to this principle is when two automatic rules match a connection, in which case, bidirectional NAT is applied.

## Bidirectional NAT

Bidirectional NAT applies to automatic NAT rules in the NAT 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 network objects, where one is the source of a connection and the other is the destination, using bidirectional NAT, both automatic NAT rules are applied and both objects are translated.

The logic behind bidirectional NAT is:

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

The operation of bidirectional NAT can be tracked using the SmartView Tracker and the **NAT Rule Number** and **NAT Additional Rule Number** fields . 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 through a network object (node, network or address range), with rules added automatically to the NAT Rule Base.

Hide NAT on a node adds one rule to the NAT Rule Base. It specifies that the source address of the packet is translated for connections originating from the node in the internal network (Source Hide Rule).

Static NAT on a node adds two rules to the NAT Rule Base. In addition to the Source Hide rule, another rule specifies that for connections originating from the external network, the Destination address of the packet is translated (Destination Static Rule).

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

## ***Example of Automatically Generated Rule (Hide NAT)***

In the scenario displayed in [Figure 3-2 on page 103](#), automatically defined Hide NAT on the address range node adds two rules to the NAT Rule Base ([Figure 3-5](#)).

**Figure 3-5**      Automatically Generated NAT Rules for Hide NAT on an Address Range

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	IP ↔ Range_Hide	IP ↔ Range_Hide	* Any	= Original	= Original	= Original	* All	Automatic rule (see the network object data).
2	IP ↔ Range_Hide	* Any	* Any	IP ↔ Range_Hide (Hiding Address)	= Original	= Original	* All	Automatic rule (see the network object data).

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

Rule 2 states 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 is used on the unprotected side of the Security Gateway. The actual addresses are private addresses that are used on the protected side of the Security Gateway.

## ***Example of Automatically Generated Rules (Static NAT)***

In the scenario in [Figure 3-1 on page 101](#), automatically defined Static NAT on the node adds two rules to the NAT Rule Base ([Figure 3-6](#)).

**Figure 3-6**    Automatically Generated NAT Rules for Static NAT on an Address Range

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALLATION	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	IP Range_static	IP Range_static	* Any	= Original	= Original	= Original	* All	Automatic rule (see the network object data).
2	IP Range_static	* Any	* Any	IP Range_static (Valid Addresses)	= Original	= Original	* All	Automatic rule (see the network object data).
3	* Any	IP Range_static (Valid Addresses)	* Any	= Original	IP Range_static	= Original	* All	Automatic rule (see the network object data).

Rule 1 states 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 states that for packets originating from the internal (protected) side of the firewall, source addresses are translated to valid (public) static NAT addresses.

Rule 3 states that for packets originating from 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 are used on the unprotected side of the Security Gateway. The actual addresses are private addresses that are used on the protected side of the Security Gateway.

## ***Order of Automatic Rules***

Automatic rules are placed in the NAT Rule Base in the following order:

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 a single IP address, based on the requested service (or destination port), which saves scarce public IP addresses. A typical implementation enables 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 create manual NAT rules. Port Translation rules are supported on Security Gateways of versions NG FP3 and higher.

## NAT and Anti-Spoofing

NAT is performed after anti-spoofing checks, which are performed only on the source IP address of the packet. This means that spoofing protection is configured on the interfaces of the Security Gateway in the same way as NAT. Unlike in previous versions of Check Point Security Gateway, there are no special requirements for anti-spoofing configuration and NAT.

## Routing Issues

### ***Static Routes on the Check Point Security Gateway***

This section is intended for administrators who have upgraded the Security Management server, where in the pre-upgrade:

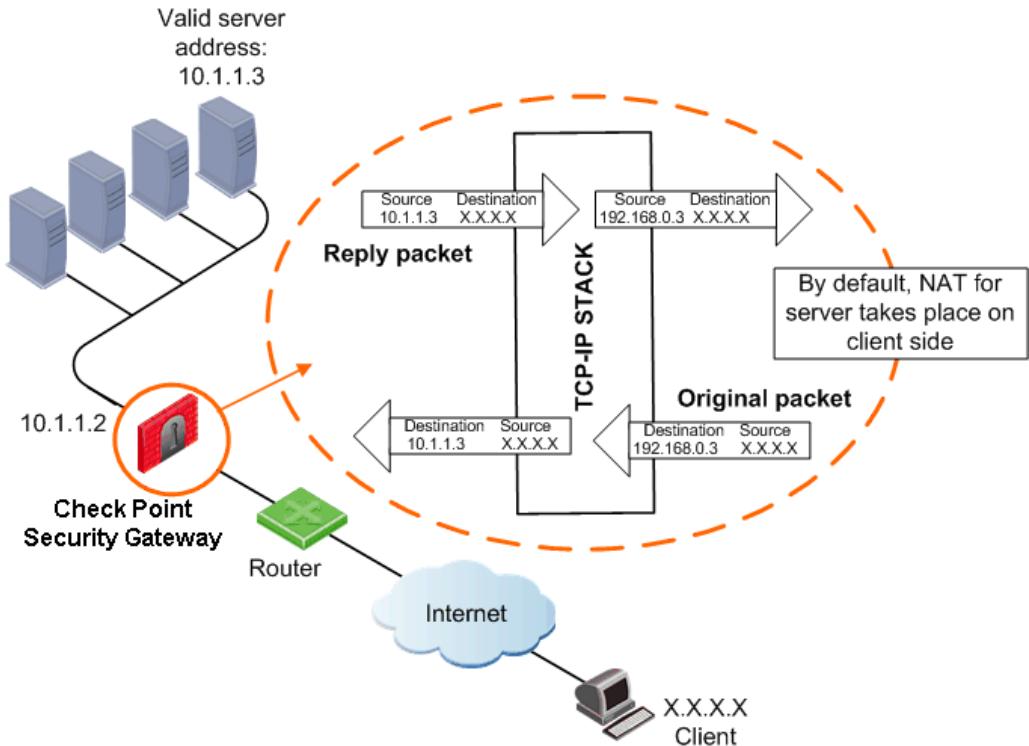
- Automatic NAT for the server was performed on the server side for pre-NG versions, or
- Manual NAT for the server was performed on the server side for pre-NG FP3 versions.

For a client-server connection that crosses the Security Gateway, connections originate at the client and the server sends reply packets back to the client.

In NG or higher versions of Security Gateways, for both manual and automatic rules, NAT for the server is performed by default on the client side of the gateway, which ensures that the operating system routes the packets correctly.

For the original packet, the Security Gateway translates the destination address to the valid address of the server and then routes the packet to its destination.

For reply packets, no NAT is performed on the destination, and the operating system correctly routes the packet back to the client.

**Figure 3-7** NAT on the Client Side

The default setting for NG and higher versions ensures reliable anti-spoofing and routing. It is recommended to leave the default setting unless you have upgraded your Security Management server from a pre-NG version gateway whose configuration requires other settings.

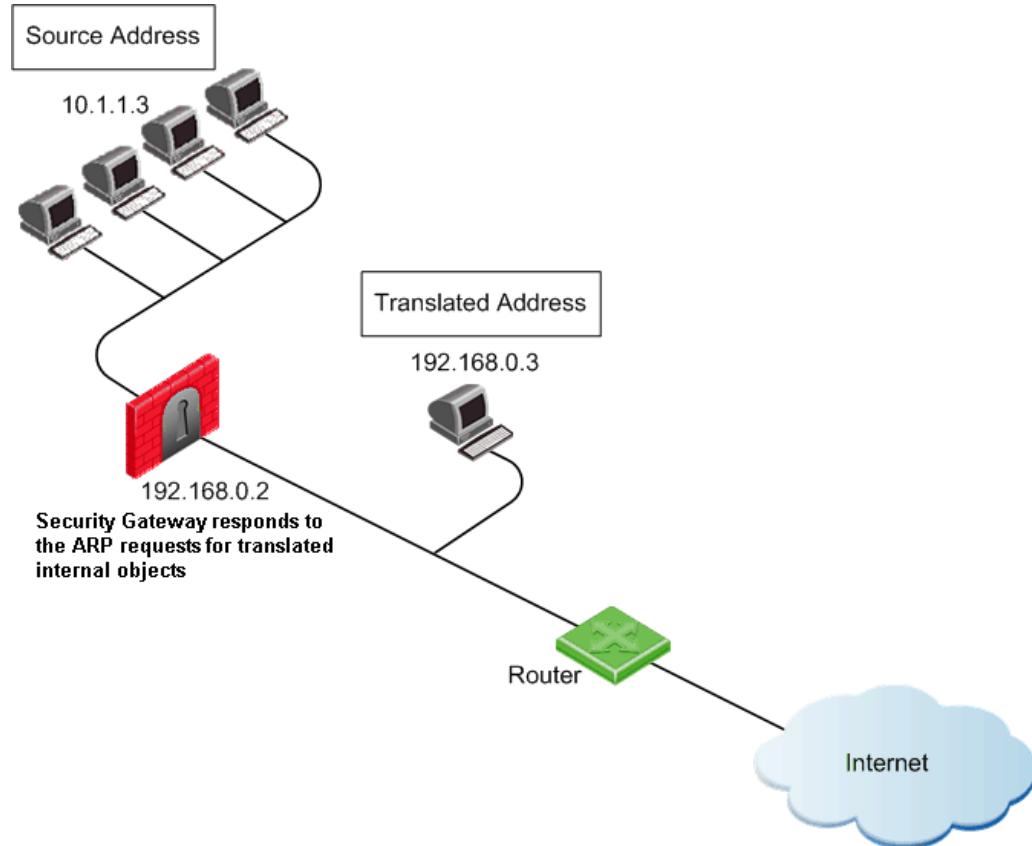
If NAT for the server destination is performed on the server side, the operating system receives the packet for routing before NAT is performed. The operating system therefore sees a valid address as the destination, and routes the packet back to the Internet router rather than to the server. To resolve this, configure Static Host Routes on the Check Point Security 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, or the Internet side of the firewall.

When NAT is configured automatically, the Check Point Security Gateway replies on behalf of translated network objects to ARP requests from the Internet router for the address of the internal machine.

**Figure 3-8** Automatic ARP Configuration



If you are using manual rules, you must configure proxy ARPs to associate the translated IP address with the MAC address of the Check Point Security Gateway interface that is on the same network as the translated addresses.

## Disabling NAT in a VPN Tunnel

When communicating within a VPN, it is normally not necessary to perform NAT. You can 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 slows down the performance of the VPN.

# Planning Considerations for NAT

## In This Section

<a href="#">Hide Versus Static</a>	<a href="#">page 114</a>
<a href="#">Automatic Versus Manual Rules</a>	<a href="#">page 114</a>
<a href="#">Choosing the Hide Address in Hide NAT</a>	<a href="#">page 115</a>

## 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 therefore are less prone to configuration errors. Automatic ARP configuration is only effective for automatic rules.

Manually defining NAT rules can be complicated, but it gives you complete control over NAT. The following operations can only be performed using manual NAT rules:

- Restricting rules to specified destination IP addresses and to specified source IP addresses.
- Translating both source and destination IP addresses in the same packet.
- Performing Static NAT in only 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 hide behind either the interface of the Install on Gateway or a specified IP address.

Choosing a fixed public IP address is a good option if you want to hide the address of the Security Gateway, however, it means you have to use an extra publicly routable IP address.

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

# Configuring NAT

## In This Section

<a href="#">General Steps for Configuring NAT</a>	<a href="#">page 116</a>
<a href="#">Basic Configuration (Network Node with Hide NAT)</a>	<a href="#">page 117</a>
<a href="#">Sample Configuration (Static and Hide NAT)</a>	<a href="#">page 119</a>
<a href="#">Sample Configuration (Using Manual Rules for Port Translation)</a>	<a href="#">page 121</a>
<a href="#">Configuring Automatic Hide NAT for Internal Networks</a>	<a href="#">page 122</a>

## General Steps for Configuring NAT

To configure NAT:

1. Determine the IP addresses to be used for translation.
2. Define the network objects.
3. Define the Access rules in the Rule Base. When defining Manual NAT rules, you must define network objects with translated addresses. If using Automatic NAT rules, you must define only one network object per real object. For example, if Static NAT is defined on an object called Alaska\_Web, then the Rule Base only needs to refer to Alaska\_Web, and there is no need to define a rule for Alaska\_Web (Valid Address).

**Table 3-1** NAT Rule

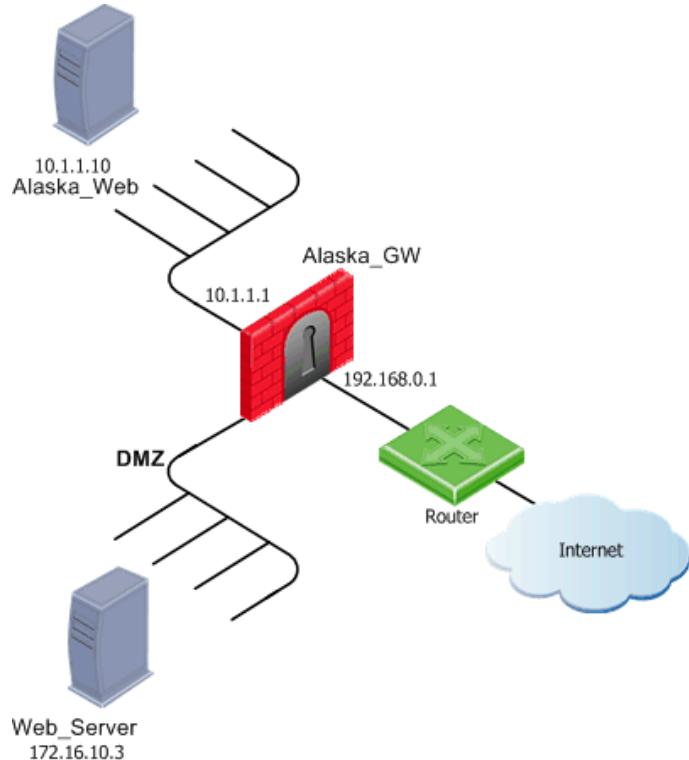
Source	Destination	Action
Any	Alaska_Web	Accept

4. Define NAT rules (automatic and/or manual).
5. Install the security policy: **Policy > Install**.

## Basic Configuration (Network Node with Hide NAT)

For example, assume a basic configuration for a network node with Hide NAT. Its goal 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 where Alaska\_Web resides.

**Figure 3-9** Network Node with Hide NAT



To configure a 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 3-10** Hide NAT Configuration



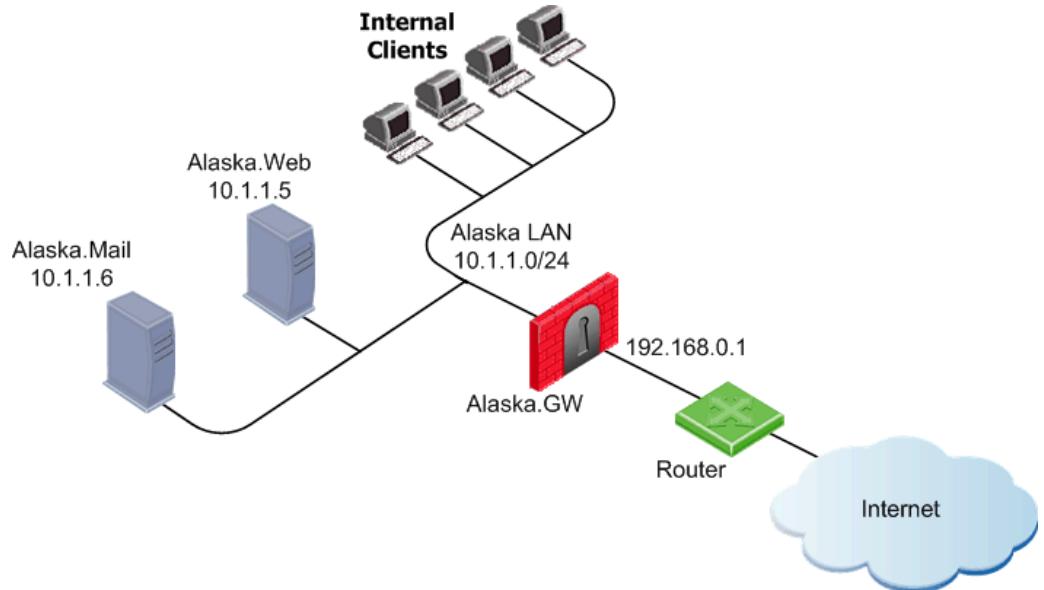
2. Select **Translation Method Hide** and the **Hide behind the interface of the Install on Gateway** option.
3. Select **Install on Gateway**. In this example, the NAT gateway is Alaska\_GW, therefore, select either **Alaska\_GW** or **All**.

Packets originating from Alaska\_Web, with the Internet as their destination, have their source address translated from 10.1.1.10 to 192.168.0.1. For example, packets originating from the Web server have their source address changed from 172.16.10.3 to 192.168.0.1.

## Sample Configuration (Static and Hide NAT)

In this next example, the objective is make the SMTP and the HTTP servers on the internal network available to the Internet using public addresses and to provide Internet access to all users on the internal network.

**Figure 3-11** Sample Configuration (Static and Hide NAT)



The Web and mail servers require static translation because incoming connections are made to them from the Internet. Two routable addresses are available. In this example, **192.168.0.5** is used for the Alaska.Web HTTP server and **192.168.0.6** is used 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 Security Gateway.

To perform a sample configuration with Static and Hide NAT:

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 Check Point Security Gateway (Alaska.GW).
2. Edit the Alaska.Web object and in the **NAT** page, select **Add Automatic Address Translation Rules**.

3. Select Static as the **Translation Method** and define the **Translate to IP Address** as **192.168.0.5**.
4. For Alaska.Mail, select Static as the **Translation Method** and define the **Translate to IP Address** as **192.168.0.6**.
5. Edit the Alaska\_LAN object and in the **NAT** page, select Hide as the **Translation Method** and then 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**. [Figure 3-12](#) displays the resulting NAT Rule Base.

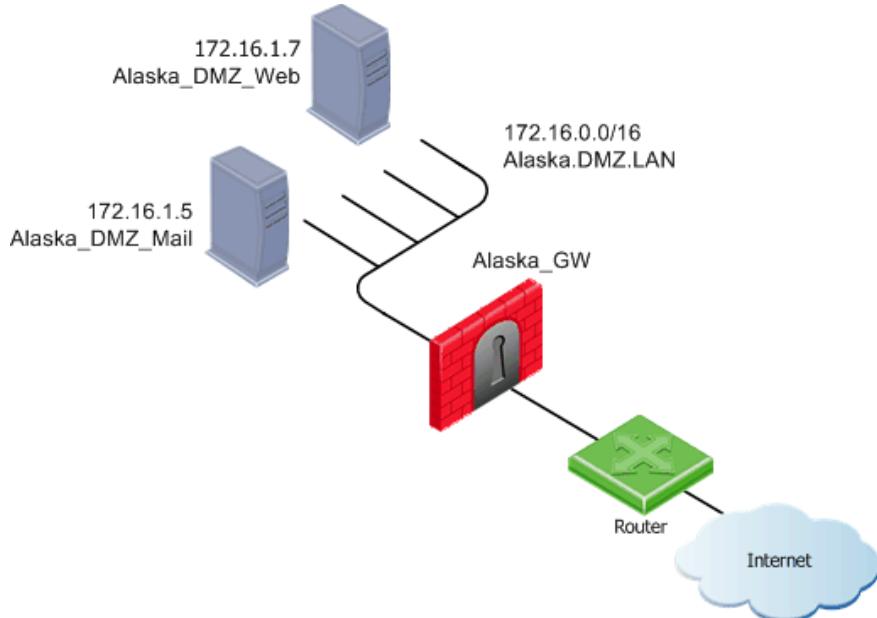
**Figure 3-12** Automatic NAT Rule Base for Static and Hide NAT

NO	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE	
1	Alaska.Mail	* Any	* Any	Alaska.Mail (Valid Address)	= Original	= Original	* All
2	* Any	Alaska.Mail (Valid Address)	* Any	= Original	Alaska.Mail	= Original	* All
3	Alaska.Web	* Any	* Any	Alaska.Web (Valid Address)	= Original	= Original	* All
4	* Any	Alaska.Web (Valid Address)	* Any	= Original	Alaska.Web	= Original	* All
5	Alaska_LAN	Alaska_LAN	* Any	= Original	= Original	= Original	* All
6	Alaska_LAN	* Any	* Any	Alaska_LAN (Hiding Address)	= Original	= Original	* All

## Sample Configuration (Using Manual Rules for Port Translation)

In [Figure 3-13](#), the objective is to make both a Web server and a mail server in a DMZ network available from the Internet using a single IP address. Hide NAT is performed on all addresses in the DMZ.

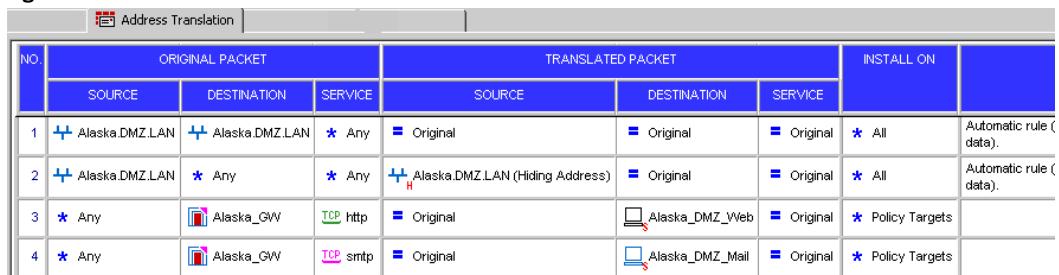
**Figure 3-13** Sample Configuration (Port Translation using Manual NAT)



To perform a sample configuration using manual rules for port translation:

1. Define network objects for the network Alaska.DMZ.LAN (172.16.0.0 with Net Mask 255.255.0.0), the Web server Alaska\_DMZ\_Web (172.16.1.7), the Mail server Alaska\_DMZ\_Mail (172.16.1.5) and the Check Point Security Gateway (Alaska.GW).
2. In the **NAT** tab on the Alaska.DMZ.LAN network object, select **Add Automatic Address Translation Rules**.
3. Select **Hide** as the **Translation Method** and then **Hide behind the interface of the Install on Gateway**. This step adds two automatic rules to the NAT Rule Base (Rules 1 and 2 in [Figure 3-14](#)).

4. In the NAT Rule Base, define a Manual NAT rule that translates requests for the HTTP service to the Web server (Rule 3 in [Figure 3-14](#)) and a Manual NAT rule to translate SMTP requests to the SMTP server (Rule 4 in [Figure 3-14](#)).

**Figure 3-14** NAT Rule Base for Port Translation


The screenshot shows the NAT Rule Base interface with the following details:

NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	Alaska_DMZ_LAN	Alaska_DMZ_LAN	* Any	Original	Original	Original	* All	Automatic rule (data).
2	Alaska_DMZ_LAN	* Any	* Any	Alaska_DMZ_LAN (Hiding Address)	Original	Original	* All	Automatic rule (data).
3	* Any	Alaska_GW	http	Original	Alaska_DMZ_Web	Original	* Policy Targets	
4	* Any	Alaska_GW	smtp	Original	Alaska_DMZ_Mail	Original	* Policy Targets	

## Configuring Automatic Hide NAT for Internal Networks

To configure automatic Hide NAT for internal networks:

1. Access the **NAT** page of the Check Point gateway object.
2. In the **Automatic Hide for Internal Networks** section, either select or clear the **Hide all connections from internal interfaces to external interfaces behind the gateway** option.

For additional information on configuring automatic Hide NAT for internal networks, see [“Automatic Hide NAT for Internal Networks” on page 105.](#)

# Advanced NAT Configuration

## In This Section

<a href="#">Connecting Translated Objects on Different Interfaces</a>	page 123
<a href="#">Internal Communication with Overlapping Addresses</a>	page 123
<a href="#">Security Management Behind NAT</a>	page 128
<a href="#">IP Pool NAT</a>	page 132

## Connecting Translated Objects on Different Interfaces

The following sections describe how to allow connections in both directions between statically translated objects (nodes, networks or address ranges) on different Check Point Security Gateway interfaces.

If NAT is defined through the network object (as opposed to using Manual NAT Rules), then you must ensure that bidirectional NAT is enabled.

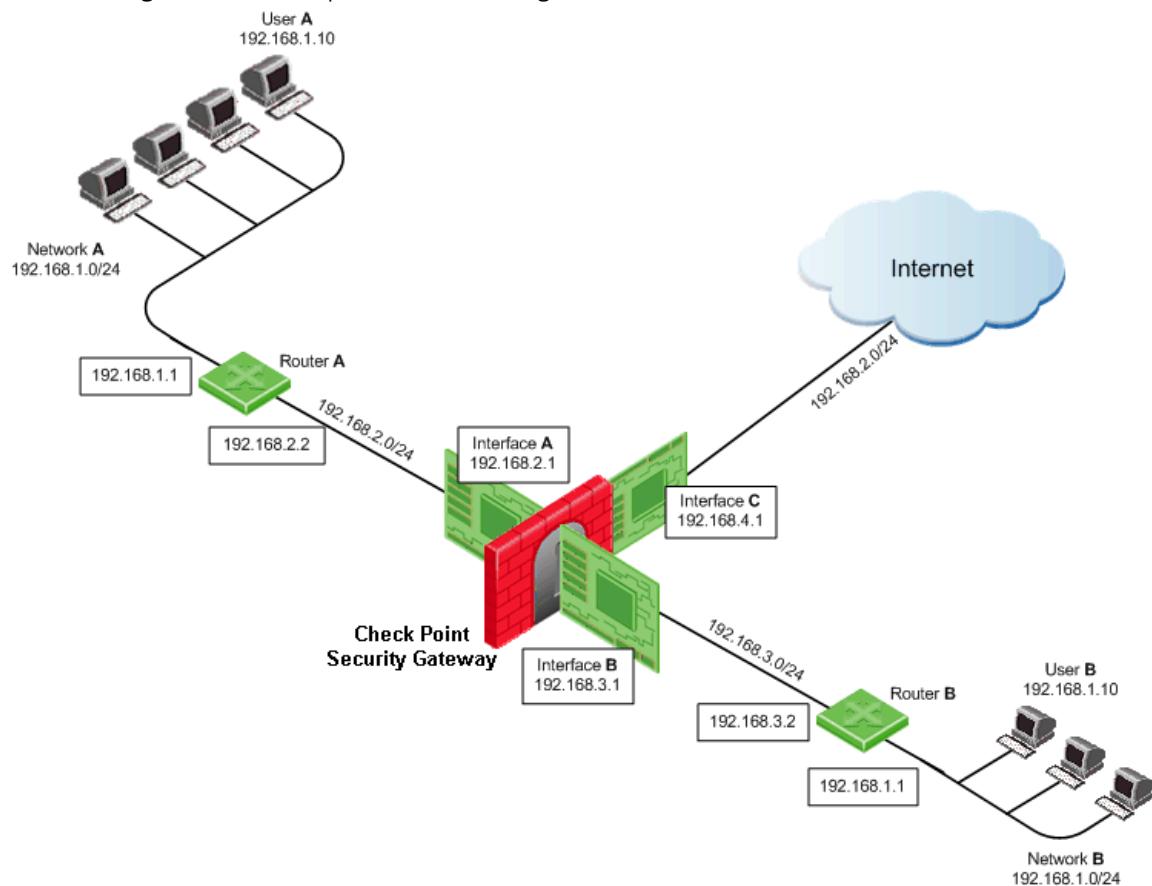
## Internal Communication with Overlapping Addresses

If two internal networks have overlapping (or partially overlapping) IP addresses, Check Point Security Gateway enables:

- Communication between the overlapping internal networks.
- Communication between the overlapping internal networks and the outside world.
- Enforcement of a different security policy for each of the overlapping internal networks.

## Network Configuration

**Figure 3-15** Sample Network Configuration: Class C Network



For example, assume both Network A and Network B share the same address space (**192.168.1.0/24**), therefore standard NAT cannot be used to enable communication between the two networks. Instead, overlapping NAT must be performed on a per interface basis.

Users in Network A who want to communicate with users in Network B must use the **192.168.3.0/24** network as a destination. Users in Network B who want to communicate with users in Network A must use the **192.168.2.0/24** network as a destination.

The Check Point Security Gateway translates the IP addresses in the following way for each individual interface:

**Interface A**

- Inbound source IP addresses are translated to the virtual network **192.168.20.0/24**.
- Outbound destination IP addresses are translated to the network **192.168.1.0/24**.

**Interface B**

- Inbound source IP addresses are translated to the network **192.168.30.0/24**.
- Outbound destination IP addresses are translated to the network **192.168.1.0/24**.

**Interface C**

Overlapping NAT is not configured for this interface. Instead, use NAT Hide in the normal way (not on a per-interface basis) to hide source addresses behind the interface's IP address (**192.168.4.1**).

***Communication Examples***

This section describes how to enable communication between internal networks, and between an internal network and the Internet.

**Communication Between Internal Networks**

If user A, at IP address **192.168.1.10** in Network A, wants 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 the IP address **192.168.30.10**.

**Table 3-2**    Communication Between Internal Networks

Step	Source IP address	Destination IP address
Interface A — before NAT	<b>192.168.1.10</b>	<b>192.168.30.10</b>
Interface A — after NAT	<b>192.168.20.10</b>	<b>192.168.30.10</b>
Security Gateway enforces the security policy for packets from network <b>192.168.20.0/24</b> to network <b>192.168.30.0/24</b> .		
Interface B — before NAT	<b>192.168.20.10</b>	<b>192.168.30.10</b>
Interface B — after NAT	<b>192.168.20.10</b>	<b>192.168.1.10</b>

## Communication Between an Internal Network and the Internet

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

**Table 3-3** Communication Between an Internal Network and the Internet

Step	Source IP address	Destination IP address
Interface A — before NAT	192.168.1.10	10.10.10.10
Interface A — after NAT	192.168.20.10	10.10.10.10
Security gateway enforces the security policy for packets from network 192.168.20.0/24 to the Internet.		
Interface C — before NAT	192.168.20.10	10.10.10.10
Interface C — after NAT Hide	192.168.4.1	10.10.10.10

## ***Routing Considerations***

To allow routing from Network A to Network B, routing must be configured on the firewall machine.

The following are routing command examples for Windows and Linux operating systems (for other operating systems, use the equivalent commands):

### **On Windows**

- `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**

- `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`

## ***Object Database Configuration***

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

In the sample network configuration, the per interface values for interface A and interface B are set in the following way:

**Table 3-4**    Sample Network Configuration: Interface Configuration

Parameter	Value
<code>enable_overlapping_nat</code>	<code>true</code>
<code>overlap_nat_dst_ipaddr</code>	The overlapping IP addresses (before NAT). In the sample network configuration, <b>192.168.1.0</b> for both interfaces.
<code>overlap_nat_src_ipaddr</code>	The IP addresses after NAT. In the sample network configuration, <b>192.168.20.0</b> for interface A, and <b>192.168.30.0</b> for interface B.
<code>overlap_nat_netmask</code>	The net mask of the overlapping IP addresses. In the sample network configuration, <b>255.255.255.0</b> .

## Security Management Behind NAT

The Security Management server sometimes uses a private IP address (as listed in RFC 1918) or some other non-routable IP address, because of the lack of public IP addresses.

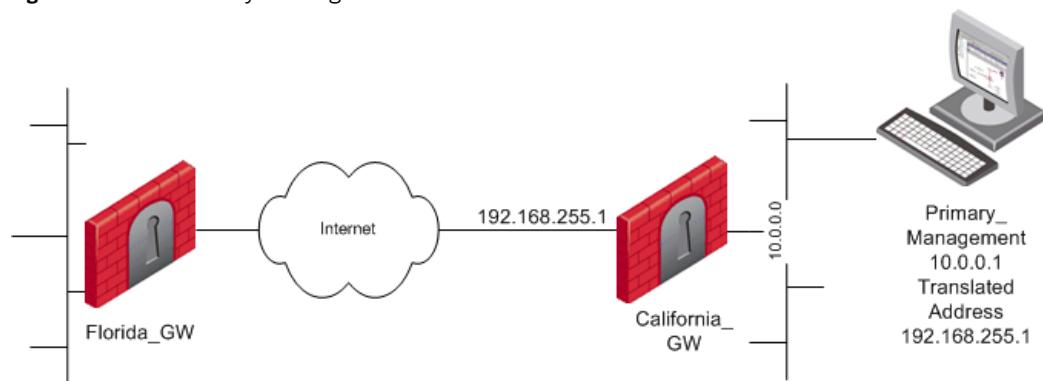
NAT (Static or Hide) for the Security Management server IP address can be configured in one click, while still allowing connectivity with managed gateways. All gateways can be controlled from the Security Management server, and logs can be sent to the Security Management server. NAT can also be configured for a Management High Availability server and a Log server.



**Note** - Security Management behind NAT is not supported for deployments where the Security Management server also acts as a gateway and must be addressed from outside the NATed domain, for example, when it receives SAM commands.

In a typical Security Management Behind NAT scenario: the Security Management server is in a network on which Network Address Translation is performed (the “NATed network”). The Security Management server can control Check Point gateways inside the NATed network, on the border between the NATed network and the outside world and outside the NATed network.

**Figure 3-16** Security Management Behind NAT Scenario



In ordinary Hide NAT configurations, connections cannot be established from the external side the NAT Security Gateway. However, when using Hide NAT on the Security Management server, gateways can send logs to the Security Management server.

When using the Security Management behind NAT feature, the remote gateway automatically selects the Security Management address to be addressed and simultaneously applies NAT considerations.

To enable NAT for the Security Management server:

- From the **NAT** page of the Security Management server object, define NAT and select **Apply for Security Gateway control connections**.

## ***Non-Corresponding Gateway Addresses***

Sometimes the gateway contacts the Security Management with an address that does not correspond to the remote gateway's deployment, for example:

- When there are gateways from a version prior to NG with Application Intelligence. For more information, see the *Security Management server with NAT* document, available from SecureKnowledge solution sk15558 at: <http://supportcontent.checkpoint.com/solutions?id=sk15558>
- When the gateway's automatic selection does not conform with the routing of the gateway's deployment. In this case, define the masters and loggers manually, to allow the remote gateway to contact the Security Management server using the required address. When an inbound connection from a managed gateway enters the Security Gateway, port translation is used to translate the hide address to the real IP address of the Security Management server.

To define masters and loggers, select **Use local definitions for Log Servers** and **Use local definitions for Masters** and specify the correct IP addresses on the gateway.

This solution encompasses different scenarios:

- The remote gateway addresses the NATed IP when you want it to address the real IP.
- The remote gateway addresses the real IP when you want it to address the NATed IP. In this case, specify the SIC name of the Security Management server in the masters file.

Notes:

- Only one object can be defined with these settings, unless the second object is defined as a Secondary Security Management server or as a Log server.
- Ensure that you properly define the Topology settings on all gateways. In [Figure 3-16](#), on California\_GW, define Primary\_Security\_Management on its internal interface.
- All managed gateways and the Security Management server must be of version NG with Application Intelligence or higher.
- All work-arounds required for previous versions still function with no changes in their behavior.

## ***Configuring the Security Management server Object***

To configure the Security Management server object:

1. From the **NAT** page on the Primary\_Security\_Management object, select either Static NAT or Hide NAT. If using Hide NAT, select **Hide behind IP Address**, for example, 192.168.55.1. Do not select **Hide behind Gateway** (address 0.0.0.0).
2. Select **Install on Gateway** to protect the NATed objects or network. Do not select **All**. For example, in [Figure 3-16](#), **Install on Gateway**: California\_GW.
3. Select **Apply for Security Gateway control connections**.

## ***Configuring the Gateway Object***

Using the example provided in [Figure 3-16](#), ensure that the California\_GW knows that the Primary\_Security\_Management is behind it.

To configure the gateway object:

1. From the California\_GW **Topology** page, define Interface Eth3.
2. In the **General** tab of the **Interface Properties** window, define the **IP Address** 10.0.0.0 and the **Netmask** 255.255.0.0.

In the **Topology** tab of the **Interface Properties** window, select **Network defined by the interface IP and Net Mask**.

### Configuring Earlier-Version Gateway Objects

For managed gateways that are earlier versions, with Application Intelligence, you must define a dummy object. Using the example provided in [Figure 3-16](#), 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 Security Management server has the address 192.168.255.1 and California\_GW knows that its Security Management server has the address 10.0.0.1.

To configure pre-NG version with Application Intelligence gateway objects:

1. Define a dummy object with the translated address of the Primary\_Security\_Management.
1. Name it, for example, Dummy-Security Management.
2. in the **Check Point Products** section of the **General Properties** page, select **Secondary Management Station** and **Log Server**.

3. Define a dummy object for the California\_GW object by doing the following:
  - a. Name it.
  - b. Assign the **IP Address** 192.168.255.1.
  - c. Assign the address of the Primary Security Management NAT definition.
  - d. In the **Check Point Products** section of the **General Properties** page, select **Secondary Management Station** and **Log Server**.
  - e. In the **Logs and Masters** page:
    - i. Define the dummy object as a Master.
    - ii. Define the dummy object as a Log server (if the Log server is on a separate machine, define two virtual objects).

## 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) that is routable to the gateway. IP Pool NAT ensures proper routing for encrypted connections for the following 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 packets are 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 occurs, each of the MEP gateways maintains a pool of IP addresses that are routable to the gateway. 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 configured in the **IP Pool** page of the gateway object. For additional information on how IP Pool NAT is used in MEP scenarios, see Chapter 11 “Multiple Entry Point VPNs” in the *Virtual Private Networks Administration Guide*.

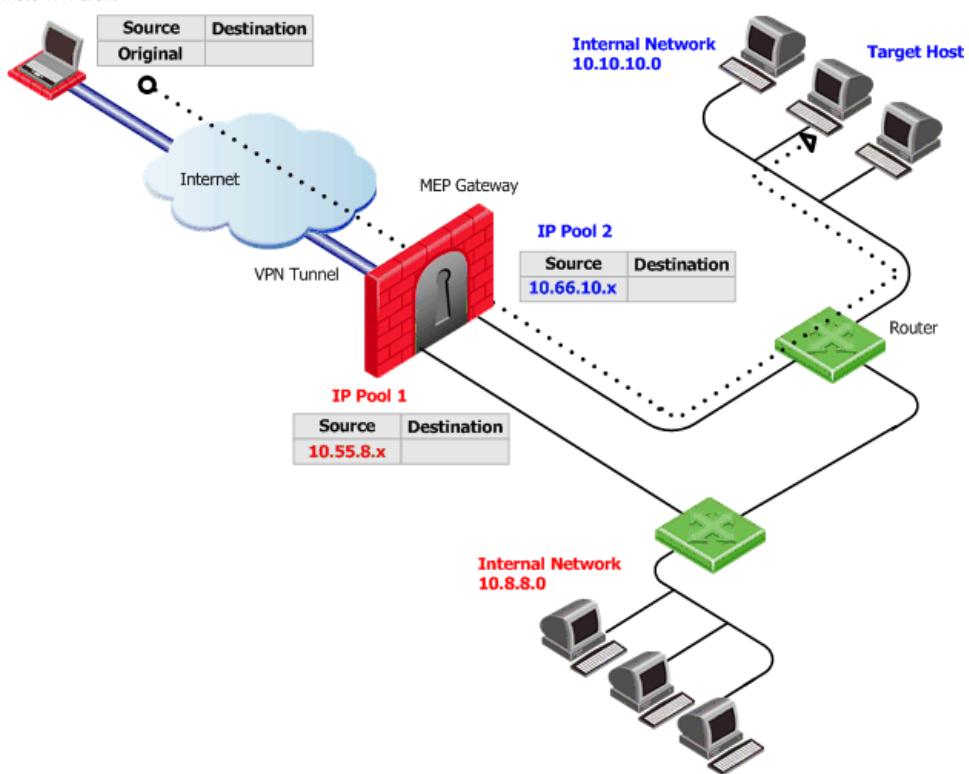
### **IP Pool Per Interface**

You can define a separate IP address pool on one or more of the gateway interfaces instead of defining a single pool of IPs for the gateway.

Defining an IP pool per interface solves routing issues that occur when the gateway has more than two interfaces. Sometimes it is necessary that reply packets return to the gateway through the same gateway interface. [Figure 3-17](#) shows one of the MEP Gateways in a SecuRemote/SecureClient to MEP (Multiple Entry Point) gateway deployment.

**Figure 3-17** IP Pool Per Interface

Remote VPN client



If a remote client opens a connection to the internal network, reply packets from hosts inside the internal networks are routed to the correct gateway interface through the use of static IP pool NAT addresses.

The remote VPN client's IP address is NATed to an address in the IP pool on one of the gateway interfaces. The addresses in the IP pool can be routed only through that gateway interface so that all reply packets from the target host are returned only to that interface. Therefore, it is important that the IP NAT pools of the interfaces do not overlap.

When the packet returns to the gateway interface, the gateway restores the remote peer's source IP address.

The routing tables on the routers that lie behind the gateway must be edited so that addresses from a gateway IP pool are returned to the correct gateway interface.

Switching between IP Pool NAT per gateway and IP Pool NAT per interface and then installing the security policy deletes all IP Pool allocation and all NATed connections.

## NAT Priorities

IP Pool NAT can be used both for encrypted (VPN) and clear (decrypted by the gateway) connections.



**Note** - To enable IP Pool NAT for clear connections through the gateway, configure INSPECT changes in the `user.def` file. For additional information, contact Check Point Technical Support.

For non-encrypted connections, IP Pool NAT has the following advantages over Hide NAT:

- New back connections (for example, X11) can be opened to the NATed host.
- User-to-IP server mapping of protocols that allow one connection per IP can work with a number of hosts instead of only one host.
- IPSec, GRE and IGMP protocols can be NATed using IP Pool NAT (and Static NAT). Hide NAT works only with TCP, UDP and ICMP protocols.

Because of these advantages, you can specify that IP Pool NAT has priority over Hide NAT, if both match the same connection. Hide NAT is only applied if the IP pool is used up.

The order of NAT priorities are:

1. Static NAT
2. IP Pool NAT
3. Hide NAT

Since Static NAT has all of the advantages of IP Pool NAT and more, it has a higher priority than the other NAT methods.

For gateways of versions lower than NGX R60 and for upgraded gateways (by default), the order of NAT priorities are:

1. Static NAT
2. Hide NAT
3. IP Pool NAT

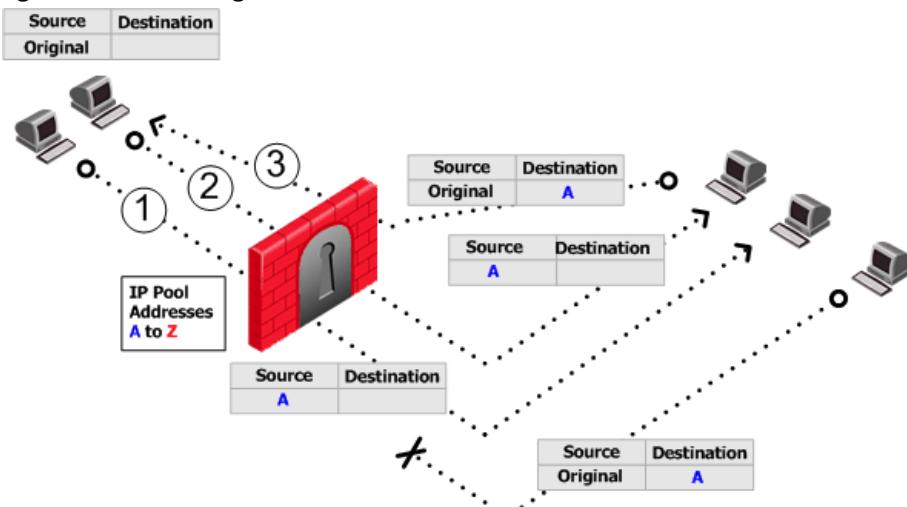
## Reusing IP Pool Addresses For Different Destinations

For pre-NGX R60 gateways that are using IP Pool NAT, if an IP pool contains N addresses, up to N different clients can be NATed.

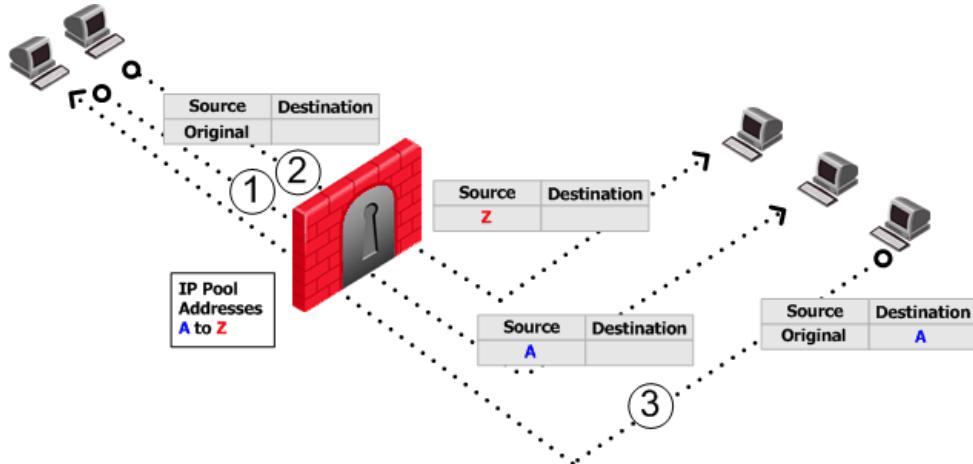
From gateway version NGX R60, IP Pool addresses can be reused for different destinations, which makes more efficient use of the addresses in the pool. If a pool contains N addresses, then any number of clients can be assigned an IP from the pool as long as there are no more than N clients per server.

Using IP Pool allocation per destination, two different clients can receive the same IP from the pool as long as they communicate with different servers (connections 1 and 2 in [Figure 3-18](#)). When reusing addresses from the IP Pool, back connections are supported from the original server only. This means that connections back to the client can be opened only from the specific server to which the connection was opened (connection 3 in [Figure 3-18](#)).

**Figure 3-18** Reusing IP Pool NAT Addresses For Different Destinations



The default **Do not reuse IP Pool** behavior means that each IP address in the IP Pool is used once (connections 1 and 2 in [Figure 3-19](#)). In this mode, if an IP pool contains 20 addresses, up to 20 different clients can be NATed and back connections can be opened from any source to the client (connection 3 in [Figure 3-19](#)).

**Figure 3-19** Do Not Reuse IP Pool NAT Addresses

Switching between Reuse and Do not reuse modes and then installing the security policy, deletes all IP Pool allocations and all NATed connections.

## **Configuring IP Pool NAT**

To configure IP Pool NAT:

1. In the **Global Properties > NAT** page, select **Enable IP Pool NAT** and the required tracking options.
2. In the gateway **General Properties** page, ensure the gateway version is specified correctly. IP Pool NAT can be defined per gateway or, for gateways of version NGX R60 or higher, per gateway interface.
3. For each gateway or gateway interface, create a network object that represents its IP pool NAT addresses. The IP pool can be a network, group, or address range. For example, for an address range, do the following:
  - In the network objects tree, right-click **Network Objects** branch and select **New > Address Range**. The **Address Range Properties** window opens.
  - In the **General** tab, enter the first and last IP of the address range.
  - Click **OK**. The new address range appears in the **Address Ranges** branch of the network objects tree.
4. Select the gateway object, access the **Gateway Properties** window and select **NAT > IP Pool NAT**.

5. In the **IP Pool NAT** page, select one of the following:
  - **Allocate IP Addresses from** and then select the address range you created to configure IP Pool NAT for the whole gateway, or
  - **Define IP Pool addresses on gateway interfaces** to configure IP Pool NAT per interface.
6. If required, select one or more of the following options:
  - **Use IP Pool NAT for VPN client connections**
  - **Use IP Pool NAT for gateway to gateway connections**
  - **Prefer IP Pool NAT over Hide NAT** to specify that IP Pool NAT has priority over Hide NAT, if both match the same connection. Hide NAT is only applied if the IP pool is used up.
7. Click **Advanced**.
  - **Return unused addresses to IP Pool after:** Addresses in the pool are reserved for t60 minutes (default), even if the user logs off. If the user disconnects from their ISP and then redials and reconnects, there will be two Pool NAT addresses in use for the user until the first address from the IP Pool times out. If users regularly lose their ISP connections, you may want to decrease the time-out to prevent the IP Pool from being depleted.
  - **Reuse IP addresses from the pool for different destinations:** This is a good option unless you need to allow back connections to be opened to clients from any source, rather than just from the specific server to which the client originally opened the connection.
8. Click **OK**.
9. Edit the routing table of each internal router so that packets with an a IP address assigned from the NAT pool are routed to the appropriate gateway or, if using IP Pools per interface, the appropriate gateway interface.

## ***IP Pool NAT for Clusters***

IP Pools for gateway clusters are configured in two places in SmartDashboard:

- In the gateway Cluster object **NAT > IP Pool NAT** page, select the connection scenario.
- In the Cluster member object **IP Pool NAT** page, define the IP Pool on the cluster member. A separate IP pool must be configured for each cluster member. It is not possible to define a separate IP Pool for each cluster member interface.

# Chapter

# ISP Redundancy

## In This Chapter

The Need for ISP Link Redundancy	page 140
Solution for ISP Link Redundancy	page 141
Considerations for ISP Link Redundancy	page 154
Configuring ISP Link Redundancy	page 155

# The Need for ISP Link Redundancy

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

A number of solutions are available on the market that enable connections to multiple ISPs, however, these solutions often require expensive and specialized hardware and are difficult to set up and maintain. A simple solution is required that makes use of the existing boundary between the Internet and the organization, which is the firewalled gateway.

# Solution for ISP Link Redundancy

## In This Section

<a href="#">ISP Redundancy Overview</a>	page 141
<a href="#">ISP Redundancy Operational Modes</a>	page 142
<a href="#">Monitoring the ISP Links</a>	page 143
<a href="#">How ISP Redundancy Works</a>	page 143
<a href="#">ISP Redundancy Script</a>	page 146
<a href="#">Manually Changing the Link Status (fw isp_link)</a>	page 146
<a href="#">ISP Redundancy Deployments</a>	page 147
<a href="#">ISP Redundancy and VPNs</a>	page 151

## ISP Redundancy Overview

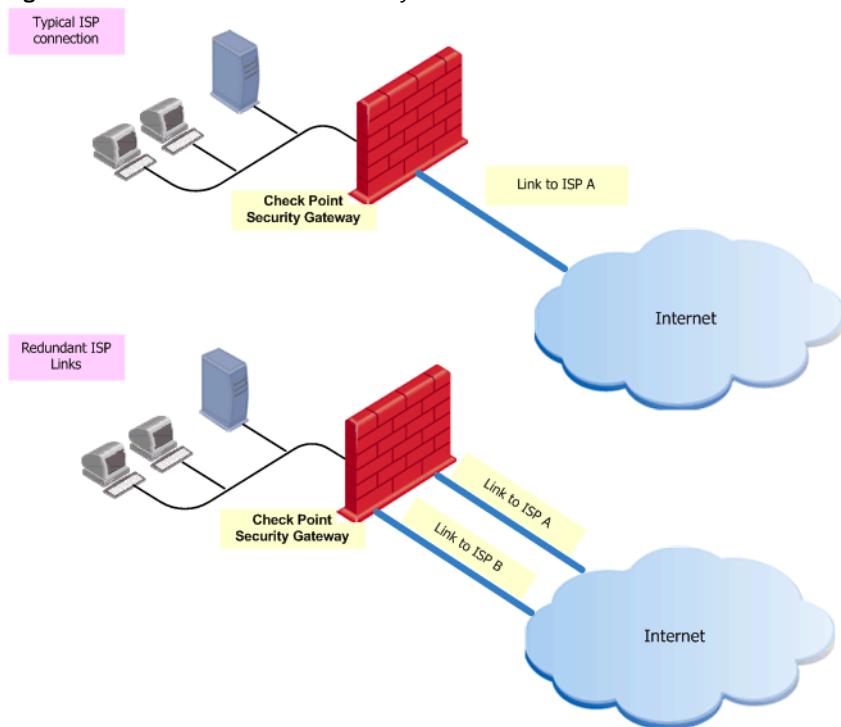
ISP Redundancy assures reliable Internet connectivity by allowing a single or clustered Check Point Security Gateway to connect to the Internet through redundant Internet Service Provider (ISP) links. This feature is part of the standard Security Gateway installation and does not require costly new networking hardware or specialized knowledge to operate.

ISP Redundancy is supported on the following platforms:

- Red Hat Linux 7.2 or higher
- SecurePlatform
- IPSO

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

[Figure 4-1](#) is a typical deployment with a single ISP link and redundant deployment with duplicate ISP links.

**Figure 4-1** ISP Link Redundancy

## ISP Redundancy Operational Modes

The following ISP Redundancy modes control the behavior of outgoing connections from clients in the internal networks to the Internet:

- **Primary/Backup:** 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:** 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 (from the Internet to application servers in the DMZ or internal networks) also benefit from the high availability of the two ISP links because Check Point Security Gateway returns packets using the same ISP Link through which the connection was initiated.

Furthermore, in Load Sharing mode, incoming connections can reach the application servers through either ISP link because Check Point Security Gateway can answer DNS requests for the IP address of internal servers with addresses from both ISPs by alternating their order.

## Monitoring 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, Check Point Security Gateway checks whether or not the interface is running and if the cable is plugged in. The next hop router is monitored automatically.

Another way of monitoring the status of the ISP link is for the administrator to configure a list of hosts that must answer ICMP echo requests (pings) in order for the ISP link to be considered active. If one of the hosts fails to return ICMP replies, the link is considered to be down. You may opt 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 Monitor in the **Firewall** section.

## How ISP Redundancy Works

Both outgoing connections, from behind the Security 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 exits the Security Gateway on its way to the Internet is distributed between the ISP Links. In Primary/Backup mode, outgoing traffic uses an active primary link.

Hide NAT is used to change the source address of outgoing packets to the address of the interface through which the packet leaves the Security Gateway. This allows return packets to be automatically routed through the same ISP link because their destination address is the address of the correct link. Hide NAT is 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 for each ISP. The administrator must also configure Static NAT to translate the routable addresses to the real server address.

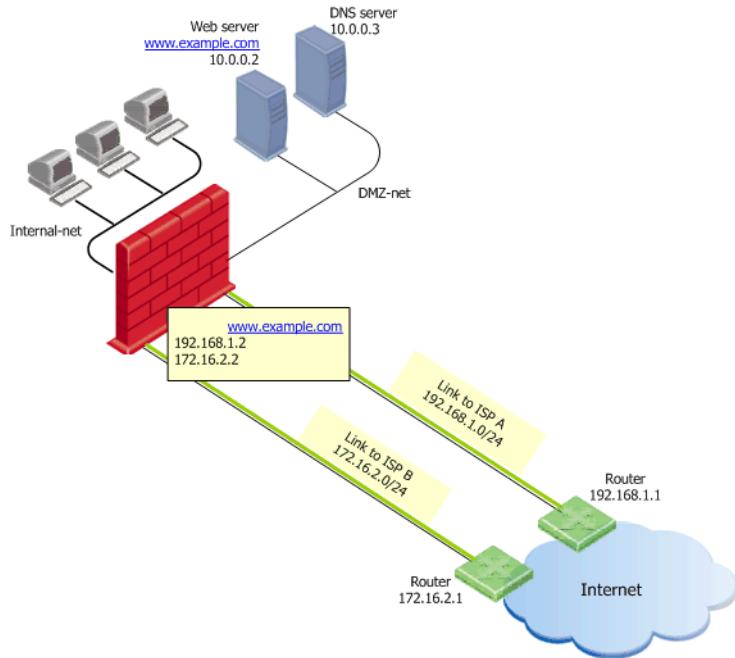
If the servers handle different services (for example, HTTP and FTP), you can use NAT to employ only two routable IP addresses for all the publicly available servers.

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 the following example, the subnets 172.16.0.0/24 and 192.168.0.0/24 represent public routable addresses.

In [Figure 4-2](#), the Web server [www.example.com](http://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 the ISP link A is down, 192.168.1.2 becomes unavailable and the clients must be able to resolve [www.example.com](http://www.example.com) to 172.16.2.2.

**Figure 4-2** IP Address Resolution for Incoming Connections[

The following is a workflow, based on [Figure 4-2](#), of how an incoming connection is established:

1. When a user in the Internet contacts [www.example.com](http://www.example.com), the client machine sends a DNS query for the IP address. The DNS query reaches the Security Gateway. Check Point Security Gateway has a built-in mini-DNS server that can be configured to intercept DNS queries (of type A) for servers in its domain.
2. A DNS query arriving at an interface belonging to one of the ISP links is intercepted by the Security Gateway.
3. If the Security Gateway recognizes the name of the host, it sends one of the following replies:
  - In Primary/Backup mode, Check Point Security Gateway replies only with the addresses associated with the primary link, as long as the primary link is active.
  - In Load Sharing mode, Check Point Security Gateway replies with two addresses, alternating their order.
4. If the Security Gateway is unable to handle DNS requests (for example, it may not recognize the host name), it passes the DNS query to its original destination or the DNS server of the domain [example.com](http://example.com).

5. When the external client receives the reply to its DNS query, it opens a connection. Once the packets reach the gateway, the Security Gateway 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.
6. The Security Gateway routes reply packets from the server to the client through the same ISP link that was used to initiate the connection.

## ISP Redundancy Script

Whenever Check Point Security Gateway starts or an ISP link state changes, a script is run. Depending on whether the ISP link is up or down, this script automatically changes the default route of the Security Gateway. The pathname of the ISP Redundancy script is \$FWDIR/bin/cpisp\_update.

If one of the ISP links is a dialup interface, you can manually edit the ISP Redundancy script to make the Security Gateway change the state of the dialup interface when the ISP links state changes or when the Security Gateway starts.

The script can also be configured to perform other actions, for example, to issue a SAM command to block certain traffic when the primary link is down in order to decrease the traffic load on the link.

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

The `fw isp_link` command is used to configure the ISP link on Check Point Security Gateway to Down or Up and is helpful when:

- Testing your configuration.
- You know the ISP link is down, but the Security Gateway thinks it is up. Use `fw isp_link` to bring the link back up when it becomes available.

This command can be executed locally on the gateway or remotely from the Security Management server. When executed from the Security Management server, you must provide the `fw isp_link [target] link-name up|down target` argument, where <target> is the name of the gateway and <link-name> is the name of the ISP link, as defined in the ISP Redundancy page of the gateway or gateway Cluster object.

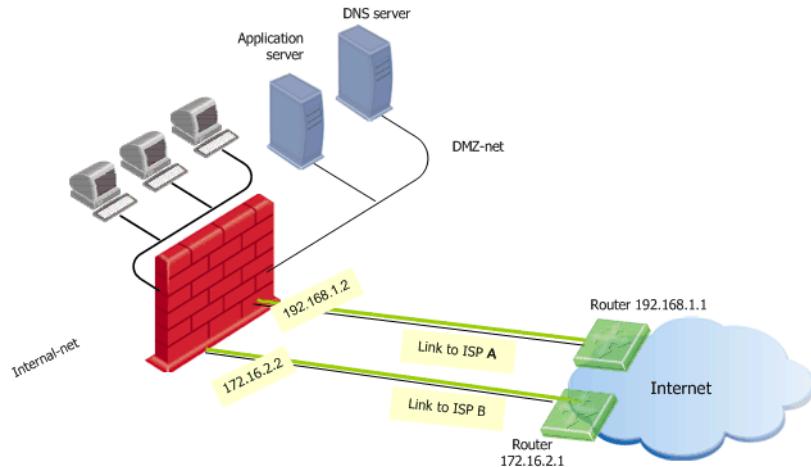
# ISP Redundancy Deployments

A number of deployments are supported. For more information, see “[Considerations for ISP Link Redundancy](#)” on page 154.

## ***Two External Interfaces***

The easiest way to connect to two ISPs is to connect each Security Gateway interface to a different ISP through a LAN. The next hop routers are either at the boundary of the organization or at the ISP.

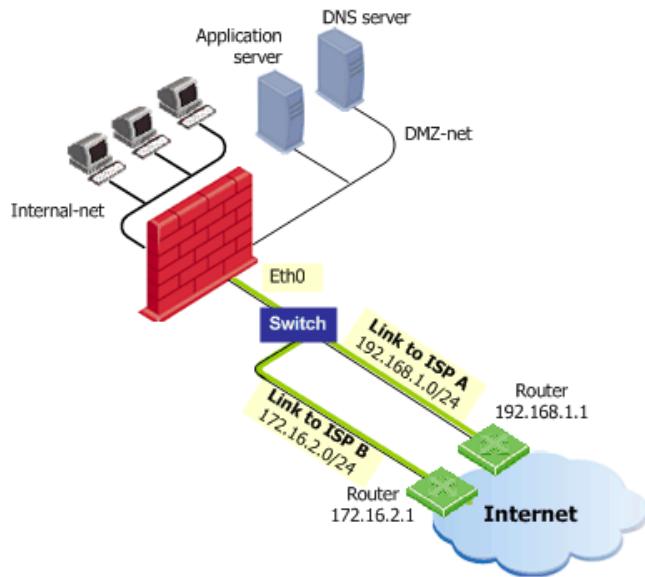
**Figure 4-3** Two ISPs Connected to Different External Security Gateway Interfaces



## One External Interface

If only one external interface is available on the Security Gateway, you can configure two subnets on the same external interface. Both ISP links are then connected to the same Security Gateway interface but to different next hop routers, usually through a switch (Figure 4-4).

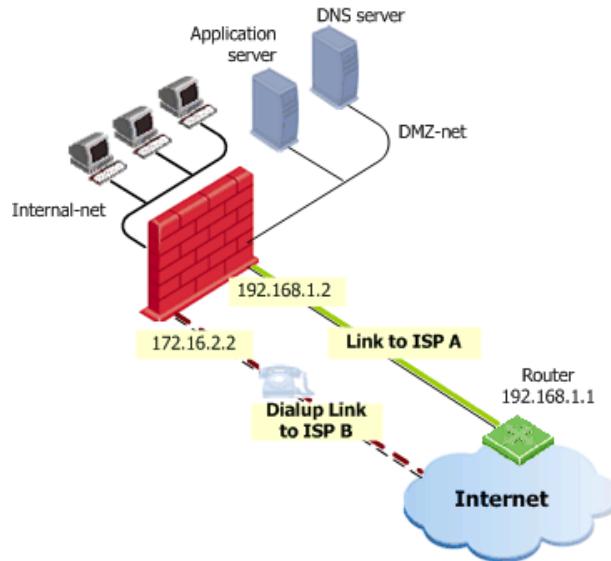
**Figure 4-4** Two ISPs Connected to the Same Security Gateway External Interface



## ***One Permanent and One Dialup (Backup) Interface***

To connect to one of the ISPs through a dialup network (a modem) and to the other ISP through a LAN, connect each Security Gateway external interface to a different ISP link ([Figure 4-5](#)). This deployment is useful if you have a dialup connection to your backup ISP.

**Figure 4-5** One ISP Link a LAN - One ISP Link a Dialup Network

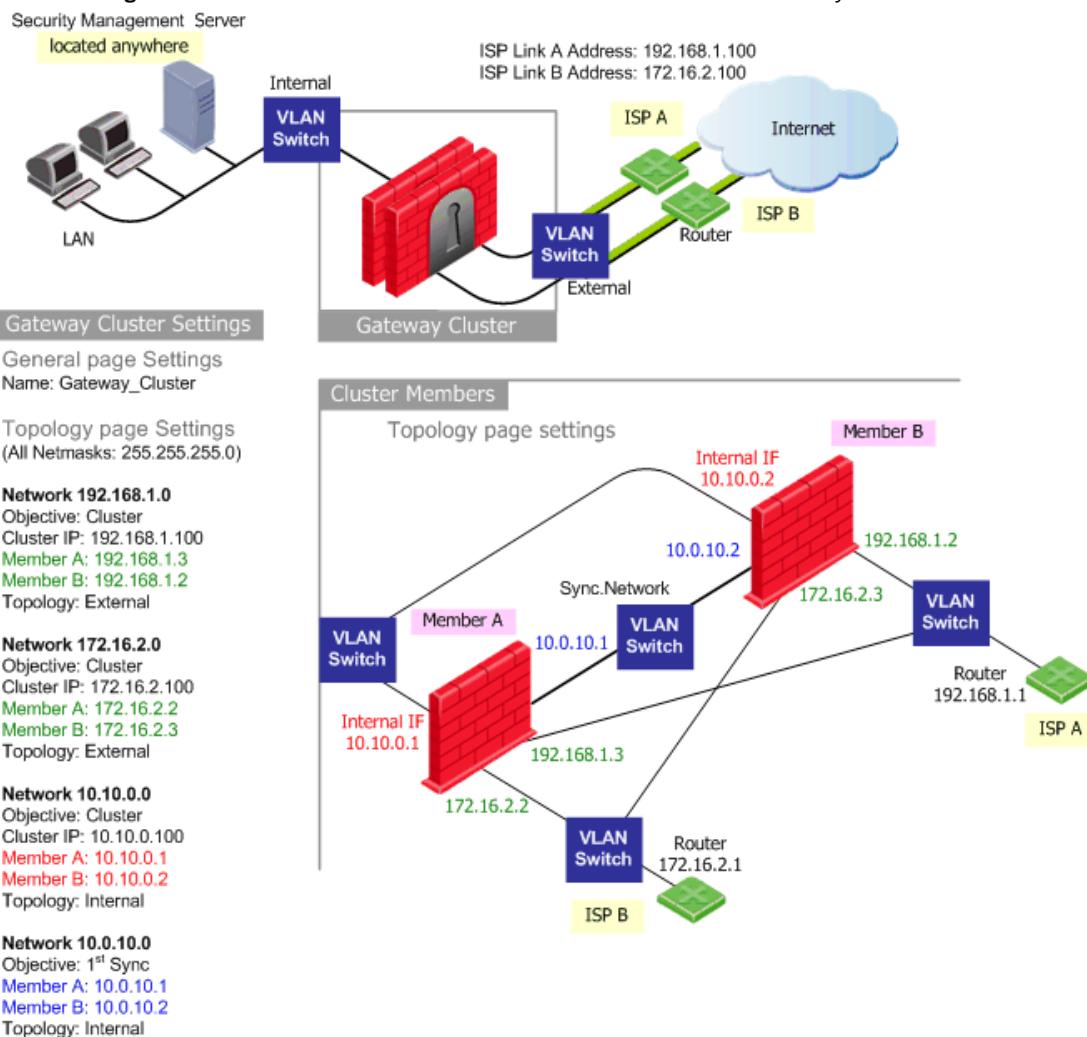


## Gateway Cluster Connection

If you have a ClusterXL gateway cluster, connect each cluster member to both ISPs through a LAN using two interfaces (Figure 4-6).

Configure ClusterXL in the usual way, however, ensure that the member interfaces are on the same subnet as the cluster external interfaces (see also the *ClusterXL Administration Guide*).

**Figure 4-6** Both ISP Links are LANs Connected to a Gateway Cluster



## ISP Redundancy and VPNs

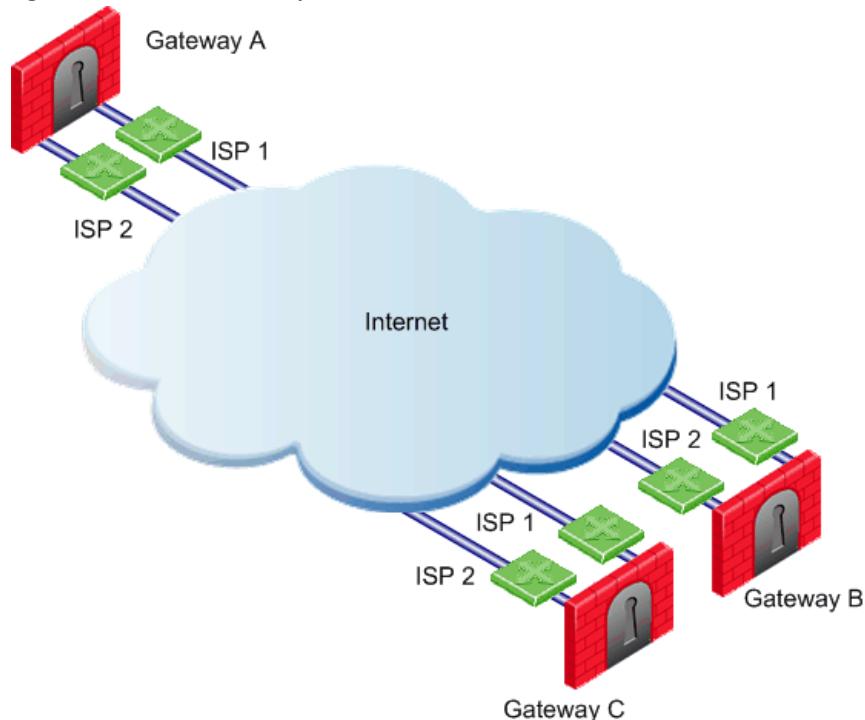
When ISP Redundancy is configured on the Security Gateway, VPN encrypted connections can survive a failure of one of the ISP links on the gateway. ISP Redundancy works with both gateway to gateway VPNs and SecuRemote/SecureClient to Remote Access VPNs.

The settings configured in the **ISP Redundancy** window, by default, are applied to the **Link Selection** page and overwrite any pre-existing configuration. If Primary/Backup mode is configured, it is transferred to the Link Selection configuration.

To configure ISP Redundancy on the Security Gateway:

1. Select **VPN > Topology > ISP Redundancy**. The **ISP Redundancy** window opens.
2. Configure the appropriate settings in the **ISP Redundancy** window. When ISP Redundancy is configured, the default setting in the **Link Selection** page is **Use ongoing probing**, however, Link Selection only probes the ISPs configured in the **ISP Redundancy** window. This feature enables connection failover of the VPN tunnel if connectivity to one of the gateway interfaces fails.

A different configuration for Link Selection is required when there are two gateways with two ISPs ([Figure 4-7](#)).

**Figure 4-7** Two Gateways with Two ISPs

In this case:

- Gateways A, B, and C have two ISPs.
- ISP Redundancy is configured on gateway A.
- Gateway A should use ISP 1 to connect to gateway B and ISP 2 to connect to gateway C. If one of the ISPs becomes unavailable, the other ISP should be used.

For additional configuration information, see the “Link Selection” chapter of the *Virtual Private Networks Administration Guide*.

## ***ISP Redundancy and Third-Party VPNs***

The ability of a third-party VPN device to detect an ISP link failure depends on the third-party device implementation. The failure of an ISP link could lead to a VPN failure for the following reasons:

1. The third-party device may not recognize incoming encrypted traffic from the secondary link as coming from the gateway.
2. The third-party device may be unable to detect an ISP link failure and therefore may continue encrypting traffic to the failed link.

# Considerations for ISP Link Redundancy

## Choosing the Deployment

The choice of deployment that best suits your organization's needs is normally evident. The following are some recommendations:

- The simplest configuration is to use a different interface for each ISP link, as shown in [Figure 4-3](#).
- If only one external interface is available on the Security Gateway, you can connect both ISPs to the same interface by defining two subnets, one for each ISP on the same interface, as shown in [Figure 4-4](#).
- If one of the ISP links is a dialup network (modem connection) that is used for backup, use the deployment shown in [Figure 4-5](#) and select the Primary/Backup mode of operation.
- If the ISP links are connected to a Check Point Security Gateway cluster, use the deployment shown in [Figure 4-6](#).

## Choosing the Redundancy Mode

If both ISPs are basically the same, use Load Sharing mode to ensure that you are making the best use of both ISPs.

You may prefer to use one of your two ISPs that is more cost-effective in terms of price and reliability. In that case, use Primary/Backup mode and set the more cost-effective ISP as the Primary ISP link.

# Configuring ISP Link Redundancy

## In This Section

Introduction to ISP Link Redundancy Configuration	page 155
Registering the Domain and Obtaining IP Addresses	page 155
DNS Server Configuration for Incoming Connections	page 156
Dialup Link Setup for Incoming Connections	page 157
SmartDashboard Configuration	page 157
Configuring Default Route for ISP Redundancy Gateway	page 160

## Introduction to ISP Link Redundancy Configuration

The following ISP Redundancy configuration allows outgoing connections from behind the Security Gateway to the Internet and incoming connections from the Internet to the networks behind the Security Gateway.



**Note** - For advanced configuration options, see SecureKnowledge solution sk23630 at <http://supportcontent.checkpoint.com/solutions?id=sk23630> (your username and password are required).

**Note** - In the following configuration examples, 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 Security 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 another internal network). It is not necessary to have an actual DNS server because the Security Gateway can be configured to intercept the DNS queries.

To register the domain and obtain IP addresses:

1. Obtain one routable IP address from each ISP for the DNS server or for the Security Gateway that intercepts DNS queries. If routable IP addresses are not available, make the DNS server accessible from the Internet using manual NAT ([step 2](#)).
2. Register your domain (for example, `example.com`) with both ISPs.
3. Inform both ISPs of the two addresses of the DNS server that respond to DNS queries for the `example.com` domain.

4. To allow incoming connections, obtain one routable IP address from each ISP for each application server that is accessed from the Internet.

For example, obtain two IP addresses for the Web server in DMZ-net. To avoid using routable IP addresses for the publicly available servers, see [step 2](#).

## DNS Server Configuration for Incoming Connections

The following section describes a DNS server configuration for incoming connections where the firewall is configured to intercept DNS queries to a Web server (for example, [www.example.com](#) in [Figure 4-2 on page 145](#)) that arrive at the Security Gateway external interfaces and to respond to them with ISP addresses 192.168.1.2 and 172.16.2.2.

To configure the DNS server for incoming connections:

1. In the **DNS Proxy** tab of the **ISP Redundancy** window, select **Enable DNS proxy**.
2. The Security Gateway responds to DNS queries with either one or two IP addresses, depending on the status of the ISP link and the redundancy mode. To configure this behavior, map each server name to an IP address pair by clicking **Add...** in the **DNS Proxy** tab.
3. Type a **Host name** (for example, [www.example.com](#)).
4. Add an IP address for ISP-1 (for example, 192.168.1.2 in [Figure 4-2 on page 145](#)) and an IP address for ISP-2 (for example, 172.16.2.2).

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, the Security Gateway replies with a TTL of 15 seconds. This can be changed in the **DNS TTL** field.

## Dialup Link Setup for Incoming Connections

To configure a dialup link for incoming connections:

1. If one of the ISP links is a dialup network, edit the ISP Redundancy Script located in \$FWDIR/bin/cpisp\_update.
2. In the script, use the Linux or SecurePlatform operating system command to bring up or to take down the dialup interface.
3. You can connect SecurePlatform to ISPs that provide xDSL services using PPPoE or PPTP xDSL modems. If using one of these connections, in the PPPoE or PPTP configuration of SecurePlatform, clear the **Use Peer Gateway** option.

## SmartDashboard Configuration

To configure SmartDashboard:

1. Define a Security Rule Base rule that accepts DNS traffic through the Security Gateway using the domain\_udp service.
2. In the **Check Point Gateway** window > **Topology** page, define the Security Gateway interfaces leading to the ISPs.
3. Select **Topology > ISP Redundancy** and then the **Support ISP Redundancy** option.
4. Perform either *Automatic ISP Link Configuration* (follow [step 1](#) to [step 4](#)) or *Manual ISP Link Configuration* (follow [step 1](#) to [step 5](#)). Automatic configuration only works if there are exactly two external interfaces defined in the **Topology** page (it does not work for gateway cluster objects).

### Automatic ISP Link Configuration

1. Click **Automatic ISP Links configuration** to configure the ISP links based on information taken from the routing table of the gateway and the **Topology** page of the gateway object.
2. To work in Primary/Backup mode, do the following:
  - a. In the **Redundancy Mode** section, select **Primary/Backup**.
  - b. Select the link and then **Edit** to define the link you want to be primary.
  - c. In the **General** tab of the **ISP Link Properties** window, select **Primary ISP**.
3. Examine the automatically configured ISP Links configuration for correctness.
4. Continue to [step 1](#).

## Manual ISP Link Configuration

1. In the **Redundancy Mode** section, select **Load Sharing** or **Primary/Backup**.
2. Click **Add** to define each of the ISP links.
3. In the **General** tab of the **ISP Link Properties** window, configure the following:
  - a. Name the ISP link and select the **Interface** leading to the ISP.
  - b. 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 [Figure 4-3 on page 147](#), the next hop router on the way to ISP A has the IP address 192.168.1.1 and the next hop router on the way to ISP B has the IP address 172.16.2.1.
  - c. In **Primary/Backup** mode, define whether the ISP link is Primary.
4. Define a list of hosts to be monitored to verify that the link is operational. To specify the hosts, select the **Advanced** tab of the **ISP Link Properties** window and then **Add** to add the hosts to the list of **Selected hosts**.
5. Define **Tracking** by selecting an option for both **ISP failure** and **ISP recovery**.

## Allowing Incoming and Outgoing Connections

1. To allow outgoing connections through both ISP links, define automatic Hide NAT on network objects that initiate the outgoing connections. Using the example shown in [Figure 4-2 on page 145](#), configure the following:
  - a. Edit the `internal_net` object.
  - b. In the **General** tab of the **Network Properties** window, select **Add Automatic Address Translation Rules**.
  - c. Select the **Hide Translation Method** and then the **Hide behind Gateway** option.
2. To allow incoming connections through 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 Security Gateway, you can allow specific services for specific servers. Using the example shown in [Figure 4-2 on page 145](#), define the NAT rules listed in [Table 4-1](#). In this example, incoming HTTP connections from both ISPs reach the Web server, [www.example.com](http://www.example.com) and DNS traffic from both ISPs reach the DNS server.

**Table 4-1** Manual Static Rules for a Web Server and a DNS Server

Original			Translated			Comment
Source	Destination	Service	Source	Destination	Serv.	
Any	192.168.1.2	http	=	10.0.0.2 (Static)	=	Incoming Web ISP A
Any	172.16.2.2	http	=	10.0.0.2 (Static)	=	Incoming Web ISP B
Any	192.168.1.2	domain _udp	=	10.0.0.3 (Static)	=	Incoming DNS ISP A
Any	172.16.2.2	domain _udp	=	10.0.0.3 (Static)	=	Incoming DNS ISP B

If you have a routable address from each ISP for each publicly reachable server (in addition to the addresses that belong to the Security Gateway), you can allow any service to reach the application servers by giving each server a nonroutable address. In the NAT Rule Base in [Table 4-1](#), do the following:

- Use the routable addresses in the **Original Destination**.
- Use the nonroutable address in the **Translated Destination**.
- Select Any as the **Original Service**.



**Note** - If using Manual NAT, automatic arp does not work for the NATed addresses. On Linux and SecurePlatform use local.arp. On IPSO set up Proxy ARP.

- Save and install the security policy: **Policy > Install**.

## Configuring Default Route for ISP Redundancy Gateway

Configure the ISP Redundancy gateway machine with only a single default route and do not give it a 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 **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 is up again, the original default route is reinstated.

# Chapter

# ConnectControl - Server Load Balancing

## In This Chapter

The Need for Server Load Balancing	page 162
ConnectControl Solution for Server Load Balancing	page 163
Configuring ConnectControl	page 172

## 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 time outs. In addition, server maintenance and other unplanned downtimes 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 the failure of any one machine.

# ConnectControl Solution for Server Load Balancing

## In This Section

<a href="#">Introduction to ConnectControl</a>	page 163
<a href="#">Load-Balancing Methods</a>	page 164
<a href="#">ConnectControl Packet Flow</a>	page 165
<a href="#">Logical Server Types</a>	page 166
<a href="#">Persistent Server Mode</a>	page 169
<a href="#">Server Availability</a>	page 171
<a href="#">Load Measuring</a>	page 171

## Introduction to ConnectControl

ConnectControl is Check Point's solution for server load balancing. ConnectControl distributes network traffic among a number of servers, which reduces the load on a single machine and thereby improves network response time and provides high availability. In addition to the performance benefits, spreading the load over multiple machines creates redundancy for your application and reduces the risk of downtime.

Load-balanced servers are represented by a single virtual IP address, so clients are unaware that more than one server is serving their requests. This is accomplished using a Logical server, which is a network object defined in SmartDashboard that represents a group 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 gateway and does not impose any additional memory or processing requirements. It continuously checks the availability of each server and if a server fails or is unreachable, ConnectControl stops directing connections to that server until it becomes available.

## Load-Balancing Methods

ConnectControl distributes network traffic to load-balanced servers according to predefined balancing methods, which include:

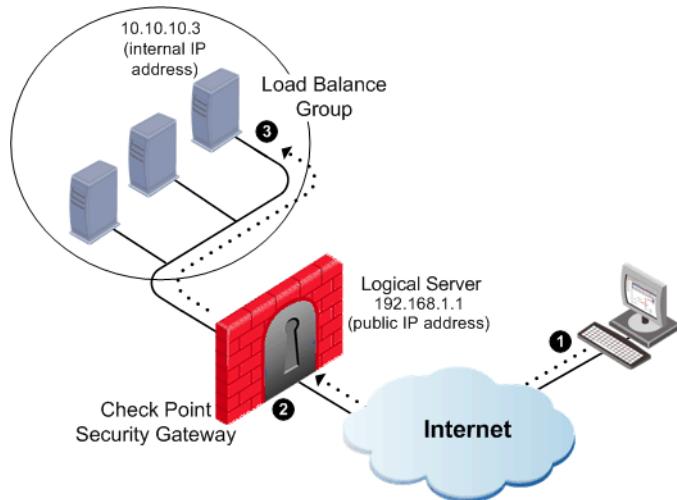
- **Server Load:** Measures the load on each server to determine which server has the most available resources to service a request. Each server in the group runs a load measuring agent that automatically reports the current system load to ConnectControl on the Security Gateway. Server Load is a good choice if your servers run other demanding applications in addition to supporting your load-balanced application. See also “[Load Measuring](#)” on page 171.
- **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 gateway executes a series of ICMP echo requests (pings) and reports which server has the shortest average round trip time. ConnectControl then directs the service request to that server. The round trip method is 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 and 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 and 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 that is load balanced by ConnectControl, the following is the packet flow ([Figure 5-1](#)):

1. A client initiates a connection with the logical IP address of the application server, which is actually 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. The firewall then directs the packet to the Logical server.
3. ConnectControl determines which of the servers in the group can best fulfill the request based on the load-balancing method.

**Figure 5-1** ConnectControl Packet Flow



## Logical Server Types

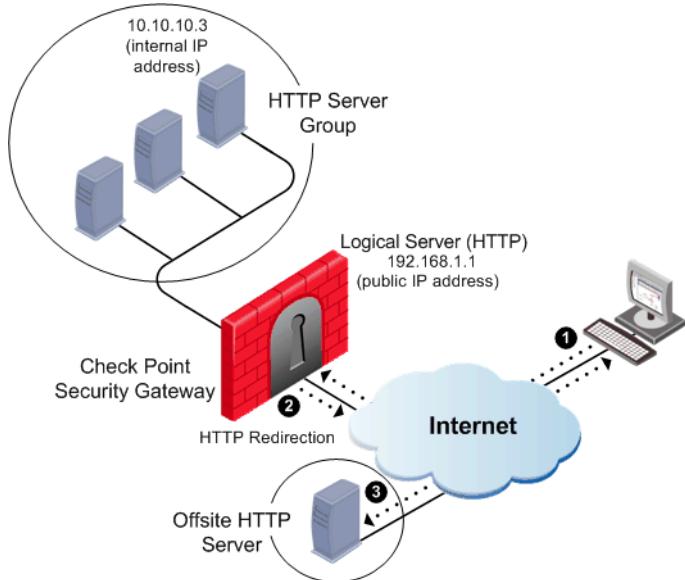
When creating the Logical server object, you must identify the server type as either HTTP or Other. This distinction is important, as ConnectControl handles the connection to the client differently for each server type. To direct network traffic, the **HTTP** server type uses HTTP redirection, while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

### **HTTP**

The **HTTP** Logical server type employs HTTP redirection to distribute network traffic and supports only HTTP services. The redirection mechanism ensures that all sessions comprising an HTTP connection are directed to a single server. This is critical 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 selected 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 to the IP address of the Logical server. The IP address can be the address of a server behind the firewall or of an offsite server. The remainder of the session is conducted without ConnectControl intervention and all operations are transparent to the user.

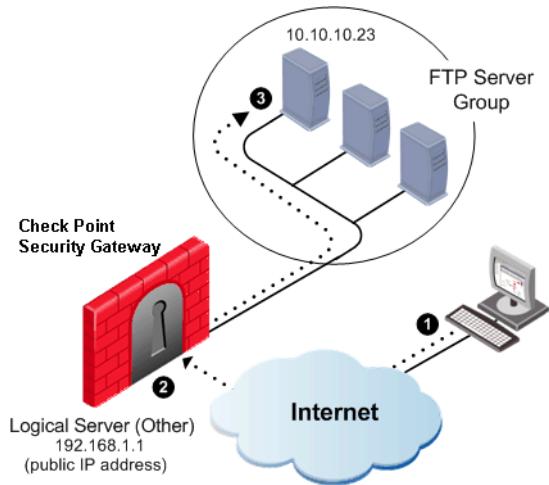
The Logical server may direct the client to an HTTP server behind the firewall or to an offsite HTTP server ([Figure 5-2](#)), depending on the result of ConnectControl's load balancing.

**Figure 5-2** Packet Flow in an HTTP Logical Server

All further communication between the client and the server takes place without the intervention of ConnectControl.

## **Other**

The **Other** Logical server type can be used for all services supported by Check Point Security Gateway including HTTP. It uses NAT to direct network traffic to the grouped servers. ConnectControl mediates each service request, even when clients continue a session. When you create an **Other** Logical server type, ConnectControl allows the connection by automatically placing entries in the Security Gateway kernel table. ConnectControl determines which server receives 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 5-3](#) shows a connection being directed to a NATed FTP server inside the firewall.

**Figure 5-3** Packet Flow in an Other Logical Server type

On the packet's return, the firewall translates the packet's original address to that of the Logical server.

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

## ***Considering Logical Server Types***

When considering the proper implementation for your environment, there are three decisive criteria: use of HTTP forms, server location and servers configured for NAT. The **HTTP** type supports offsite HTTP servers and form based applications, but only works with the HTTP protocol. The **Other** type supports all protocols and may provide the most effectively 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 also "["Persistent Server Timeout" on page 170](#)"). When using this feature, you must decide whether the persistency is by server or by service.

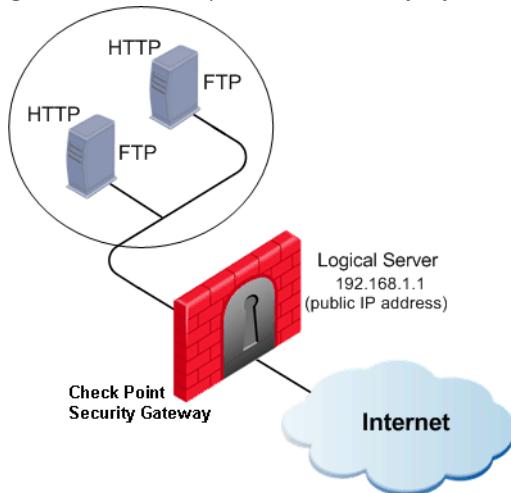
### ***Persistency By Server***

Persistency by server is useful for certain types of HTTP applications, such as forms support, for example, in a load-balanced environment of three Web servers ([Figure 5-4](#)). When **Persistency by server** is enabled, ConnectControl directs an HTTP client to a specific server and each subsequent request by the client is directed to the same server. This mode allows clients to fill out forms without the data loss that occurs if separate service requests are directed to different servers. If you support forms, enable **Persistent server mode** (the default setting) and the **Persistency by server** option.

## Persistency By Service

The persistency by service feature is useful if you are load balancing multiple services in your server group, for example, in a redundant environment of two machines, each running HTTP and FTP (Figure 5-4).

**Figure 5-4** Example of Persistency by Service



Using persistency by service, the client can be directed to one server for HTTP services and another for FTP services. This prevents you from being locked in to a server under a heavy load, as may occur if you opt for persistency by server in this configuration. **Persistency by service** directs previously load-balanced clients, which request a different service, to be load balanced and directed once again to the correct server.

## Persistent Server Timeout

The **Persistent server timeout** sets the amount of time that a client, once directed to a particular server, continues to be directed to that server. In the event that a server becomes unavailable, new connections are directed to an available server, even if Persistent server mode is enabled. For optimal load balancing between servers, disable **Persistent server mode** so that all application traffic is distributed according to the load-balance method. The **Persistent server timeout** is configured in the **ConnectControl** page of the **Global Properties** window.

## Server Availability

You can configure various properties of ConnectControl in order to check the availability of servers in the Logical server group. You can define how often the gateway pings the servers to ensure they are still active and the number of attempts it makes to contact a nonresponsive server after ConnectControl stops directing connections to it.

These settings are located in the **ConnectControl** page of the **Global Properties** window. The **Server availability check interval** option defines how often the servers are pinged. The **Server check retries** option defines the number of attempts to contact nonresponsive servers.

## Load Measuring

The server load-balancing method is unique because it requires a 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 ConnectControl.

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 want to write their own agents. You can download the load agent application for your OS from SecureKnowledge at: <http://support.checkpoint.com>. Sign in with your User Center email and password and enter the SecureKnowledge ID 47.0.1569467.2530820.

You can configure certain properties of the load-measuring agent in the **ConnectControl** page of the **Global Properties** window. The **Load agents port** property determines the port that the load agent uses to communicate with the Security Gateway. All the load-measuring agents in a configuration must use the same port number. The **Load measurement interval** property defines 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-measuring agent using the `load_agent_nt <port_number> <load_value>` syntax.

The default port used by ConnectControl for version NG or higher 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

To configure ConnectControl:

1. In SmartDashboard, right-click **Network Objects** in the **Network Objects** tree and select **New > Node > Host**.
2. Define a server object that represents a load-balanced server.
3. Repeat step 2 for each server you place in the group.
4. In Security Management, right-click **Network Objects** and select **New > Group > Simple Group**.
5. Name the group (for example, `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.
7. In SmartDashboard, right-click **Network Objects** in the **Network Objects** tree and select **New > Logical Server**. Ensure 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. Add the Group object you created in [step 3](#) to the **Servers Group**.
10. To enable Persistent server mode, select either **Persistency by service** or **server** (the default mode is **Persistency by service**).
11. Select a load-balance method as the **Balance Method**.
12. Add the following rule to the Rule Base:

**Table 5-1** Load Balancing Rule

Source	Destination	Service	Action
Any	Logical_Server	[load-balanced service(s)]	Accept or User Auth or Client Auth or Session Auth

13. For applications using HTTP redirection (HTTP Logical server type), add a second rule to allow the physical server group to communicate directly with clients after sessions have started.

**Table 5-2** Server Group Connection Rule

Source	Destination	Service	Action
Any	HTTP_Server_Group	http	Accept

14. From the **Policy** menu, select **Global Properties > ConnectControl**. Review the default settings and adjust according to your implementation. The following options are available:

- **Servers Availability:** Manages how often ConnectControl ensures that 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. The **Server availability check interval** option default value is 20 seconds. The **Server check retries** option default value is 3 times.
- **Servers Persistency:** Defines the amount of time that a client, once directed to a particular server, directs traffic to it. The **Persistent server timeout** option default value is 1800 seconds.
- **Servers Load Balancing:** Manages how often the load measuring agents (if employed) report their load status to ConnectControl and the port from which they communicate with ConnectControl. The **Load agents port** option default value is 18212. The **Load measurement interval** default value is 20 seconds.



# Chapter

# Bridge Mode

## In This Chapter

[Introduction to Bridge Mode](#)

[page 176](#)

[Configuring Bridge Mode](#)

[page 178](#)

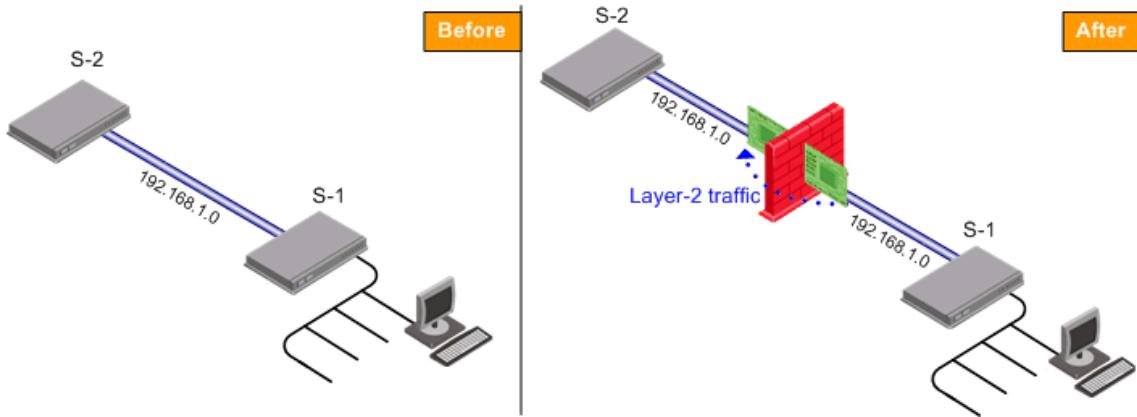
# Introduction to Bridge Mode

Installing a new gateway in an existing network often requires reconfiguration of the routing scheme. However, in more complex deployments, you may find that the reconfiguration necessary to enable a new routing scheme is prohibitive. Check Point Security Gateway bridge mode allows for the placement of a firewall without changing the existing IP routing.

A Check Point Security Gateway in bridge mode operates as a regular firewall, inspecting traffic and dropping or blocking unauthorized or unsafe traffic. A gateway in bridge mode is invisible to all Layer-3 traffic. When authorized traffic arrives at the gateway, it is passed from one interface to another through a procedure known as bridging. Bridging creates a Layer-2 relationship between two or more interfaces, whereby any traffic that enters one interface always exits the other. This way, the firewall can inspect and forward traffic without interfering with the original IP routing.

Bridge mode allows a transparent deployment of a Security Gateway. [Figure 6-5](#) illustrates how a firewall in bridge mode does not alter the IP routing of an existing network.

**Figure 6-5** Deploying a Single Security Gateway in bridge mode



In [Figure 6-5](#) the subnet's network address is **192.168.1.0** and objects labeled **S-\*** are switches.

For IP routing, the firewall is transparently inserted into the existing network, leaving the **192.168.1.0** subnet on both sides of the firewall. Internal traffic is inspected and authorized by the firewall, without changes to the IP routing scheme. Traffic that is accepted by the firewall is forwarded from one interface to the other.

See also “[Bridging Interfaces](#)” on page 178.

# Limitations in Bridge Mode

- Each bridge supports a pair of interfaces only.
- Cluster configurations are not supported.
- Bridge mode is supported on the Check Point operating system SecurePlatform.



**Warning** - To manage a gateway in bridge mode, an interface with an IP address is required. It is important to configure a separate, routed interface for this purpose.

# Configuring Bridge Mode

## Bridging Interfaces

You can bridge interfaces using either the SecurePlatform WebUI, or from the command line.

### Using the SecurePlatform WebUI:

1. Connect to the management interface of the Security Gateway using WebUI.
2. Select **Network > Connections > New > Bridge**.
3. Select the interfaces to comprise the bridge and click **Add**.
4. Enter the **IP Address** and **Netmask** of the bridge (not the physical) interface, or assign IP address 0.0.0.0 for a bridge without an IP address. Note that while a bridge can function without an IP address, some security servers require an IP address on the relevant subnet.
5. Select **Apply**.

### From the Command Line:

1. Enter the command `sysconfig`.
2. Select Network Connections > Add new connection > Bridge.
3. Add a pair of interfaces which are not configured with an IP address to the bridge.
4. Enter `N` for next.
5. Enter the IP address and netmask of the bridge (not the physical) interface, or assign IP address 0.0.0.0 for a bridge without an IP address. Note that while a bridge can function without an IP address, some security servers require an IP address on the relevant subnet.

## Configuring Anti-Spoofing

When bridging interfaces, it is not possible to define the network behind a bridged interface by IP address and subnet, since this is true for the other interface of the bridge. If anti-spoofing is required for the bridged interfaces, see “[Configuring Anti-Spoofing for Internal Interfaces](#)” on page 37 for instructions on defining IP addresses ranges behind each of the bridged interfaces. Do not use the same network for both interfaces, as this may cause a loss of connectivity.

# Displaying the Bridge Configuration

## ***brctl show***

The `brctl show` command displays the status of the bridge configuration. The following is an example of a `brctl show` command report:

bridge name	bridge id	STP enabled	interfaces
br0	8000.000423b93e56	no	eth0 eth1

The `brctl show` command report displays the following results:

- bridge name: The name given to the bridge.
- bridge id: The unique identifier of the bridge.
- Interfaces: The names of the two interfaces in the bridge.

The MAC address of the bridge is inherited from one of the physical interfaces.



# **CoreXL**

This section gives a conceptual overview of CoreXL, a component of the Check Point firewall that enables customers to take advantage of multi-core processors.



# Chapter

# CoreXL Administration

## In This Chapter

Introduction to CoreXL	page 184
Performance Tuning	page 186
Command Line Reference	page 193

# Introduction to CoreXL

CoreXL is a performance-enhancing technology for Check Point Security Gateways on multi-core processing platforms. CoreXL enhances Security Gateway performance by enabling the processing cores to concurrently perform multiple tasks.

CoreXL provides almost linear scalability of performance, according to the number of processing cores on a single machine. The increase in performance is achieved without requiring any changes to management or to network topology.

CoreXL joins ClusterXL Load Sharing and SecureXL as part of Check Point's fully complementary family of traffic acceleration technologies.

In a CoreXL gateway, the firewall kernel is replicated multiple times. Each replicated copy, or instance, of the firewall kernel runs on one processing core. The instances handle traffic concurrently, and each instance is a complete and independent inspection kernel.

Regarding network topology, management configuration, and security policies, a CoreXL gateway functions as a regular Security Gateway. All of the kernel instances of a gateway handle traffic going through the same gateway interfaces and apply the same gateway security policy.

## Supported Platforms and Features

CoreXL is supported on SecurePlatform, Nokia, and Crossbeam platforms.

CoreXL does not support Check Point Suite with the following features:

- Check Point QoS (Quality of Service)
- Traffic view in SmartView Monitor (all other views are available)
- Firewall-1 GX (Firewall of Check Point Suite versions prior to NGX R60)
- Route-based VPN
- IP Pool NAT
- IPv6
- Overlapping NAT
- SMTP resource

To enable a non-supported feature in the Check Point Suite, disable CoreXL using cpconfig and reboot the gateway (see “[Configuring CoreXL](#)” on page 192).

## Default Configuration

Upon installation of CoreXL, the number of kernel instances is derived from the total number of cores in the system as described in the following table:

**Table 7-1** Default configuration for SecurePlatform

Number of Cores	Number of Kernel Instances
1	CoreXL is disabled
2	2
4	3
8	6
more than 8	number of cores, minus 4

The default affinity setting for all interfaces is Automatic when Performance Pack is installed (see “[Processing Core Allocation](#)” on page 186). Traffic from all interfaces is directed to the core running the Secure Network Distributor (SND).

# Performance Tuning

The following sections are relevant only for SecurePlatform.

## Processing Core Allocation

The CoreXL software architecture includes the Secure Network Distributor (SND). The SND is responsible for:

- Processing incoming traffic from the network interfaces
- Securely accelerating authorized packets (if Performance Pack is running)
- Distributing non-accelerated packets among kernel instances.

Traffic entering network interface cards (NICs) is directed to a processing core running the SND. The association of a particular interface with a processing core is called the interface's *affinity* with that core. This affinity causes the interface's traffic to be directed to that core and the SND to run on that core. Setting a kernel instance or a process to run on a particular core is called the instance's or process's *affinity* with that core.

The default affinity setting for all interfaces is Automatic. Automatic affinity means that if Performance Pack is running, the affinity for each interface is automatically reset every 60 seconds, and balanced between available cores. If Performance Pack is not running, the default affinities of all interfaces are with one available core. In both cases, any processing core running a kernel instance, or defined as the affinity for another process, is considered unavailable and will not be set as the affinity for any interface.

In some cases, which are discussed in the following sections, it may be advisable to change the distribution of kernel instances, the SND, and other processes, among the processing cores. This is done by changing the affinities of different NICs (interfaces) and/or processes. However, to ensure CoreXL's efficiency, all interface traffic must be directed to cores not running kernel instances. Therefore, if you change affinities of interfaces or other processes, you will need to accordingly set the number of kernel instances and ensure that the instances run on other processing cores.

Under normal circumstances, it is not recommended for the SND and an instance to share a core. However, it is necessary for the SND and an instance to share a core when using a machine with exactly two cores.

# Allocating Processing Cores

In certain cases, it may be advisable to change the distribution of kernel instances, the SND, and other processes, among the processing cores. This section discusses these cases.

Before planning core allocation, make sure you have read the “[Processing Core Allocation](#)” on page 186.

## In This Section

<a href="#">Adding Processing Cores to the Hardware</a>	page 187
<a href="#">Allocating an Additional Core to the SND</a>	page 188
<a href="#">Allocating a Core for Heavy Logging</a>	page 191

## ***Adding Processing Cores to the Hardware***

Increasing the number of processing cores on the hardware platform does not automatically increase the number of kernel instances. If the number of kernel instances is not increased, CoreXL does not utilize some of the processing cores. After upgrading the hardware, increase the number of kernel instances using cpconfig.

Reinstalling the gateway will change the number of kernel instances if you have upgraded the hardware to an increased number of processing cores, or if the number of processing cores stays the same but the number of kernel instances was previously manually changed from the default. Use cpconfig to reconfigure the number of kernel instances.

In a clustered deployment, changing the number of kernel instances (such as by reinstalling CoreXL) should be treated as a version upgrade. Follow the instructions in the *Upgrade Guide*, in the “Upgrading ClusterXL Deployments” chapter, and perform either a Minimal Effort Upgrade (using network downtime) or a Zero Downtime Upgrade (no downtime, but active connections may be lost), substituting the instance number change for the version upgrade in the procedure. A Full Connectivity Upgrade cannot be performed when changing the number of kernel instances in a clustered environment.

## ***Allocating an Additional Core to the SND***

In some cases, the default configuration of instances and the SND will not be optimal. If the SND is slowing the traffic, and your platform contains enough cores that you can afford to reduce the number of kernel instances, you may want to allocate an additional core to the SND. This is likely to occur especially if much of the traffic is of the type accelerated by Performance Pack; in a ClusterXL Load Sharing deployment; or if IPS features are disabled. In any of these cases, the task load of the SND may be disproportionate to that of the kernel instances.

To check if the SND is slowing down the traffic:

1. Identify the processing core to which the interfaces are directing traffic using `fw ctl affinity -l -r`.
2. Under heavy traffic conditions, run the `top` command on the CoreXL gateway and check the values for the different cores under the ‘idle’ column.

It is recommended to allocate an additional core to the SND only if all of the following conditions are met:

- Your platform has at least eight processing cores.
- The ‘idle’ value for the core currently running the SND is in the 0%-5% range.
- The sum of the ‘idle’ values for the cores running kernel instances is significantly higher than 100%.

If any of the above conditions are not met, the default configuration of one processing core allocated to the SND is sufficient, and no further configuration is necessary.

Allocating an additional processing core to the SND requires performing the following two stages in the order that they appear:

1. Reduce the number of kernel instances using `cpconfig`.
2. Set interface affinities to the remaining cores, as detailed below.
3. Reboot to implement the new configuration.

## Setting Interface Affinities

Check which cores are running the kernel instances (see “[Allocating Processing Cores](#)” on page 187). Allocate the remaining cores to the SND by setting interface affinities to the cores. The correct method of defining interface affinities depends on whether or not Performance Pack is running, as described in the following sections.

- When Performance Pack is Running

If Performance Pack is running, interface affinities are handled by using Performance Pack’s `sim affinity` command.

The default `sim affinity` setting is Automatic. In Performance Pack’s Automatic mode, interface affinities are automatically distributed among cores that are not running kernel instances and that are not set as the affinity for any other process.

In most cases, you do not need to change the `sim affinity` setting. For further information on `sim affinity` settings, see the *Performance Pack Administration Guide*.

- Setting Interface Affinities when Performance Pack is not Running

If Performance Pack is not running, interface affinities are loaded at boot from a configuration text file called `fwaffinity.conf`, located under: `$FWDIR/conf`. In the text file, lines beginning with the letter `i` define interface affinities.

If Performance Pack is running, interface affinities are defined by `sim affinity` settings, and lines beginning with `i` in `fwaffinity.conf` are ignored.

If you are allocating only one processing core to the SND, it is best to have that core selected automatically by leaving the default interface affinity set to automatic, and having no explicit core affinities for any interfaces. To do this, make sure `fwaffinity.conf` contains the following line:

```
i default auto
```

In addition, make sure that `fwaffinity.conf` contains no other lines beginning with `i`, so that no explicit interface affinities are defined. All interface traffic will be directed to the remaining core.

If you are allocating two processing cores to the SND, you need to explicitly set interface affinities to the two remaining cores. If you have multiple interfaces, you need to decide which interfaces to set for each of the two cores. Try to achieve a balance of expected traffic between the cores (you can later check the balance by using the `top` command).

To explicitly set interface affinities, when Performance Pack is not running:

1. Set the affinity for each interface by editing `fwaffinity.conf`. The file should contain one line beginning with `i` for each interface. Each of these lines should follow the following syntax:

```
i <interfacename> <cpuid>
```

where `<interfacename>` is the interface name, and `<cpuid>` is the number of the processing core to be set as the affinity of that interface.

For example, if you want the traffic from `eth0` and `eth1` to go to core #0, and the traffic from `eth2` to go to core #1, create the following lines in `fwaffinity.conf`:

```
i eth0 0
```

```
i eth1 0
```

```
i eth2 1
```

Alternatively, you can choose to explicitly define interface affinities for only one processing core, and define the other core as the default affinity for the remaining interfaces, by using the word `default` for `<interfacename>`.

In the case described in the previous example, the lines in `fwaffinity.conf` would be:

```
i eth2 1
```

```
i default 0
```

2. Run `$FWDIR/scripts/fwaffinity_apply` for the `fwaffinity.conf` settings to take effect.

The affinity of virtual interfaces can be set using their physical interface(s).

## ***Allocating a Core for Heavy Logging***

If the gateway is performing heavy logging, it may be advisable to allocate a processing core to the `fwd` daemon, which performs the logging. Like adding a core for the `SND`, this too will reduce the number of cores available for kernel instances.

To allocate a processing core to the `fwd` daemon, you need to do two things:

1. Reduce the number of kernel instances using `cpconfig`.
2. Set the `fwd` daemon affinity, as detailed below.

### **Setting the `fwd` Daemon Affinity**

Check which processing cores are running the kernel instances and which cores are handling interface traffic using `fw ctl affinity -l -r`. Allocate the remaining core to the `fwd` daemon by setting the `fwd` daemon affinity to that core.



**Note** - Avoiding the processing core or cores that are running the `SND` is important only if these cores are explicitly defined as affinities of interfaces. If interface affinities are set to Automatic, any core that is not running a kernel instance can be used for the `fwd` daemon, and interface traffic will be automatically diverted to other cores.

Affinities for Check Point daemons (such as the `fwd` daemon), if set, are loaded at boot from the `fwaffinity.conf` configuration text file located at: `$FWDIR/conf`. Edit the file by adding the following line:

```
n fwd <cpuid>
```

where `<cpuid>` is the number of the processing core to be set as the affinity of the `fwd` daemon. For example, to set core #2 as the affinity of the `fwd` daemon, add to the file:

```
n fwd 2
```

Reboot for the `fwaffinity.conf` settings to take effect.

## Configuring CoreXL

To enable/disable CoreXL:

1. Run the `cpconfig` command.
2. Select **Configure Check Point CoreXL**.
3. Choose whether to enable or disable CoreXL.
4. Reboot the gateway.

To configure the number of instances:

1. Run the `cpconfig` command.
2. Select **Configure Check Point CoreXL**.
3. If CoreXL is enabled, choose to change the number of firewall instanced.  
If CoreXL is disabled, choose to enable CoreXL and then set the required number of firewall instances.
4. Reboot the gateway.



**Note** - In a clustered deployment, changing the number of kernel instances should be treated as a version upgrade. See “[Command Line Reference](#)” on page 193.

# Command Line Reference

## In This Section

<a href="#">fw ctl affinity</a>	page 195
<a href="#">fw ctl multik stat</a>	page 198

## Affinity Settings

Affinity settings are changed by the `fwaffinity_apply` script file, which runs automatically at boot. Therefore, when you make a change to affinity settings, the settings will not take effect until you either reboot or manually run `fwaffinity_apply`.

`fwaffinity_apply` executes affinity definitions according to the information in the `fwaffinity.conf` text file. To change affinity settings, edit the text file.



**Note** - If Performance Pack is running, interface affinities are only defined by Performance Pack's `sim affinity` command, and `fwaffinity.conf` interface affinity settings are ignored.

# fwaffinity.conf

fwaffinity.conf is located at: \$FWDIR/conf.

## Syntax

Each line in the text file uses the same format: <type> <id> <cpu>

Data	Values	Description
<type>	i	interface
	n	Check Point daemon
	k	kernel instance
<id>	interface name	if <type> = i
	daemon name	if <type> = n
	instance number	if <type> = k
	default	interfaces that are not specified in another line
<cpuid>	<number>	number(s) of processing core(s) to be set as the affinity
	all	all processing cores are available to the interface traffic, daemon or kernel instance
	ignore	no specified affinity (useful for excluding an interface from a default setting)
	auto	Automatic mode (see “ <a href="#">Processing Core Allocation</a> ” on page 186)



**Note** - Interfaces that share an IRQ cannot have different cores as their affinities, including when one interface is included in the default affinity setting. Either set both interfaces to the same affinity, or use ignore for one of them. To view the IRQs of all interfaces, run: fw ctl affinity -l -v -a .

## **fwaffinity\_apply**

fwaffinity\_apply is located at: \$FWDIR/scripts . To run fwaffinity\_apply, use the following syntax:

```
$FWDIR/scripts/fwaffinity_apply <option>
```

where <option> is one of the following parameters:

Parameter	Description
-q	Quiet mode - print only error messages.
-t <type>	Only apply affinity for the specified type.
-f	Sets interface affinity even if automatic affinity is active.

## **fw ctl affinity**

The fw ctl affinity command controls affinity settings. However, fw ctl affinity settings will not persist through a restart of the Check Point Security Gateway.

To set affinities: fw ctl affinity -s

To list existing affinities: fw ctl affinity -l

### ***fw ctl affinity -s***

Use this command to set affinities.

fw ctl affinity -s settings are not persistent through a restart of Check Point Security Gateway. If you want the settings to be persistent, either use sim affinity (a Performance Pack command - see the *Performance Pack Administration Guide* for details) or edit the fwaffinity.conf configuration file.

To set interface affinities, you should use fw ctl affinity only if Performance Pack is not running. If Performance Pack is running, you should set affinities by using the Performance Pack sim affinity command. These settings will be persistent. If Performance Pack's sim affinity is set to Automatic mode (even if Performance Pack was subsequently disabled), you will not be able to set interface affinities by using fw ctl affinity -s.

## Syntax

```
fw ctl affinity -s <proc_selection> <cpuid>
```

<proc\_selection> is one of the following parameters:

Parameter	Description
-p <pid>	Sets affinity for a particular process, where <pid> is the process ID#.
-n <cpdname>	Sets affinity for a Check Point daemon, where <cpdname> is the Check Point daemon name (for example: fwd).
-k <instance>	Sets affinity for a kernel instance, where <instance> is the instance's number.
-i <interfacename>	Sets affinity for an interface, where <interfacename> is the interface name (for example: eth0).

<cpuid> should be a processing core number or a list of processing core numbers. To have no affinity to any specific processing core, <cpuid> should be: all.



**Note** - Setting an Interface Affinity will set the affinities of all interfaces sharing the same IRQ to the same processing core.

To view the IRQs of all interfaces, run: fw ctl affinity -l -v -a .

## Example

To set kernel instance #3 to run on processing core #5, run:

```
fw ctl affinity -s -k 3 5
```

## ***fw ctl affinity -l***

Use this command to list existing affinities. For an explanation of kernel, daemon and interface affinities, see the “[CoreXL Administration](#)” on page 183.

### **Syntax**

```
fw ctl affinity -l [<proc_selection>] [<listtype>]
```

If <proc\_selection> is omitted, fw ctl affinity -l lists affinities of all Check Point daemons, kernel instances and interfaces. Otherwise, <proc\_selection> is one of the following parameters:

Parameter	Description
-p <pid>	Displays the affinity of a particular process, where <pid> is the process ID#.
-n <cpdname>	Displays the affinity of a Check Point daemon, where <cpdname> is the Check Point daemon name (for example: fwd).
-k <instance>	Displays the affinity of a kernel instance, where <instance> is the instance's number.
-i <interfacename>	Displays the affinity of an interface, where <interfacename> is the interface name (for example: eth0).

If <listtype> is omitted, fw ctl affinity -l lists items with specific affinities, and their affinities. Otherwise, <listtype> is one or more of the following parameters:

Parameter	Description
-a	All: includes items without specific affinities.
-r	Reverse: lists each processing core and the items that have it as their affinity.
-v	Verbose: list includes additional information.

### **Example**

To list complete affinity information for all Check Point daemons, kernel instances and interfaces, including items without specific affinities, and with additional information, run:

```
fw ctl affinity -l -a -v
```

## **fw ctl multik stat**

The fw ctl multik stat (multi-kernel statistics) command displays information for each kernel instance. The state and processing core number of each instance is displayed, along with:

- The number of connections currently being handled.
- The peak number of concurrent connections the instance has handled since its inception.

# **Application Intelligence**

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



# Chapter

# Anti-Virus and URL Filtering

## In This Chapter

[Anti-Virus Protection](#)

page 202

[URL Filtering](#)

page 217

# Anti-Virus Protection

## In This Section

Introduction to Integrated Anti-Virus Protection	page 202
Architecture	page 203
Configuring Integrated Anti-Virus Scanning	page 203
Database Updates	page 204
Understanding Scan By Direction and Scan By IP	page 205
Scanning by Direction: Selecting Data to Scan	page 209
File Type Recognition	page 211
Continuous Download	page 212
Logging and Monitoring	page 213
File Size Limitations and Scanning	page 214
UTM-1 Edge Anti-Virus	page 216

## Introduction to Integrated Anti-Virus Protection

Viruses are a major threat to network operations and have become increasingly dangerous and sophisticated. For example, worms, blended threats (which use combinations of malicious code and vulnerabilities for infection and dissemination) and trojans.

Content Inspection (CI) gateways contain integrated Anti-Virus technology. Integrated Anti-Virus solutions require no extra IT resources and organizations benefit from their easy management in the familiar Check Point SMART infrastructure, which 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, SMTP and POP3 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.

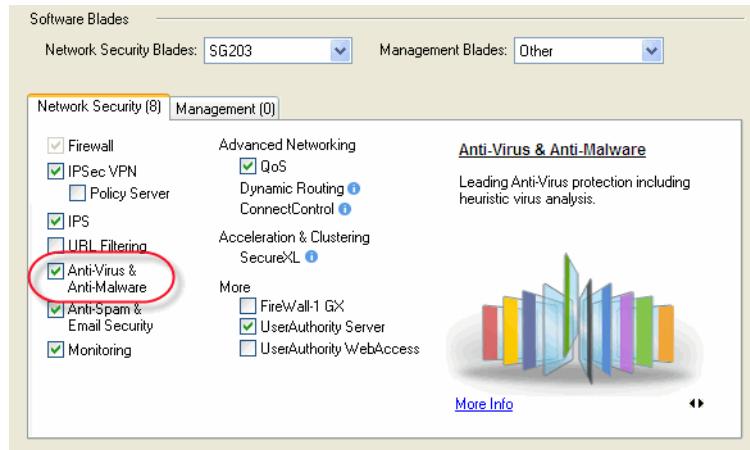
For Check Point CI, an Anti-Virus configuration makes CVP resource configuration obsolete. In cases where both Anti-Virus and CVP are used ,only Anti-Virus works.

## Configuring Integrated Anti-Virus Scanning

To configure integrated Anti-Virus scanning:

1. For all CI gateway objects, select **Anti-Virus & Anti-Malware** in the **Software Blades > Network Security** list of the **General Properties** page.

**Figure 8-1** Check Point Software Blades - Network Security



2. From the **Topology** page, define the gateway topology, specifying the internal networks and the DMZ.
3. Define rules in the Security Rule Base to permit specific services. Anti-Virus scanning is applied only to accepted traffic.
4. In the **Anti-Virus & URL Filtering** tab, select the services to be scanned using the following options:

- From the **Anti-Virus** page, configure options for file handling and scan failures.
- From the **Signature Updates** page, configure when to perform automatic signature updates or to initiate a manual signature update.
- From the **SMTP, FTP, HTTP** and **POP3** pages, configure Anti-Virus scanning options for these services.
- From the **File Types** page, configure whether to Scan, Block or Pass traffic according to the file type and configure continuous Download settings.

## Database Updates

The following kinds of database updates are available:

- **Automatic:** Updates of the virus signature can be scheduled at a predefined interval.
- **Manual:** Updates of virus signatures can be initiated at any time.

When using the CI gateway and/or the Security Management server, download updates from a Check Point server prior to downloading signature updates. First verify that:

- HTTP and HTTPS Internet connectivity with DNS is properly configured.
- You have a valid Check Point User Center username and password.

The following signature update methods are available (the default update interval is 120 minutes for all methods):

- **Download signature updates every x minutes:** Enables you to define the update interval.
- **Download from Check Point site:** Indicates that each Security Gateway is responsible for contacting Check Point's site to obtain Anti-Virus signatures. Updates are downloaded directly to the CI gateways. This method usually results in faster update times.
- **Download from My local Security Management server:** Indicates that updates are only downloaded by the Security Management server from the default Check Point signature distribution server and then redistributed all CI gateways. This method is useful when Internet access is not available for all gateways or if the download can only occur once for all the gateways.

# Understanding Scan By Direction and Scan By IP

## In This Section

<a href="#">Definitions</a>	page 205
<a href="#">Comparing Scan by Direction and by IP</a>	page 206

### ***Definitions***

Scan by Direction and Scan by IP are two file scanning methods used by Content Inspection. Anti-Virus scanning is performed only on traffic that is allowed by the Security Rule Base.

### **Scan By Direction**

Scan by Direction scans all files passing in one direction, either to or from the external, internal and/or DMZ networks. Using this method (the default) is fairly intuitive and does not require the specification of hosts or networks. This method also enables you to define exceptions, for example, locations to or from which files are not scanned.



**Note** - Scan By Direction works only when CI is connected as a gateway and is placed in line between the external and the internal/DMZ networks. It does not work when CI is connected as a node in Proxy mode. The gateway topology must also be correctly defined.

### **Scan By IP Address**

Scan by IP address enables you to define which traffic is scanned. For example, if all incoming traffic from external networks reaches the DMZ using Scan by IP, you can configure CE to scan only traffic to the FTP, SMTP, HTTP and POP3 servers. Conversely, Scan by Direction scans all traffic to the DMZ.

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

## Comparing Scan by Direction and Scan by IP

**Scan by Direction** enables you to specify file scanning according to the file's (and not necessarily the connection's) origin and destination.

**Scan by IP** enables you to specify file scanning according to the connection they are sent through and the protocol phase/command (where applicable).

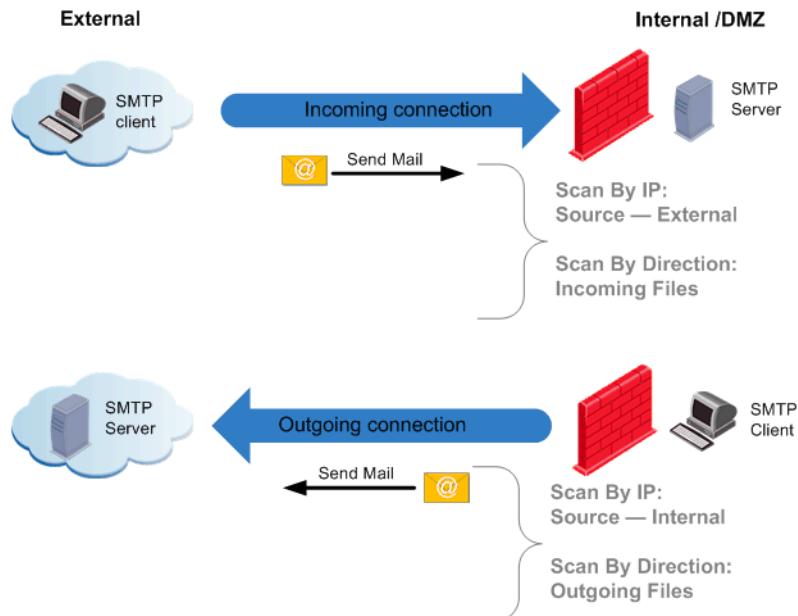
If you want most or all files in a given direction to be Anti-Virus scanned, select **Scan by Direction**.

If you want to specify a connection or part of a connection's source or destination to be scanned, select **Scan by IP**.

### Comparing Scan by Direction and Scan by IP for SMTP Protocol

For the SMTP protocol, Scan by Direction and Scan by IP are comparable options. Figure 8-2 illustrates that for the SMTP protocol, the files (data) are always sent in the same direction as the connection. The SMTP protocol is used to send mail. Protocols that are used to receive mail (for example, POP3 and IMAP) are not scanned when SMTP is selected.

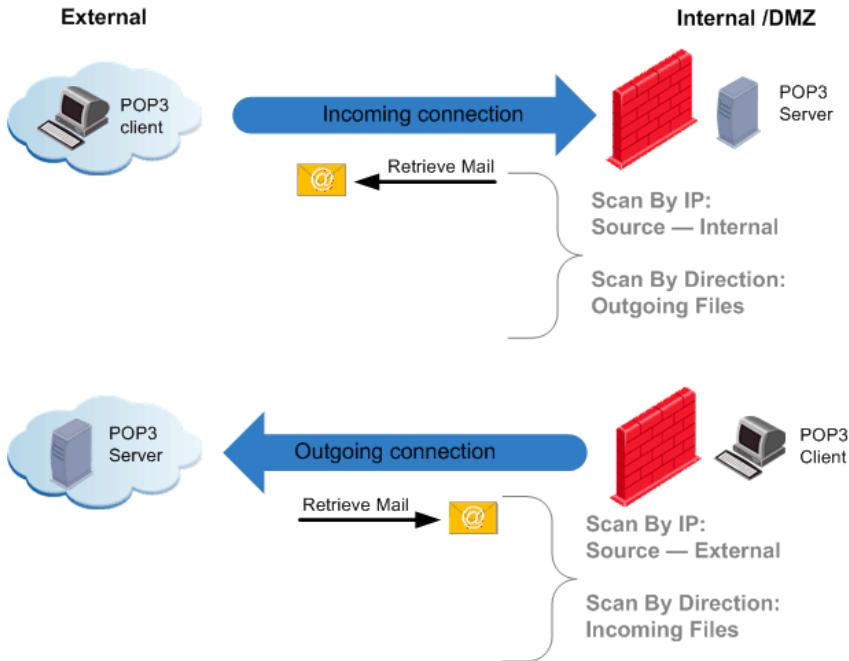
**Figure 8-2** Comparing Scan by Direction to Scan by IP Address for SMTP



## Comparing Scan by Direction and by IP for POP3 Protocol

Figure 8-3 illustrates that for the POP3 protocol, the files (data) are always sent in the opposite direction of the connection. POP3 is used to retrieve mail.

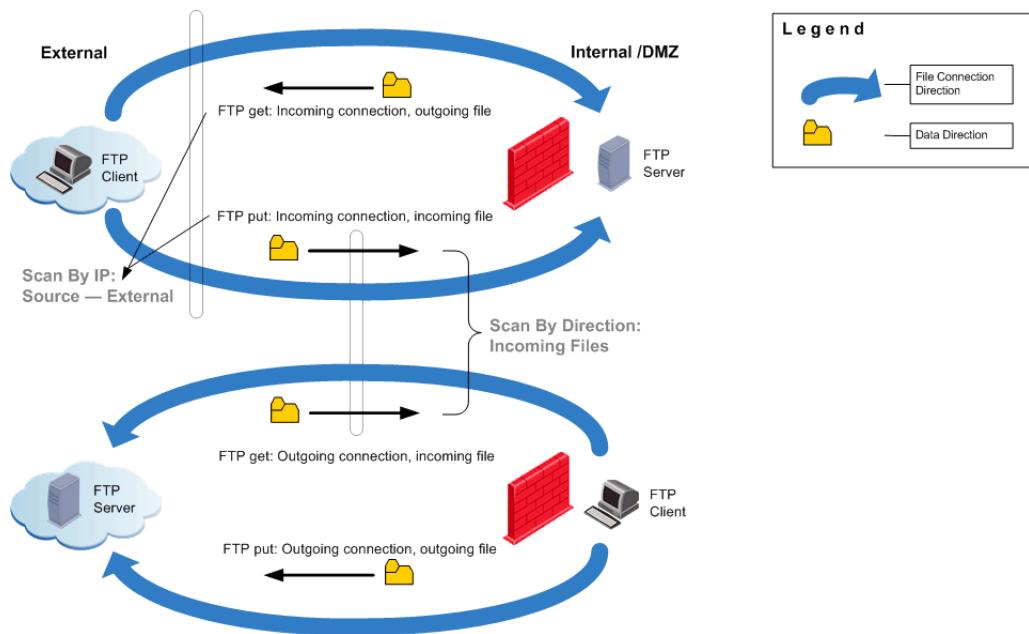
**Figure 8-3** Comparing Scan by Direction to Scan by IP Address for POP3



## Comparing Scan by Direction and Scan by IP for FTP Protocol

For the FTP protocol, the difference between Scan by IP and Scan by Direction is illustrated in [Figure 8-4](#). 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. In this scenario, the Scan by Direction option enables you to scan files without having to consider the direction of the connection.

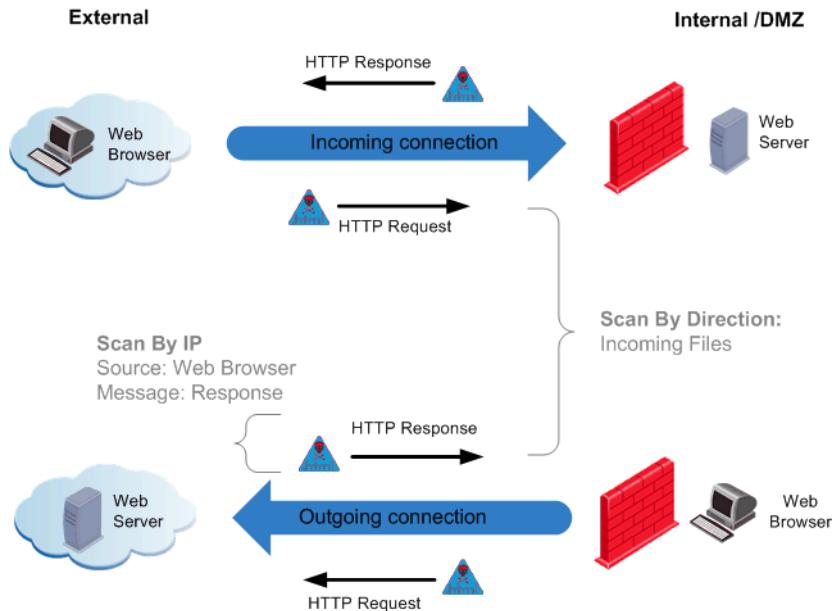
**Figure 8-4** Comparing Scan by Direction to Scan by IP Address for FTP



## Comparing Scan by Direction and Scan by IP for HTTP Protocol

For the HTTP protocol, the difference between Scan by IP and Scan by Direction is illustrated in [Figure 8-5](#). Using Scan by IP, the source and destination of the connection are specified and whether the Request, Response or both is scanned.

**Figure 8-5** Comparing Scan by Direction to Scan by IP Address for HTTP



## Scanning by Direction: Selecting Data to Scan

Using Scan by Direction, you must select the direction of the data to scan, which depends on whether you want 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 security. Its security level lies between trusted internal networks, such as a corporate LAN, and non-trusted external networks, such as the Internet.

Typically, the DMZ contains devices accessible to Internet traffic, for example, Web (HTTP), FTP, SMTP (email), DNS and POP3 servers.

Scan By Direction enables you to define 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, but to still scan traffic passing from the DMZ to internal networks and from the external to internal networks.

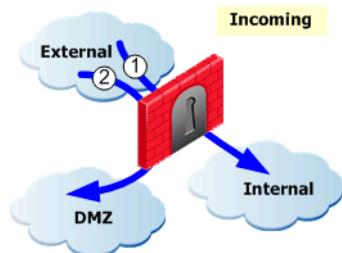
An internal interface can be defined leading to the DMZ in the CI gateway topology.

## **Scan By Direction Options**

The following Scan By Direction options are available:

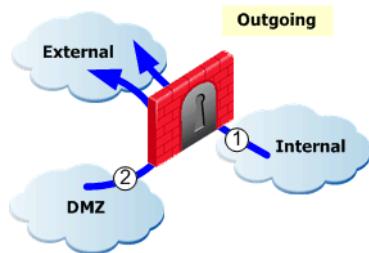
- **Incoming files arriving to** ([Figure 8-6](#)): Files arriving from external interfaces: the internal networks (1), the DMZ (2) and the DMZ and internal networks (1 and 2).

**Figure 8-6** Scanning Options for Arriving Incoming Files

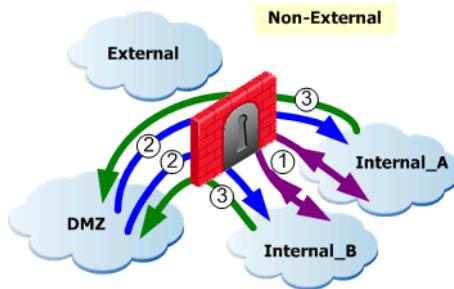


- **Outgoing files leaving** ([Figure 7-7](#)): Files leaving through external interfaces: the internal networks (1), the DMZ (2) and the DMZ and internal networks (1 and 2).

**Figure 8-7** Scanning Options for Leaving Outgoing Files



- **Internal files** ([Figure 8-8](#)): If there is no DMZ, files passing between all internal networks (1). If there is a DMZ, files passing between the DMZ and internal networks and files passing between all internal networks (between internal networks (1), from the DMZ to internal networks (2) and from internal networks to the DMZ (3)).

**Figure 8-8** Scanning Options for Internal Files

## File Type Recognition

CI has a built-in File Type recognition engine, which identifies the types of files passed as part of the connection and enables you to define a per-type policy for handling files of a given type.

You can specify safe file types that are allowed to pass through the CI gateway without being scanned for viruses. It is also possible to configure file types to be scanned or blocked.

The following file types can be configured:

- **Scan:** Performs Anti-Virus file scanning according to the settings in the different services pages. By default, all unrecognized file types are scanned.
- **Block:** Does not allow passage of file types that are preset for blocking according to IPS advisories.
- **Pass:** Allows files to pass though the CI gateway without being scanned for viruses. Files specified as this type are considered to be safe.

File types are considered to be safe if they are not known to contain viruses, for example, some picture and video files are considered safe. Other formats are considered to be safe because they are relatively hard to tamper with. What is considered to be safe changes according to published threats and depends on how the administrator balances security versus performance considerations.

CI reliably identifies binary file types by examining the file type signatures (magic numbers). 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 for files that need to be scanned.

When scanning large files, if the whole file is scanned before being made available, the user may experience a long delay before the file is delivered. A similar problem may arise when using client applications with short timeout periods (for example, certain FTP clients) 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 problem, Continuous Download starts sending information to the client while Anti-Virus scanning is still taking place. If a virus is found during the scan, file delivery to the client is terminated.

You can specify the file types for which you do not want Continuous Download to occur. Some file types (for example, Adobe Acrobat PDF and Microsoft Power Point files) 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** - The SMTP and POP3 protocols support Continuous Download for the entire email message.

## Logging and Monitoring

Logging information on the Anti-Virus scan is sent to the Security Management server and can be viewed using SmartView Tracker. Scan results information is shown in the logs. In addition, there are logs for signature updates, new update checks, and download results.

The Anti-Virus status is monitored using SmartView Monitor. The Anti-Virus status appears under the Firewall product. The status contains information on the currently installed signature file and the Anti-Virus engine version. The Anti-Virus status also includes statistics about scanned files and found viruses.

# File Size Limitations and Scanning

## ***General Settings***

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, use the options in the Anti-Virus window to determine:

- Whether to allow files that have not been scanned to pass. Selecting this option leaves you open to virus attacks.
- Whether to block all files. Selecting this option may result in connectivity problems.

## ***File Handling***

The following file handling options are available:

- **Maximum file size to scan:** Limits the file size that is allowed to pass through the gateway. If the file is a compressed archive, the limit applies to the file after decompression (the Anti-Virus engine decompresses archives before scanning them). Before performing Anti-Virus scanning, the gateway reassembles the entire file and then scans it. The limit protects the gateway resources and the destination client.

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. By default, any file type that is not identified as non-archive is assumed to be an archive and the Anti-Virus engine tries to expand it.

- **When file exceeds limit:** Determines whether to scan or block the file.



**Note** - An email is treated as an archive and as a result it is not affected when the file exceeds the limit.

## ***Archive File Handling***

The following file handling archiving options are available:

- **Maximum archive nesting level:** Limits the number of nested archives (one within another). This limit protects the gateway and destination client from attacks that employ deep nesting levels.
- **Maximum compression ratio:** Prevents attacks that employ a small size archive that decompresses into a very large file on target.
- **When archive file exceeds limit or extraction fails:** Determines whether to scan or block the file.

## ***Scan Failure***

The following scan failure options are available:

- **When Anti-Virus engine is overloaded or scan fails:** Determines whether to scan or block the file.
- **When Anti-Virus engine fails to initialize:** Determines whether to scan or block the file.

## UTM-1 Edge Anti-Virus

You can now enable Anti-Virus protection within UTM-1 Edge. Selecting the **Anti-Virus Protection enabled** option indicates that Anti-Virus protection is installed and that updates are sent to the specified gateway.

Using UTM-1 Edge Anti-Virus, you can define the maximum archive file sizes for UTM-1 Edge machines that are scanned, and configure procedures for when these limits are exceeded and/or the scan fails.

The UTM-1 Edge Anti-Virus feature enables you to automatically or manually update virus signatures for UTM-1 Edge machines and provides you with the tools to configure how UTM-1 Edge traffic is scanned.



**Note** - It is important to configure a valid DNS server address on your management and gateway in order for the signature update to work.

The UTM-1 Edge Anti-Virus scanning policy enables you to select the service(s) to and from which a source and/or destination is scanned. Files set for scanning is determined using a classic Rule Base, which defines the source and destination of the connection to be scanned. It is recommended to use this method if you want to define exactly which traffic to scan, for example, if all incoming traffic from external networks reaches the DMZ, you can specify that only traffic to the Anti-Virus servers is scanned.

To enable and configure Anti-Virus protection:

1. From the **General Properties** tab of the UTM-1 Edge gateway, select the **Anti-Virus Protection enabled** option.
2. In the **Edge Anti-Virus** section of the **Anti-Virus & URL Filtering** tab, configure Anti-Virus to work on UTM-1 Edge gateways. All of the Anti-Virus settings in the **Anti-Virus & URL Filtering** tab do not work for UTM-1 Edge machines. The Edge Anti-Virus settings in the **Anti-Virus & URL Filtering** tab only work for UTM-1 Edge machines.

# URL Filtering

## In This Section

<a href="#">Introduction to URL Filtering</a>	page 217
<a href="#">Terminology</a>	page 218
<a href="#">Architecture</a>	page 218
<a href="#">Configuring URL Filtering</a>	page 219

## Introduction to URL Filtering

Access to the Internet can expose your organization to a variety of security threats and negatively affect employee productivity as a result of non-work-related surfing and downloading of files.

Due to the problems associated with excessive employee Web surfing, organizations are turning to URL Filtering to control employee Internet access, reduce legal liability and improve organizational security. URL Filtering enforces filtering rules based on the organization's needs and predefined categories made up of URLs and patterns of URLs.

URL Filtering includes reporting and monitoring tools that capture and present Web traffic data, providing organizations with an in-depth look at how Web surfing affects their organization's security and supports decisions regarding Web surfing limitations.

A Web filter is a function that screens incoming Web pages to determine whether or not to display its Web content. The Web filter verifies the Web page URL against a list of approved sites and blocks access to complete sites or pages within sites that contain objectionable material (for example, pornography, illegal software and spyware).

## Terminology

The following terms are used in URL Filtering applications:

- **Allow List:** A list of allowed URL addresses, for example, a URL in the Allow List is allowed even if it is associated with a category that is blocked.
- **Block List:** A list of blocked URL addresses, for example, a URL in the Block List is blocked even if it is associated with a category that is not blocked.
- **Blocking Notifications:** Contains the message that appears when a URL address is blocked and the URL to which a blocked URL address is redirected.
- **Category:** Contains a group of topics sharing a common attribute (for example, crime, education and games).
- **Network Exceptions:** Contains a list of connections for which URL Filtering should not be enforced.
- **Web Filter:** Enables you to allow or block URLs based on network connections and/or an external categorized database and local exception lists.

## Architecture

When a URL request arrives at a local machine, the machine checks the Network Exceptions List to determine whether to enforce the URL Filtering policy. The URL Filtering policy is activated if the connection is accepted by the Security Policy. If the URL Filtering policy is enforced, the URL header is stripped and the address is sent to the Web Filter engine.

The URL is allowed or blocked based on categories in the predefined database and/or the Web Filter Allow/Block Lists. For example, if the URL address matches two or more categories, and one of them is blocked, the URL address is denied, however, if the same address appears in the Allow List it is accepted.

The Web Filter engine is installed on Check Point Security Gateway and the categories are updated by selecting: **SmartDashboard > Content > URL Filtering > URL Filtering Policy.**

# Configuring URL Filtering

To configure URL Filtering:

1. For each Check Point gateway object, in the **General Properties** page > **Software Blades** > **Network Security**, select **URL Filtering**.
2. In the **Anti-Virus & URL Filtering** tab of **SmartDashboard**, select **URL Filtering > URL Filtering Policy**.
3. On the **URL Filtering Policy** page, configure the following:
  - a. Select one of the following **URL Filtering Policy Modes**:
    - **On**: URL Filtering is active and URLs associated with blocked categories are blocked.
    - **Monitor**: URLs associated with blocked categories are logged and not blocked.
    - **Off**: URL Filtering is off and does not inspect URL addresses.
  - b. In the **Enforcing Gateways** window, select the gateways for which you want to activate URL Filtering. This window contains all of the gateways for which URL Filtering can and has been enforced.
  - c. In the **Categories** list, select the URL categories to block.
    - A green icon indicates that URLs associated with this category are allowed.
    - A red icon indicates that URLs associated with this category are blocked.
  - d. In the **Tracking** section, select how to track a detected URL address. All options other than **None** generate a log record in SmartView Tracker.
4. Select **Advanced > Allow URLs/IPs** to add a URL or IP address to be allowed even if it is associated with a blocked category.
5. Select **Advanced > Block URLs/IPs** to add a URL or IP address to be blocked even if it is associated with an allowed category.

6. Select **Advanced > Network Exceptions** to create a list of the networks connections through which traffic should not be inspected or in order to enforce URL Filtering on all Web traffic. **Network Exceptions** works according to a source and destination Rule Base and does not use the URL Filtering engine.
7. Select **Advanced > Blocking Notifications** to notify the user when the URL request is blocked. Choose one of the options:
  - Enter the message to be displayed when a URL address is blocked according to the URL Filtering policy.
  - Enter the URL to which the user is to be redirected.

# Chapter

# Anti-Spam and Mail

In This Chapter:

- [Introduction to Anti-Spam and Mail Security](#)
- [Mail Management](#)
- [Tracking and Reporting Options](#)

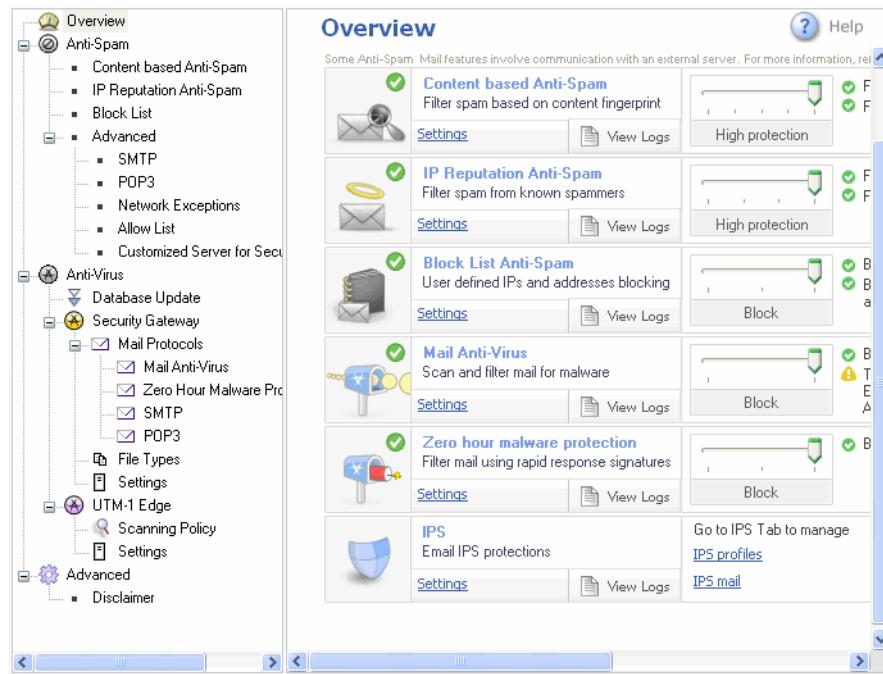
page 222  
page 224  
page 239

# Introduction to Anti-Spam and Mail Security

The relentless and unprecedented growth in unwanted email now poses an unexpected security threat to the network. As the amount of resources (disk space, network bandwidth, CPU) devoted to handling unsolicited emails increases from year to year, employees waste more and more time sorting through unsolicited bulk email commonly known as spam. Anti-Spam and Mail provides network administrators with an easy and central way to eliminate most of the spam reaching their networks.

**Table 9-1** Anti-Spam and Mail Features

Feature	Explanation
<b>Content based Anti-Spam</b>	The core of the Anti-Spam functionality is the content based classification engine.
<b>IP Reputation Anti-Spam</b>	Using an IP reputation service, most of the incoming spam is blocked at connect time.
<b>Block List Anti-Spam</b>	Block specific senders based on IP address or sender's address.
<b>Mail Anti-Virus</b>	Scan and filter mail for malware.
<b>Zero Hour Malware Protection</b>	Filter mail using rapid response signatures.
<b>IPS</b>	Intrusion prevention system for mail protection.

**Figure 9-9** SmartDashboard Anti-Spam & Mail tab

# Mail Management

## In This Section

<a href="#">Mail Security Overview</a>	page 224
<a href="#">Configuring Anti-Spam</a>	page 228
<a href="#">Configuring Anti-Virus</a>	page 234
<a href="#">Logging and Monitoring</a>	page 237
<a href="#">Reporting False Positives to Check Point</a>	page 237

This section covers Anti-Spam and Anti-Virus protections for incoming, outgoing, and internal corporate email.

## Mail Security Overview

On the **Anti-Spam & Mail** tab:

- Select gateways that enforce Anti-Virus checking
- Select gateways that enforce Anti-Spam protection
- Enable automatic updates
- View settings and logs

### ***Anti-Spam***

A typical spam outbreak lasts only a few hours but during that time, many millions of unsolicited messages bombard the corporate mail server. To generate a maximum return on investment, the spammer will have varied the content of each message to prevent its identification as spam. Nonetheless, all messages within the same outbreak share at least one and often more than one unique, identifiable value which can be used to distinguish the outbreak — for example a link to a specific commercial website. Different spam attacks are often launched from the same network of zombie machines — this constitutes a characteristic, a recurring pattern or value that can be logged and analyzed.

The Anti-Spam functionality employs unique licensed technology. Unlike many Anti-Spam applications that rely on searching for keywords and a lexical analysis of the content of an email message, this Anti-Spam solution classifies spam by analyzing known and emerging distribution patterns. By avoiding a search for key

words and phrases that might classify a legitimate email as spam and instead focusing on other message characteristics, this solution offers a high spam detection rate with a low number of false positives.

To preserve personal privacy and business confidentiality, only select characteristics are extracted from the message envelope, headers, and body (no reference to actual content or attachments are included). Hashed values of these message characteristics are sent to a Detection Center for pattern analysis. The Detection Center identifies spam outbreaks in any language, message format, or encoding type. Responses are returned to the enterprise gateway within 300 milliseconds.

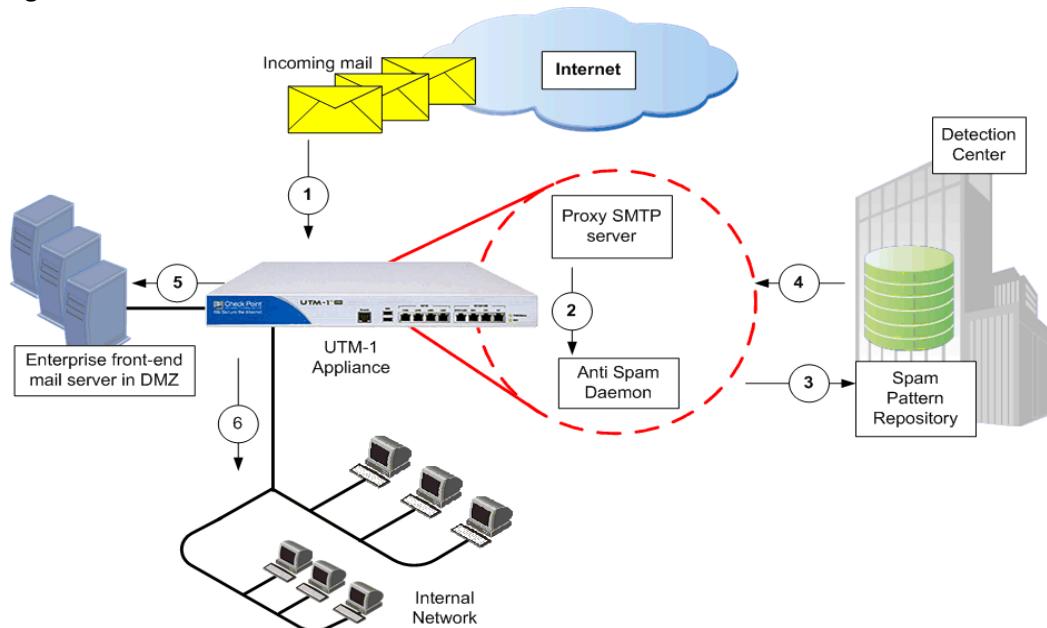
Key benefits of an active Anti-Spam policy configured in SmartDashboard:

- Real-time protection
- High spam-detection rate.
- Spam detection in any language across all message formats.

Once identified, the network of zombie machines is blacklisted. If the network changes its behavior, for example no longer launches spam attacks, the network is removed from the black list.

## Architecture

Figure 9-10 Mail Architecture



1. Proxy SMTP server on the gateway receives incoming mail
2. The SMTP proxy forwards the mail to an Anti-Spam daemon to extract selected message characteristics, and produce a hash fingerprint.
3. Using a special Anti-Spam protocol, the Anti-Spam daemon queries the Detection center. The hashed fingerprint is compared to other fingerprints in the pattern repository to determine whether the email is spam.
4. The detection classifies the email as either spam or not spam, and returns the result to the gateway.
5. If the email has been classified as spam, the email is flagged as such (in the header or subject) and forwarded to the enterprise mail server.
6. The mail server forwards the email to its recipient on the network. Because the header or subject has been flagged as spam, recipients can use that tag or marker to set up filtering rules in their native mail program — for example in **Microsoft Outlook** a rule can be configured to delete all emails with the word SPAM in either the subject line or header.

To prevent delays while large email files are scanned for Spam, a feature known as *Adaptive Continuous Download* transfers email to the recipient while Anti-Spam detection takes place.

## ***Adaptive Continuous Download***

For emails that need to be scanned, the Anti-Spam engine acts as a proxy which caches the file before delivering it to the recipient. If an email happens to be a large file, the recipient may experience delays before the file is delivered. To avoid delays, *Adaptive Continuous Download* starts delivering the email to the recipient while Anti-Spam scanning is still in progress. If the email is designated as Spam, the email is flagged as spam before it is completely transferred to the recipient. SMTP and POP3 protocols support Adaptive Continuous Download for the entire email message.

# Configuring Anti-Spam

## In This Section

Configuring a Content Anti-Spam Policy	page 228
Configuring an IP Reputation Policy	page 229
Configuring a Block List	page 230
Configuring Anti-Spam SMTP	page 230
Configuring Anti-Spam POP3	page 231
Configuring Network Exceptions	page 231
Configuring an Allow List	page 232
Selecting a Customized Server	page 232
Anti-Spam on UTM-1 Edge Devices	page 232
Bridge Mode and Anti-Spam	page 233

## ***Configuring a Content Anti-Spam Policy***

A content Anti-Spam policy is set on the **Anti-Spam & Mail** tab of SmartDashboard > **Anti-Spam** > **Content based Anti-Spam**.

1. Use the slider to select an Anti-Spam policy protection level.
2. Select flagging options.
3. In the **Security Gateway Engine settings** section, set a maximum data size to scan.
4. In the **UTM-1 Edge Engine settings** section, set a confidence level for spam and suspected spam.

A spam confidence level is a grade or rating (usually between zero and a hundred) used decide whether a particular email message should be treated as spam. For example, if the confidence level is set to 70, then all email messages rated at 70 or above will be treated as spam.

SofaWare UTM-1 Edge devices contain their own Anti-Spam engines. Values entered in the **UTM-1 Edge Engine settings** section are used to correlate SofaWare Anti-Spam engine ratings with Check Point Anti-Spam engine ratings. For example if a particular email message is rated by the SofaWare Anti-Spam engine as 90, and this value, once translated into Check Point ratings, means the email should be treated as spam, then the **Actions** defined for Spam or Suspected spam on the **Anti-Spam Policy** page are enforced.

5. Select **Tracking Options** for **Spam**, **Suspected Spam**, or **Non Spam**. Tracking options include:
  - None (no logging)
  - Log
  - Popup Alert
  - Mail Alert
  - SNMP trap alert
  - Three custom user-defined scripts.

## ***Configuring an IP Reputation Policy***

This window enables IP reputation, an Anti-Spam mechanism that checks the IP address of the message sender (contained in the opening SYN packet) against a dynamic database of suspect IP addresses. If, according to the IP reputation service, the originating network has a reputation for sending spam, then the spam session is blocked at connect time. In this way, the IP reputation feature creates a list of trusted email sources.

1. Use the slider to select an IP Reputation Policy:

**Table 9-2** IP Reputation Policy

Policy	Result
Off	No IP Reputation service
Monitor Only	Monitors spam and suspected spam
Medium Protection	Rejects spam and monitors suspected spam
High Protection	Rejects spam and suspected Spam

2. Select tracking options for **Spam**, **Suspected Spam**, or **Non spam**. Tracking options include
  - None (no logging)
  - Log
  - Popup Alert
  - Mail Alert
  - SNMP trap alert
  - Three custom user-defined scripts.

## ***Configuring a Block List***

A list of email sources to block can be configured according to either the senders name, domain name, or IP address.

1. Use the slider to select a Block Policy:

**Table 9-3** Block Policy

Block Policy	Result
Off	No blocking
Monitor Only	Monitors sends by IP and email address
Block	Blocks senders by IP address and email address

2. In the **Blocked senders\domains** section, click **Add** and enter the name of a sender or domain to be rejected.
3. In the **Blocked IPs** section, click **Add** and enter an IP address that should be blocked.
4. From the drop-down list in the **Tracking** section, select a tracking option for either blocked mail or non spam.

## ***Configuring Anti-Spam SMTP***

SMTP traffic can be scanned according to direction.

1. Select a scanning direction for:
  - Incoming files
  - Outgoing files
  - Internal files through the gateway
2. Select **Activate Continuous download** to avoid client time-outs when large files are scanned.

See “[Adaptive Continuous Download](#)” on page 227 for further information.

## Configuring Anti-Spam POP3

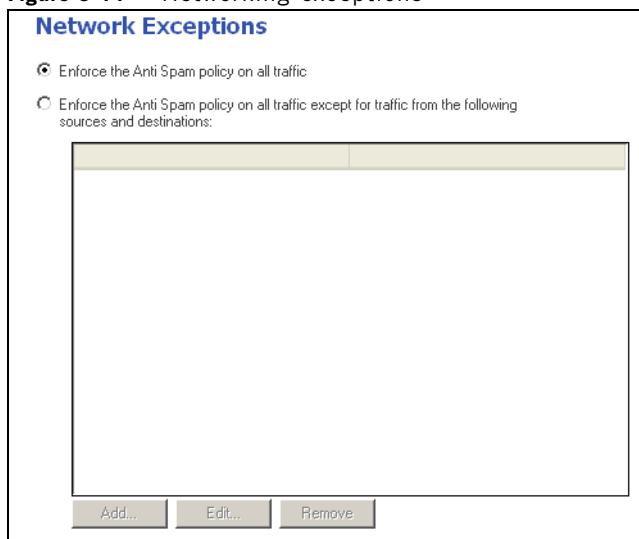
POP3 traffic can be scanned according to direction.

1. Select a scanning direction for:
  - Incoming files
  - Outgoing files
  - Internal files
2. Select **Activate Continuous download** to avoid client time-outs when large files are scanned.  
See "["Adaptive Continuous Download" on page 227](#)" for further information.

## Configuring Network Exceptions

An Anti-Spam policy can be enforced on all email traffic or only on traffic that has not been deliberately excluded from the policy.

**Figure 9-11** Networking exceptions



To exclude sources and destinations:

1. In the **Anti-Spam & Mail** tab, click **Anti-Spam > Advanced > Network Exceptions**.
2. Select **Enforce the Anti-Spam policy on all traffic except for traffic between the following sources and destinations**.
3. Click **Add**. The **Network Exception** window opens.

4. For **Source** and **Destination**, select **Any**, or select **Specific** and one gateway from each list.
5. Click **OK**.

## ***Configuring an Allow List***

A list of email sources to allow can be configured according to either the senders name and domain name, or IP address.

1. In the **Anti-Spam & Mail** tab, click **Anti-Spam > Advanced > Allow List**.
2. In the **Allowed Senders / Domains** section, click **Add** and enter the name of a sender or domain to be allowed.
3. In the **Allowed IPs** section, click **Add** and enter an allowed IP address.
4. From the drop-down list in the **Tracking** section, select a tracking option.

## ***Selecting a Customized Server***

You can select an alternative data center for Anti-Spam analysis.

To select a data center:

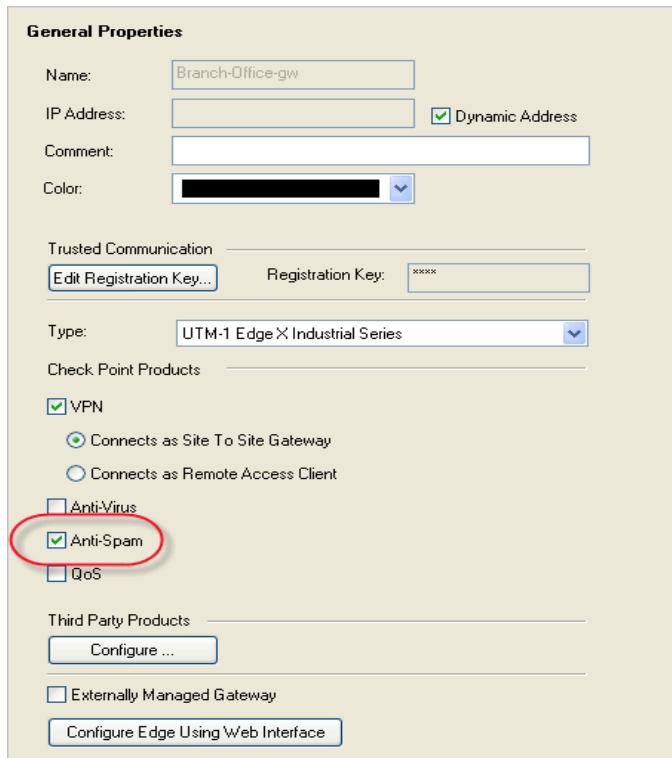
1. In the **Anti-Spam & Mail** tab, click **Anti-Spam > Advanced > Customized Server**.
2. Select **Use Customized Server**.
3. From the drop-down list, select a server.

## ***Anti-Spam on UTM-1 Edge Devices***

Anti-Spam protection is available on UTM-1 Edge devices.

To configure Anti-Spam on UTM-1 Edge devices:

1. Open the **General Properties** window of the UTM-1 Edge gateway.
2. Select the **Anti-Spam** option.

**Figure 9-12** Enabling Anti-Spam on UTM-1 Edge devices.

## ***Bridge Mode and Anti-Spam***

If an UTM-1 appliance is configured to run in bridge mode, Anti-Spam is supported providing that:

- The bridge interface has an IP address
- The bridge interface has a default gateway

# Configuring Anti-Virus

## In This Section:

Configuring Mail Anti-Virus	page 234
Configuring Zero Hour Malware Protection	page 235
Configuring File Types	page 235
Configuring Settings	page 236
Configuring a Disclaimer	page 236

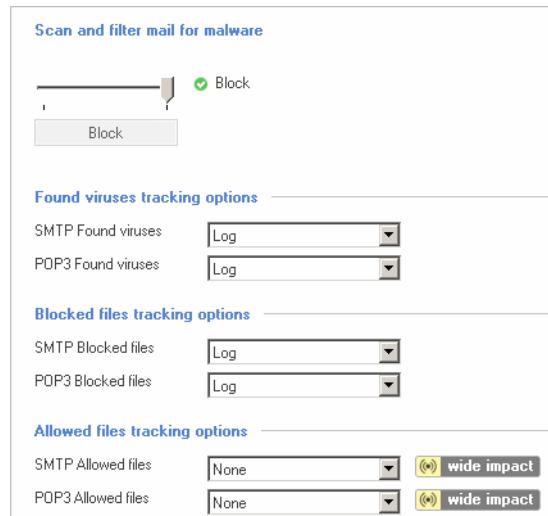
## ***Configuring Mail Anti-Virus***

The Mail Anti-Virus policy prevents email from being used as a virus delivery mechanism.

To configure a mail Anti-Virus policy:

1. In the **Anti-Spam & Mail** tab, click **Anti-Virus > Security Gateway > Mail Protocols > Mail Anti-Virus**.
2. Set the slider to **Block**.
3. Select tracking options for either all POP3 and SMTP mail, or just blocked mail.

**Figure 9-13** Mail Anti-Virus



## ***Configuring Zero Hour Malware Protection***

By proactively scanning the Internet, the Data Center identifies massive virus outbreaks as soon as they occur. This Zero-Hour solution provides protection during the critical time it takes to discover a new virus outbreak and assign it a signature.

1. In the **Anti-Spam & Mail** tab, click **Anti-Virus > Security Gateway > Mail Protocols > Zero Hour Malware Protection**.
2. Using the slider, select a Zero hour malware protection level:
  - Off
  - Monitor Only
  - Block
3. Select tracking options for SMTP and POP3 mail.

## ***Configuring File Types***

In the **Anti-Spam & Mail** tab, click **Anti-Virus > Security Gateway > File Types** page, set an action to take place when a file of a certain type passes through the gateway. Certain file types can pass through the gateway without being scanned for viruses. For example, picture and video files are normally considered safe. Other formats can be considered safe because they are relatively hard to tamper with. Update the list as necessary.

On this window you can also configure Continuous Download options. (See “[Adaptive Continuous Download](#)” on page 227 for more information.)

**Figure 9-14** File types

File Types			
	( wide impact		
Type	Description	Action	
7z	7z archive data	Scan	Pass
8BPS	8BPS Adobe Photoshop Image	Scan	Pass
ace	ACE compressed archive	Scan	Pass
AFX compressed file data	AFX compressed file data	Scan	Pass
qt	Apple QuickTime	Scan	Pass
arc	ARC archive data	Scan	Pass
arj	ARJ archive data	Scan	Pass
bz	bzip compressed data	Scan	Pass
b2	bzip2 compressed data	Scan	Pass
class	compiled Java class data	Scan	Pass
Unknown	Default Scan Values for Unknown File Types	Scan	Pass
eps	DOS EPS Binary File	Scan	Pass
gif	GIF image data	Scan	Pass
win.rar	win.rar compressed data	Scan	Pass

**Update...** **Show Continuous Download options**

## ***Configuring Settings***

In the **Anti-Spam & Mail** tab, click **Anti-Virus > Security Gateway > Settings** page, define maximum sizes for files and archives that should be scanned. Configure actions to take if the set limits are exceeded, or when a scan fails.

## ***Configuring a Disclaimer***

A custom disclaimer notice can be created.

**Figure 9-15** Disclaimer notice

<b>Disclaimer</b>
<input checked="" type="checkbox"/> Add disclaimer to email scanned by Anti Virus and Anti Spam engines
Scanned by Check Point VPN-1 UTM Content Inspection

1. In the **Anti-Spam & Mail** tab, click **Advanced > Disclaimer**.
2. Select **Add disclaimer to email scanned by Anti-Virus and Anti-Spam engines**.
3. In the text box, type your disclaimer notice.

## Logging and Monitoring

Logs derived from Anti-Spam scanning are sent to Security Management server, and viewed using SmartView Tracker.

Anti-Spam status is monitored using SmartView Monitor. The Anti-Spam status appears under the Firewall product. The status contains information such as the Anti-Spam engine version. Anti-Spam status also includes statistics regarding scanned files. See also: [Tracking and Reporting Options page 239](#).

## Reporting False Positives to Check Point

A small number of genuine emails will inevitably be classified as spam. To help Check Point fine-tune the Anti-Spam service, please report them to Check Point support.

The sender of an email that is falsely classified as spam will receive an email notification that the email could not be delivered. This email contains an **Email session ID**.

1. Request the email session ID from the sender.
2. Open SmartView Tracker.
3. On the **Log tab > Content-based Anti-Spam** section locate the email session ID.
4. Open the **Record Details** and click **Copy**.
5. At the **Check Point Support Center**, open a Service Request and paste in the record details.

For more information on how to create and view Service Requests, see **sk31615** at: <http://supportcontent.checkpoint.com/solutions?id=sk31615>

**Figure 9-16** Record details

Network & Endpoint Active Management

lv\_messecc\_all\_recs.fws : All

No. Date Time Origin Service Source Src. Country Destination

No.	Date	Time	Origin	Service	Source	Src. Country	Destination
1	12Nov2008	11:32:54	cptmodule	smtp	192.168.0.1	mailserver	
2	12Nov2008	11:33:34	cptmodule	smtp	192.168.0.1	mailserver	
3	12Nov2008	11:33:51	cptmodule	smtp	192.168.0.1	mailserver	
4	12Nov2008	11:34:05	cptmodule	smtp	192.168.0.1	mailserver	
5	12Nov2008	11:35:42	cptmodule	smtp	192.168.0.1	mailserver	
6	12Nov2008	11:36:07	cptmodule	smtp	192.168.0.1	mailserver	
7	12Nov2008	11:36:42	cptmodule	smtp	192.168.0.1	mailserver	
8	12Nov2008	11:44:58	cptmodule	smtp	192.168.0.1	mailserver	
9	12Nov2008	11:46:18	cptmodule	smtp	192.168.0.1	mailserver	
10	12Nov2008	11:47:01	cptmodule	smtp	192.168.0.1	mailserver	
11	12Nov2008	11:51:18	cptmodule	smtp	192.168.0.1	mailserver	
12	12Nov2008	11:51:23	cptmodule	pop-3	192.168.0.1	mailserver	
13	12Nov2008	11:52:48	cptmodule	smtp	192.168.0.1	mailserver	
14	12Nov2008	11:52:55	cptmodule	pop-3	192.168.0.1	mailserver	
15	12Nov2008	15:00:45	cptmodule	pop-3	192.168.0.1	mailserver	
16	12Nov2008	15:01:14	cptmodule	pop-3	192.168.0.1	mailserver	
17	12Nov2008	15:01:50	cptmodule	pop-3	192.168.0.1	mailserver	
18	12Nov2008	15:05:15	cptmodule	pop-3	192.168.0.1	mailserver	
19	12Nov2008	15:10:42	cptmodule	smtp	192.168.0.1	mailserver	
20	12Nov2008	15:31:16	cptmodule	M.. pop-3	192.168.0.1	mailserver	
21	12Nov2008	15:54:30	cptmodule	smtp	216.163.176.214	USA	mailserver
22	12Nov2008	15:55:39	cptmodule	smtp	216.163.176.214	USA	mailserver
23	12Nov2008	16:01:25	cptmodule	M.. smtp	216.163.176.202	USA	mailserver
24	12Nov2008	16:02:22	cptmodule	M.. smtp	216.163.176.202	USA	mailserver
25	12Nov2008	16:03:43	cptmodule	M.. smtp	216.163.176.200	USA	mailserver
26	12Nov2008	16:06:42	cptmodule	smtp	216.163.176.200	USA	mailserver
27	12Nov2008	16:09:52	cptmodule	smtp	216.163.176.200	USA	mailserver
28	12Nov2008	16:09:53	cptmodule	smtp	216.163.176.200	USA	mailserver
29	12Nov2008	16:10:26	cptmodule	smtp	216.163.176.200	USA	mailserver
30	12Nov2008	16:10:57	cptmodule	smtp	216.163.176.200	USA	mailserver

Total records in file: 37

Ready

# Tracking and Reporting Options

Anti-Spam tracking and reporting options are available in:

- SmartView Tracker
- SmartView Monitor
- Eventia Reporter

## SmartView Tracker

SmartView Tracker now logs Anti-Spam activity. Record details exist for Number, Date, Time, Product, Interface, Origin, Type, Action, Service, Source, Source country, Destination, Sender, Original sender, Recipients, Original recipients, Spam category, Control, and Information.

Right-clicking on a row displays a new **Follow Email Session ID** option. Following the session provides granular information, as shown in [Figure 9-17](#):

**Figure 9-17** Followed session

No.	Date	Time	Origin	Service	Source	Destination	
5441	3Sep2007	9:17:25	aspm-pilot	TCP smtp	chenlev.checkpoint....	aspm-pilot	1
5442	3Sep2007	9:17:26	aspm-pilot	TCP smtp	chenlev.checkpoint....	aspm-pilot	1
5443	3Sep2007	9:17:26	aspm-pilot	TCP smtp	chenlev.checkpoint....	aspm-pilot	1
5444	3Sep2007	9:17:27	aspm-pilot	TCP smtp	chenlev.checkpoint....	smtp_server	1

## SmartView Monitor

SmartView Monitor reports on URL Filtering, Anti-Spam, and Anti-Virus activity.

## Eventia Reporter

New express reports for content inspection have been added to Eventia Reporter:

- Anti-Virus
- Web (URL) Filtering
- Anti-Spam

## MIB

To facilitate reporting and logging, additional objects have been added to the Check Point MIB.



# Chapter

# Securing Voice Over IP

## In This Chapter

The Need to Secure Voice Over IP	page 242
Introduction to the Check Point Solution for Secure VoIP	page 243
Control Signalling and Media Protocols	page 244
VoIP Handover	page 245
VoIP Application Intelligence	page 247
VoIP Logging	page 251
Protocol-Specific Security	page 252

# The Need to Secure Voice Over IP

Many organizations use Voice over IP (VoIP) connectivity to communicate with remote locations and to carry data, voice and video. VOIP connectivity is also used for video conferences and for other activities that provide efficiency and 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 exits the network. Potential threats from voice and video traffic include:

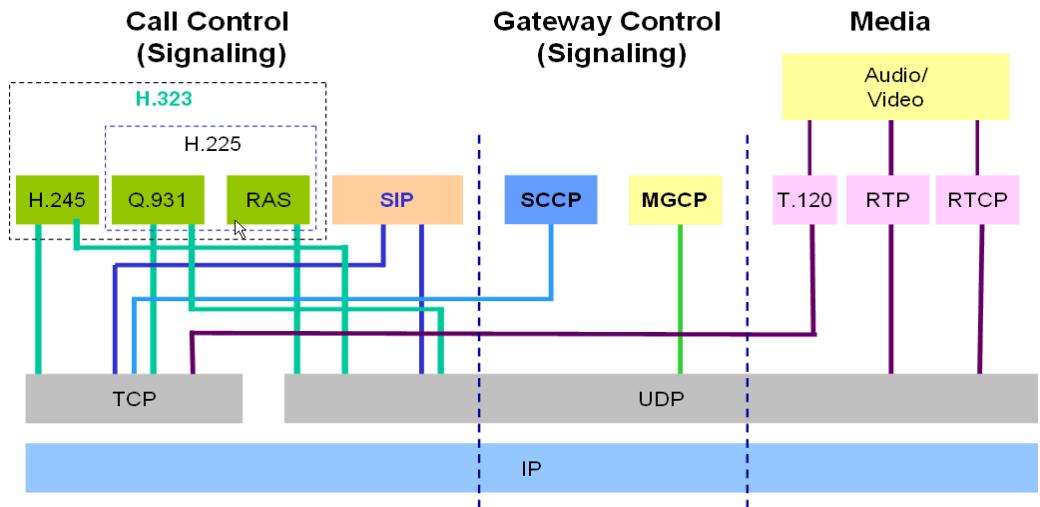
- **Stealing calls:** The caller pretends to be someone else by registering the calls in the name of another user.
- **Call hijacking:** Calls intended for the recipient are redirected to the hijacker.
- **Systems hacking:** Hackers abuse ports opened for VoIP connections.
- **Denial of Service attacks:** A rogue phone floods the network with calls, thereby interfering with proper use of the phone network.

# Introduction to the Check Point Solution for Secure VoIP

Check Point Security Gateway secures VoIP traffic in H.323, SIP, MGCP and SCCP environments.

VoIP calls use a series of complex protocols, each of which can carry potentially threatening information through many ports.

**Figure 10-1** Secured VoIP Protocols: SIP, H.323, MGCP and SCCP



**H.323** Version 4 supports H.245 over UDP/TCP and Q.931 over UDP/TCP and RAS over UDP.  
**SIP** supports TCP and UDP.

Check Point Security Gateway ensures that caller and recipient addresses are where they claim to be and that the caller and recipient are allowed to make and receive VoIP calls. In addition, the firewall examines the contents of the packets passing through every allowed port to ensure that they contain the correct 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 and 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 in [Figure 10-1 on page 243](#), VoIP protocols handle the following call control (or gateway) control and media functions:

- **Call Control (Signalling):** Responsible for setting up the call, finding the peer, negotiating coding protocols, making the connection and ending the call.
- **Gateway Control:** Similar to call control, Gateway Control is responsible for communication between VoIP gateways, rather than between endpoint phones. These gateways act as intermediaries on behalf of the phones.
- **Media:** 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 of a call then use control signals to negotiate dynamically assigned ports that each side opens to receive the RTP/RTCP media stream.

# VoIP Handover

The simplest method of communication between VoIP endpoints is to send both the signalling and media from endpoint to endpoint. In many VoIP networks, however, the endpoints do not know the location of their peers. In this case, the call is managed by a handover device, which allows a VoIP call to reach its peer.

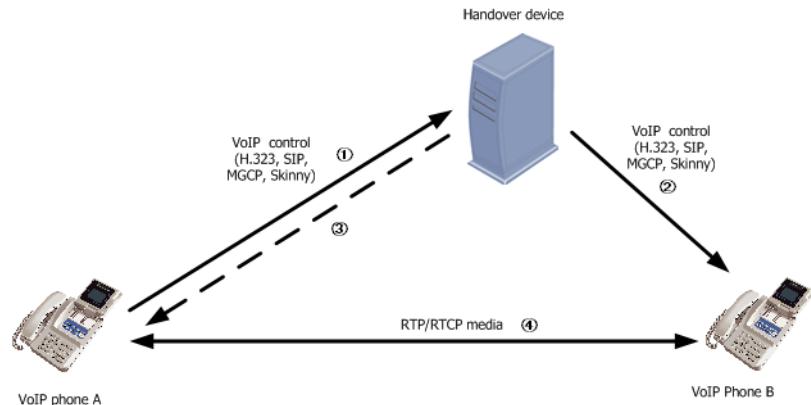
When a handover device is used, the signalling follows a different route through the network than the media. Handover is performed in the following manner:

- **SIP**: By the Proxy and/or Registrar.
- **H.323**: By the Gatekeeper and/or Gateway.
- **MGCP**: By the Call Agent (also called the Media Gateway Controller).
- **SCCP**: By the CallManager.

In a regular phone network and in H.323, the Security Gateway identifies a user based on the telephone number or IP address. In other VoIP networks, the Security Gateway identifies a user in other ways, such as by email address or by 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 through another handover device. After the call setup phase, the RTP/RTCP media always passes from endpoint to endpoint.

[Figure 10-2](#) 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 10-2** VoIP Handover

The following is a typical VoIP Handover workflow:

1. Endpoint A sends control signals to the handover device.
2. The handover device and the endpoints agree on which ports to use to communicate, depending on the protocol and the topology.
3. The handover device routes the control signal to endpoint B.
4. The handover device provides A with the IP address and the destination port of B.
5. A sends the media directly to and from endpoint to endpoint.

### ***When to Enforce Handover***

Although enforcing handover using a VoIP domain adds security by providing access control for the VoIP signal protocols, it is not always possible to define a VoIP domain. The handover device may be maintained by an external carrier and you do not know which machines the handover device controls. Likewise, the handover device may be trusted. In these cases, it is either impossible or unnecessary to enforce the handover and there is no need to define a VoIP domain.

# VoIP Application Intelligence

## In This Section

Introduction to VoIP Application Intelligence	page 247
Restricting Handover Locations Using a VoIP Domain	page 248
Controlling Signalling and Media Connections	page 249
Protocol-Specific Application Intelligence	page 250

## Introduction to VoIP Application Intelligence

Check Point Security Gateway secures VoIP networks by eliminating common threats to VoIP traffic. These threats include call hijacking, call theft, network hacking and Denial of Service (DoS) attacks (for a description of these threats, refer to “[The Need to Secure Voice Over IP](#)” on page 242).

Check Point Security Gateway provides VoIP security by inspecting the VoIP control signals that pass through the gateway. Using information derived from the control signals, the Security Gateway is responsible for:

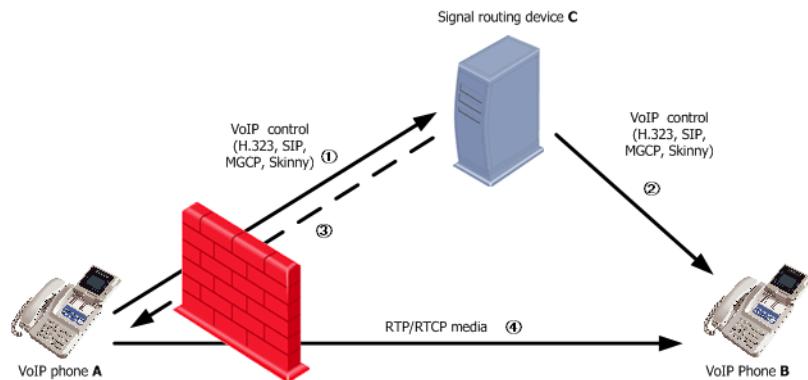
- “[Restricting Handover Locations Using a VoIP Domain](#)”
- “[Controlling Signalling and Media Connections](#)”
- “[Preventing Denial of Service Attacks](#)”
- “[Protocol-Specific Application Intelligence](#)”

# Restricting Handover Locations Using a VoIP Domain

Handover devices are responsible for rerouting call control signals. Check Point Security Gateway prevents the abuse of the redirection capabilities by defining a VoIP domain. The handover device can only route calls to the endpoints in its VoIP domain. The VoIP domain also controls the allowed direction of the call.

For example, in [Figure 10-3](#), if A and B are in the VoIP domain of the handover device C, the Security Gateway ensures that A sends its media streams only to B by verifying that the address of B (which in step 3 the handover device C provided to A) is in the VoIP domain. This process prevents unwanted callers from getting through the firewall.

**Figure 10-3** VoIP Security by Check Point Security Gateway



## Controlling Signalling and Media Connections

Control signals always pass through the Security Gateway. Check Point Security Gateway secures the call by opening RTP/RTCP ports only for those endpoints that were negotiated during signalling. It keeps those ports open only for as long as required and then closes them as soon as the call ends (without waiting for a time-out). The order and direction of the packets is also secured.

### ***VoIP Billing Issues***

The Security Gateway closes RTP/RTCP data connections due to potential security threats in VoIP billing. Security is compromised when the control and media connections follow different routes. The handover device is responsible for billing, but the RTP (the voice media) is not routed through this device. Instead, the RTP is routed between the IP Phones, which poses a security threat because IP Phones can send VoIP control messages that indicate the call has ended, but continue sending and receiving media (the RTP connection).

The Security Gateway secures billing processes by monitoring the relationship between the control and media connections. The firewall inspects the VoIP services and deletes the media connection when the messages in the control connection specify that the media connection must end.

If both endpoints are on the same side of the Security Gateway, the firewall does not open any ports for the media.

## Preventing Denial of Service Attacks

A rogue IP phone could create Denial of Service (DoS) attacks by flooding the network with calls and interfering with the proper use of the phone network.

IPS protects against DoS attacks directed against VoIP networks by limiting the number of call attempts per minute that the Security Gateway allows from an individual IP address. Calls from handover devices are not counted because they make a large number of calls.

## Protocol-Specific Application Intelligence

Check Point Security Gateway understands complex VoIP protocols and performs application layer filtering of SIP, H.323, MGCP and SCCP packets. See also:

- “Application Intelligence for SIP” on page 256.
- “Application Intelligence for H.323” on page 274.
- “MGCP Network Security and Application Intelligence” on page 296.
- “SCCP Network Security and Application Intelligence” on page 303

# VoIP Logging

Check Point Security Gateway provides detailed, protocol-specific logs for VoIP traffic. If VoIP logging is disabled, then only standard logging takes place, showing the source, destination and protocol information. SIP, H.323, MGCP and SCCP events are logged in SmartView Tracker. There is also a predefined SmartView Tracker VoIP log query.

To enable VoIP logging:

- From the **Global Properties Log and Alert** page, select the **Log VoIP connection** option. The following VoIP log fields are displayed:
  - **Reg. IP-phones:** Call registration events. For SIP and MGCP events, this field shows the URL, for example, `example@checkpoint.com`. For H.323 events, this field shows the phone number, for example, `123456#7`.
  - **Source IP Phone and Destination IP Phone:** Call setup events.
  - **Media Type:** Type of media (audio, video, instant messaging, applications or unknown) flowing between the source and destination IP Phones.
  - **Information:** Call and security information, for example, the port used, commands used and illegal direction and setup messages. For MGCP events, the commands are shown.

# Protocol-Specific Security

The following sections describe the specific security requirements of the supported VoIP protocols.

## In This Section

Securing SIP-Based VoIP	page 252
Securing H.323-Based VoIP	page 270
Securing MGCP-Based VoIP	page 294
Securing SCCP-Based VoIP	page 302

## Securing SIP-Based VoIP

### In This Section

SIP Architectural Elements in the Security Rule Base	page 253
Supported SIP RFCs and Standards	page 253
Secured SIP Topologies and NAT Support	page 254
Application Intelligence for SIP	page 256
IPS Application Intelligence for SIP	page 257
Synchronizing User Information	page 259
SIP Services	page 259
Using SIP on a Non-Default Port	page 260
ClusterXL and Multicast Support for SIP	page 260
Configuring SIP-Based VoIP	page 261



**Note** - Before reading this section, read “Introduction to the Check Point Solution for Secure VoIP” on page 243 to “Protocol-Specific Security” on page 252.

The SIP protocol is described in this section only to the extent required to secure SIP traffic using the firewall.

## **SIP Architectural Elements in the Security Rule Base**

SIP contains the following supported architectural elements:

- **SIP Terminal(IP Phone):** Supports real-time, two-way communication with another SIP entity. It supports both signalling (SIP commands) and media. In SIP, only IP enabled phones can be used. IP Phones are defined in SmartDashboard as a network of IP Phones and 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 through.
- **Redirect Server:** Converts SIP URL addresses into zero or more new addresses and returns them to the client 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 and the Registrar are handover devices. Handover devices are defined in SmartDashboard as host nodes that manage a VoIP domain. To limit handover locations, it is recommended to define a VoIP domain. A VoIP domain is typically a network or a group of networks. If the handover devices have the same IP address, only one VoIP domain needs to be defined, otherwise, a VoIP domain must be defined for each device.

In order to allow SIP conversations, you must create rules that permit SIP control signals in the Security Gateway. There is no need to define a media rule that specifies which ports to open and which endpoints that can talk because the Security Gateway derives this information from the signalling. Given a particular VoIP signalling rule, the firewall automatically opens ports for the endpoint-to-endpoint RTP/RTCP media stream.

## **Supported SIP RFCs and Standards**

The following SIP RFCs and standards are supported by Check Point Security Gateway:

- RFC 3261 - The most recent SIP RFC.
- RFC 3372 - Session Initiation Protocol for Telephones (SIP-T).  
See "[Configuring SIP-T Support](#)" on page 268 for details.
- RFC 3311 - UPDATE message.
- RFC 2976 - INFO message.
- RFC 3515 - REFER message.

- RFC 3265 - SIP Events.
- RFC 3262 - Reliability of Provisional Responses.
- RFC 3428 - MESSAGE message.
- MSN messenger over SIP.
- SIP over TCP.
- SIP over UDP.
- SIP early media.

SIP can be configured using the standard, dynamic and nonstandard ports.

## ***Secured SIP Topologies and NAT Support***

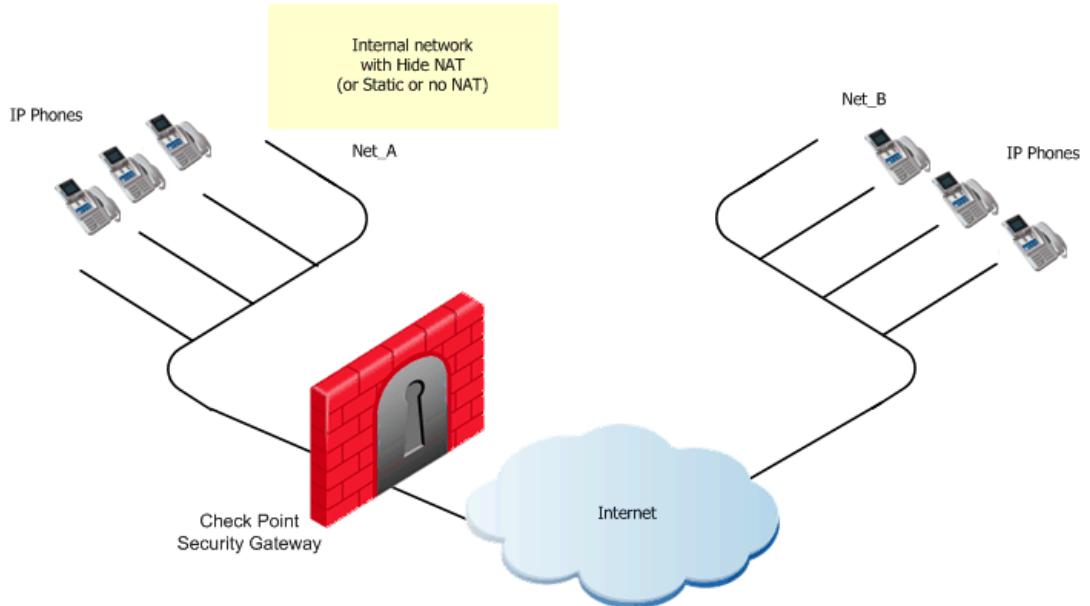
[Table 10-1](#) displays a list of supported SIP deployments. You can configure NAT (either Hide or Static) for the phones in the internal network as well as for the proxy.

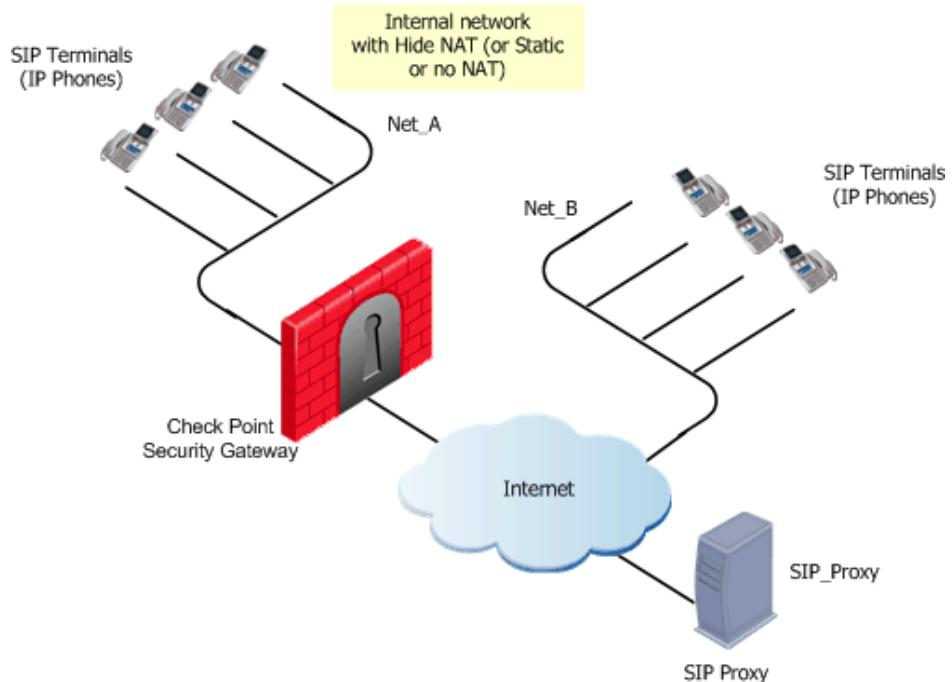
**Table 10-1** Supported SIP Topologies

	No NAT	NAT for Phones - Hide/Static NAT	NAT for Proxy - Static NAT
Peer-to-Peer ( <a href="#">Figure 10-4</a> )	Yes	Yes	Not applicable
Proxy in External ( <a href="#">Figure 10-5</a> )	Yes	Yes	Not applicable

The Proxy is any SIP handover device (Proxy and/or Registrar). In Peer-to-Peer connections topologies both signalling and media pass from endpoint to endpoint. If there is more than one handover device, signalling passes through one or more Proxies or Registrars. Once the call has been set up, the media passes peer to peer.

The SmartDashboard configuration depends on the topology (see also “[Configuring SIP-Based VoIP](#)” on page 261).

**Figure 10-4** SIP Peer-to-Peer Topology

**Figure 10-5** SIP Proxy in Internet with NAT for Internal Phones

### ***Additional Conditions for Using NAT in SIP Networks***

SIP can be used with Network Address Translation (NAT), subject to the following conditions:

- Hide NAT can be used for all types of calls (incoming, outgoing, internal and external). 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.
- When both endpoints are on the trusted side of the Security Gateway, 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.
- Bidirectional NAT of VoIP calls is not supported.

### ***Application Intelligence for SIP***

Check Point Security Gateway restricts handover locations and controls signalling and data connections (see also “[VoIP Application Intelligence](#)” on page 247). For SIP, Application Intelligence ensures that packets conform to RFC 3261 for SIP

---

over UDP and TCP and inspects SIP-based Instant Messaging protocols. It protects against Denial of Service (DoS) attacks and penetration attempts such as connection hijacking and manipulation.

Check Point Security Gateway 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 is denied because this behavior is characteristic of a DoS attack.

Application layer verification includes:

- Checking for binaries and illegal characters in the packets.
- Enforcing RFC header fields.
- Restricting the length of header fields.
- Removing unknown media types.

## ***IPS Application Intelligence for SIP***

Additional security verification for SIP connections can be configured in IPS. There are predefined SIP methods. It is possible to allow or disallow any command as dictated by the security needs.

To access additional SIP connection security features:

1. In IPS, select **Application Intelligence > VoIP > SIP**. The following options are available:
  - **Verify SIP header content:** Ensures that the headers do not contain forbidden characters. If found, the message is blocked.
  - **Block calls from unregistered users:** Prevents unregistered users from making calls.
  - **Block Notify with invalid Subscription state:** Blocks Notify messages without a valid Subscription state header.
  - **Block Basic authorization:** Blocks SIP messages with the Basic authorization header.
  - **Block the destination from re-inviting calls:** Prevents the destination from opening additional data connections with IP addresses that are not the same as the first data connection while a call is still active.
  - **Maximum invitations per call (from both directions):** Defines the maximum number of participants that can participate in a conference call.
  - **Maximum allowed retransmissions:** Defines the maximum number of allowed transmissions.

2. Select **SIP Custom Properties**. The following options are available:
  - **Block SIP early media**: Blocks SIP calls that use the early media mechanism.
  - **Block SIP proxy failover**: Blocks SIP calls that switch SIP proxies during the call.
  - **Block SIP calls that use two different voice connections (RTP) for incoming audio and outgoing audio**: Applies to SIP implementations that use two different RTP connections to transfer voice and/or video information between two peers. If your implementation does not use this scheme, select this option to ensure that the firewall allows only one of these connections.
  - **Block calls using a proxy or a redirect server**: Prevents calls from being made using an SIP server. When selected, only endpoint-to-endpoint calls are permitted. 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.
  - **SIP user suffix length**: Defines the user suffix length, for example, the extension number.
  - **Default proxy registration expiration time period**: Determines the period of time the firewall holds registration information from clients in its database if a timeout is not present in the registration related messages (see also "[Synchronizing User Information](#)" on page 259). The time period should be greater than or equal to the registration time period of the client or the proxy. If the client does not send a user registration message, the registration information is deleted after the defined time period.
3. Select **SIP Filtering**. The following options are available:
  - **Block SIP-based video**: Blocks all applications that use SIP to carry video, which includes the video components of MSN Messenger (when configured to use SIP). The default is not to block.
  - **Block SIP-based audio**: Blocks all applications that use SIP to carry audio, which includes the audio components of MSN Messenger (when 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 block.
    - To selectively block applications provided by MSN Messenger, select **Instant Messengers > MSN over SIP**.
    - To block peer-to-peer applications that allow Instant Messaging, select **Application Intelligence > Peer to Peer**.

- **Block Push to talk over cellular:** Blocks Nokia's proprietary Push to talk messages.
- **Drop unknown SIP messages:** Drops SIP messages that the firewall does not recognize. This option is enabled by default. If disabled, the firewall accepts unrecognized messages, but only if they conform to the SIP RFC (i.e., they are properly formatted and contain the mandatory CALL-ID, FROM and TO fields).

## ***Synchronizing User Information***

The user IP Phone sends SIP messages to the Redirect server in order to register on the network. Once a phone is registered, it can make calls.

These SIP messages cross the Check Point Security Gateway, which reads them. The VoIP user databases on the Security Gateway and the Redirect server are therefore always synchronized.

Registration makes it possible to initiate calls from outside the Security Gateway to phones whose addresses are translated using Hide NAT.

If the Check Point Security Gateway machine is rebooted, the VoIP user database is deleted. The cpstop/cpstart commands do not delete the user database.

## ***SIP Services***

The following predefined SIP services are available:

- **sip** and **sip-tcp**: Used to enforce handover. Use a VoIP domain in the source or destination of the rule together with the **sip** service.
- **sip\_any** and **sip-tcp\_any**: Used if not enforcing handover. 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** or **sip-tcp\_any** service. If a VoIP domain is used with the **sip\_any** or **sip-tcp\_any** service, it is equivalent to the **sip** service.

For VoIP equipment that uses SIP TCP, use the **sip-tcp** and **sip-tcp\_any** services. When it uses UDP, use the **sip** and **sip\_any** services.



**Note** - The services **sip** and **sip\_any** cannot be used in the same rule because they contradict each other. The same is true for **sip-tcp** and **sip-tcp\_any**.

When these services are employed, registration messages 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 NATed address, the Security Gateway verifies that the user exists in the sip registration database before allowing the call, which can prevent DoS attacks.

To view a list of the online IP phones:

- Run the `fw tab -t sip_registration -f` command.

## **Using SIP on a Non-Default Port**

By default, SIP uses the UDP port 5060, however, SIP phones and SIP Proxies can be configured to use a different port. Check Point Security Gateway can enforce SIP security on any SIP port. To configure a new port, a new UDP service must be defined in SmartDashboard, with SIP rules defined in the Security Rule Base. You can use both the newly defined service and the predefined services (**sip** and **sip\_any**) in the same rule.

To configure a new SIP service:

1. From the SmartDashboard main menu, select **Manage > Services > New > UDP**.
2. In the **UDP Service Properties** window, name the new service and specify the new SIP port.
3. Click **Advanced**.
4. In the **Advanced UDP Service Properties** window, select the **Protocol Type** and click **OK**.
5. Define a rule in the Security Rule Base that uses the new service.

## **ClusterXL and Multicast Support for SIP**

SIP calls can be made across a ClusterXL gateway cluster in either High Availability or Load Sharing modes. In Load Sharing Mode, the Sticky Decision Function must be enabled (see also the *ClusterXL Administration Guide*).

The `fw_sip_allow_mcast` (true, false) property allows or drops multicast RTP traffic. The default value of this property is false. This is a per gateway property. To change the value, run the `fw ctl set int fw_sip_allow_mcast` command.

## Configuring SIP-Based VoIP

### In This Section

<a href="#">SIP Rules for a Peer-to-Peer No-Proxy Topology</a>	page 261
<a href="#">SIP Rules for a Proxy in an External Network</a>	page 262
<a href="#">SIP Rules for a Proxy-to-Proxy Topology</a>	page 264
<a href="#">SIP Rules for a Proxy in DMZ Topology</a>	page 266
<a href="#">Configuring SIP-Based Instant Messenger Applications</a>	page 268
<a href="#">Configuring SIP-T Support</a>	page 268

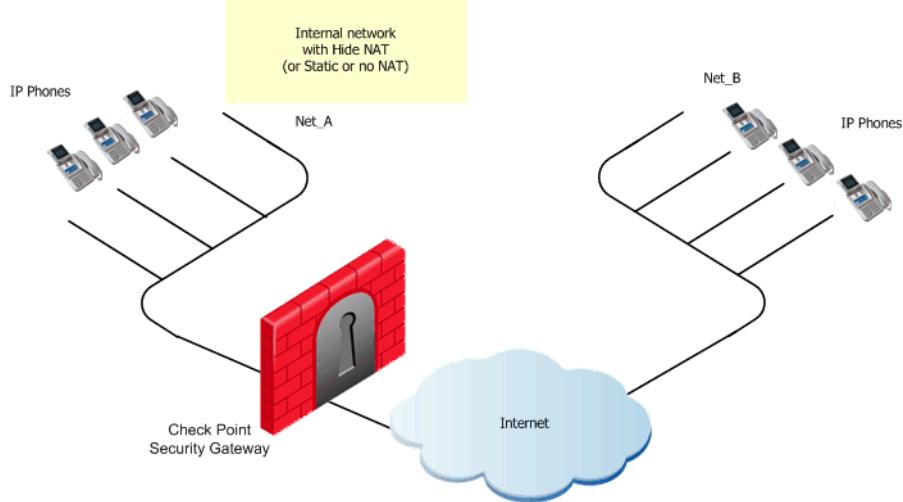


**Note** - Security rules can be defined that allow either bidirectional calls or only incoming or outgoing calls. The examples provided in the following sections describe how to define bidirectional rules.

### SIP Rules for a Peer-to-Peer No-Proxy Topology

This example illustrates SIP rules for a peer-to-peer topology.

**Figure 10-6** SIP Peer-to-Peer Topology



To configure SIP rules for a peer-to-peer topology:

1. Define a rule that allows IP phones in Net\_A to call Net\_Band, and vice versa:

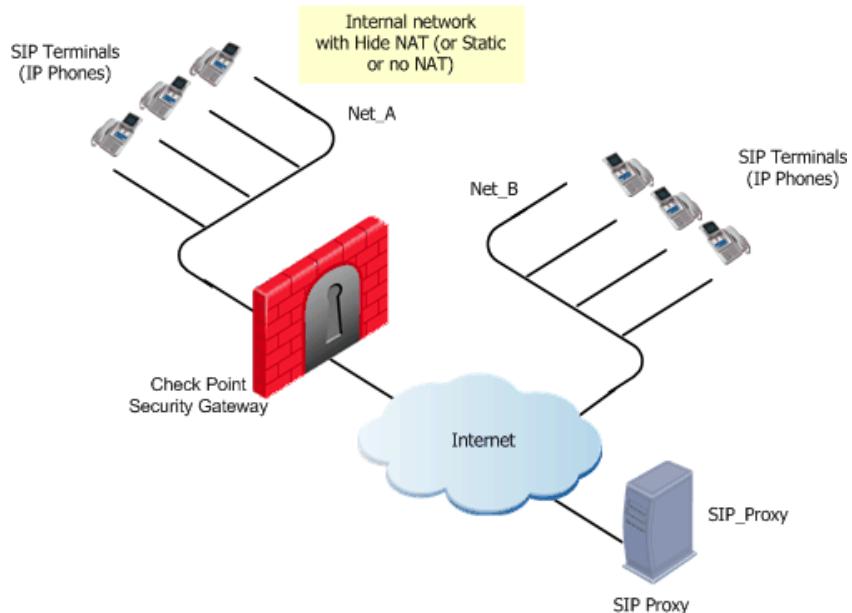
**Table 10-2** Peer-to-Peer SIP Rule

Source	Destination	Service	Action	Comment
Net_A	Net_B	sip or sip-tcp	Accept	Bidirectional calls
Net_B	Net_A			

2. Define Hide NAT (or Static NAT) for the phones in the internal network by editing the network object for Net\_A.
3. In the **NAT** tab, select **Add Automatic Address Translation Rules** and then the **Translation method** (Hide or Static).
4. Select **Application Intelligence > VoIP > SIP** to configure IPS options (see also “[IPS Application Intelligence for SIP](#)” on page 257 or the online help).
5. Install the security policy: **Policy > Install**.

## SIP Rules for a Proxy in an External Network

This example illustrates a topology for both internal SIP and external to a SIP-Proxy.

**Figure 10-7** SIP Proxy in External Network

To enable bidirectional calls between SIP phones in both an internal and an external network (Net\_A and Net\_B), and to define NAT for the internal phones:

1. Define the network objects (nodes or networks) for the IP Phones that are managed by the handover device (SIP Proxy or Registrar), permitted to make calls and whose calls are tracked by the Security Gateway. In [Figure 10-7](#), these are Net\_A and Net\_B.
2. Define the network object for the handover device (SIP\_Proxy).
3. Define the VoIP domain object by right-clicking the Network Objects tree and selecting **New... > VoIP Domains > VoIP Domain SIP Proxy**. [Table 10-3](#) provides a list of VoIP domain definitions. If the Proxy and Registrar (SIP\_Proxy) are 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.

The definition of the VoIP domain depends on whether or not you want to enforce handover locations for phones in the external network. For phones in the internal network, handover should always be enforced.

**Table 10-3**    VoIP Domain Definitions

VoIP Domain Definition	With Handover	No Handover for External Phones
<b>Name</b>	VoIP_Domain	VoIP_Domain_A
<b>Related endpoints domain</b>	Group of Net_A and Net_B	Net_A
<b>VoIP Gateway installed at</b>	SIP_Proxy	SIP_Proxy

4. Define one of the following SIP rules:

- For full handover enforcement, define the following rule:

**Table 10-4**    Bidirectional SIP Rule - Handover Enforced

Source	Destination	Service	Action	Comment
VoIP_Domain Net_A	Net_A VoIP_Domain	sip or sip-tcp	Accept	Bidirectional calls. Handover enforced.

- If you do not want to enforce handover for the external phones (in Net\_B), define the following rules:

**Table 10-5**    Bidirectional SIP Rule - Handover Note Enforced

Source	Destination	Service	Action	Comment
Net_A	Any	sip_any or sip-tcp_any	Accept	Outgoing calls. No handover enforced.
Any	VoIP_Domain_A	sip or sip-tcp	Accept	Incoming calls. Handover enforced.

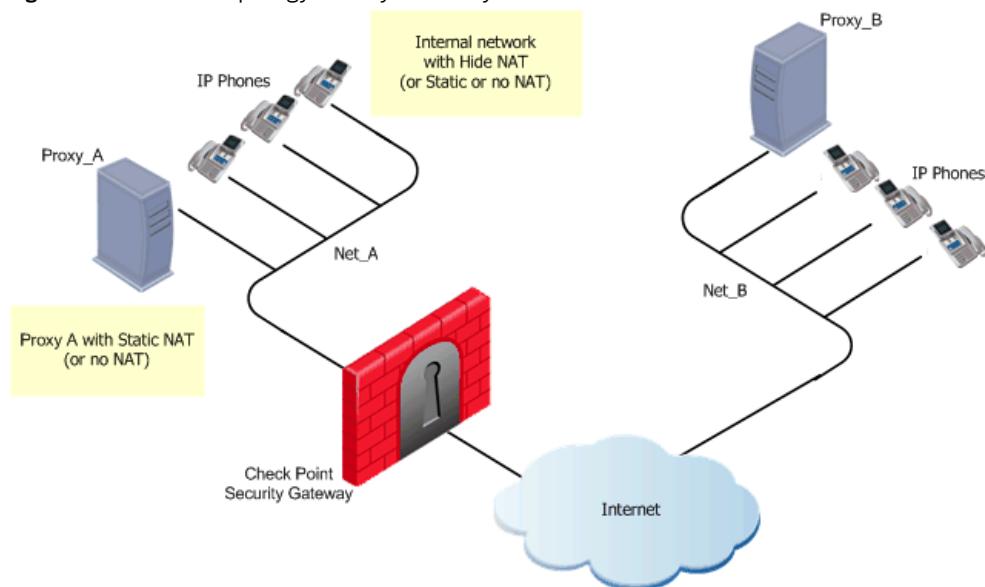
For additional information on SIP services, see “[SIP Services](#)” on page 259.

5. Define Hide NAT (or Static NAT) for the phones in the internal network by editing the network object for Net\_A. In the **NAT** tab, select **Add Automatic Address Translation Rules**, and then the **Translation method** (Hide or Static).
6. Select **Application Intelligence > VoIP > SIP** to configure IPS options (see also “[IPS Application Intelligence for SIP](#)” on page 257 or the online help).
7. Install the security policy: **Policy > Install**.

### SIP Rules for a Proxy-to-Proxy Topology

The next example illustrates a Proxy-to-Proxy topology with Net\_A and Net\_B on opposite sides of the Check Point Security Gateway.

**Figure 10-8** SIP Topology: Proxy-to-Proxy



To enable bidirectional calls between phones in both the internal and the external networks (Net\_A and Net\_B) and to define NAT for the internal phones and the internal Proxy (GW\_A):

1. Define the network objects (nodes or networks) for the phones that are permitted to make calls and whose calls are tracked by the Security Gateway. In [Figure 10-8](#), these are Net\_A and Net\_B.
2. Define the network object for the Proxy objects (Proxy\_A and Proxy\_B).

3. Define Security Rule Base rules with a VoIP domain to enforce handover by right-clicking the Network Objects tree and selecting **New... > VoIP Domains > VoIP Domain SIP Proxy**.
4. Define the following two VoIP domains:

**Table 10-6** Defining VoIP Domains

Name	VoIP_Domain_A	VoIP_Domain_B
Related endpoints domain	Group containing Net_A and Net-B	Group containing Net_A and Net_B
VoIP installed at	Proxy_A	Proxy_B

5. Define one of the following SIP rules:

- For full handover enforcement, define the following rule:

**Table 10-7** External SIP Handover Enforced

Source	Destination	Service	Action	Comment
VoIP_Domain_A	VoIP_Domain_B	sip or sip-tcp	Accept	Bidirectional calls.
VoIP_Domain_B	VoIP_Domain_A	sip or sip-tcp	Accept	Handover enforced.

- If you do not want to enforce handover for the external phones (in Net\_B), define the following rules:

**Table 10-8** External SIP Handover Not Enforced

Source	Destination	Service	Action	Comment
VoIP_Domain_A	Any	sip_any or sip-tcp_any	Accept	Outgoing calls. No handover enforced.
Any	VoIP_Domain_A	sip or sip-tcp	Accept	Incoming calls. Handover enforced.

For additional information on SIP services, refer to “[SIP Services](#)” on [page 259](#).

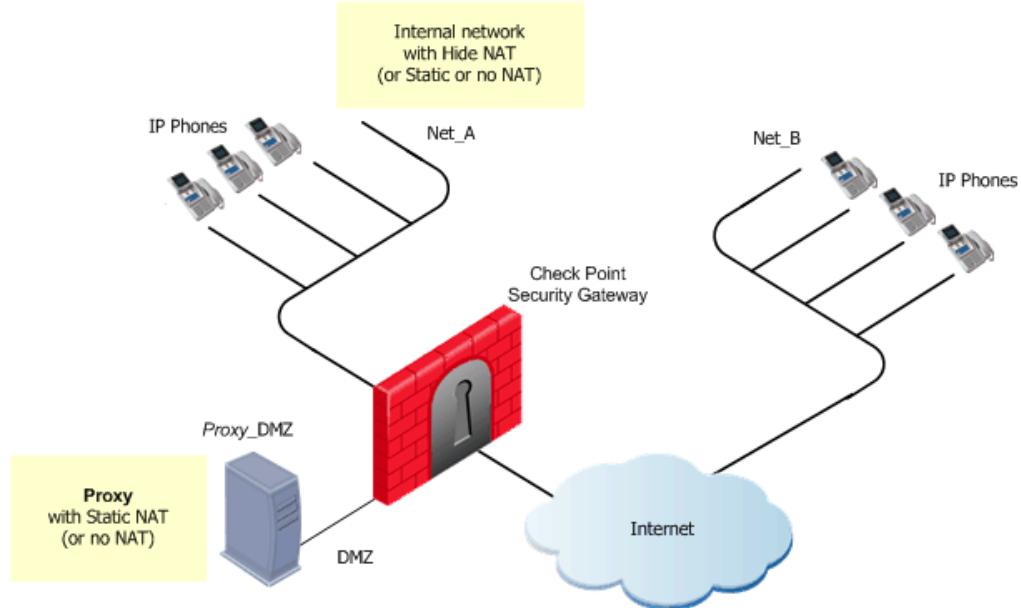
6. Define Hide NAT (or Static NAT) for the phones in the internal network by editing the network object for the internal network (Net\_A). In the **NAT** tab, select **Add Automatic Address Translation Rules** and then the **Translation method** (Hide or Static).
7. Define Static NAT for the Proxy in the internal network by repeating [step 6](#) for the Proxy object (Proxy\_A).

8. Select **Application Intelligence > VoIP > SIP** to configure IPS options (see also “[IPS Application Intelligence for SIP](#)” on page 257 or the online help).
9. Install the security policy: **Policy > Install**.

## SIP Rules for a Proxy in DMZ Topology

[Figure 10-9](#) illustrates an SIP-based VoIP topology where a Proxy is installed in the DMZ.

**Figure 10-9** SIP Topology: Proxy in the DMZ



To enable bidirectional calls between phones both in an internal and an external network (Net\_A and Net\_B) and to define NAT for the internal phones and the Proxy in the DMZ (Proxy\_DMZ):

1. Define the network objects (nodes or networks) for the phones that are permitted to make calls and whose calls are tracked by the Security Gateway. In [Figure 10-9](#), these are Net\_A and Net\_B.
2. Define the network object for the Proxy (Proxy\_DMZ).

3. Define Security Rule Base rules with or without a VoIP domain to enforce handover by right-clicking the Network Objects tree and selecting **New > VoIP Domains > VoIP Domain SIP Proxy**.

**Table 10-9** VoIP by Domain

VoIP Domain Definition	With Handover
Name	VoIP_Domain
Related endpoints domain	Group containing Net_A and Net_B
VoIP installed at	Proxy_DMZ

4. Define the rules for full handover enforcement.

**Table 10-10** Handover Enforced by Domain

Source	Destination	Service	Action	Comment
VoIP_Domain	Net_A	sip or	Accept	Bidirectional calls.
Net_A	Net_B	sip-tcp		Handover enforced.
Net_B	VoIP_Domain			

For additional information on SIP services, refer to “[SIP Services](#)” on [page 259](#).

5. Define Hide NAT (or Static NAT) for the phones in the internal network by doing the following:
- To edit the network object for Net\_A, In the **NAT** tab, select **Add Automatic Address Translation Rules** and then the **Translation method** (Hide or Static).
  - If using Hide NAT, you must select the **Hide behind IP address** option and type the IP address of the Hiding address of the phones in the internal network.
  - If using Hide NAT, you must add a Node object with the Hide NAT IP address to the **Destination** of the rule(s) defined in [step 4](#).

6. Define Static NAT for the Proxy in the DMZ by creating a node object for the Static address of the Proxy (for example, Proxy\_DMZ\_NATed) and by adding the following manual NAT rules:

**Table 10-11** DMZ Rule in VoIP

Original			Translated			Comment
Source	Destination	Service	Source	Destination	Service	
Proxy_DMZ	Net_B	*Any	Proxy_DMZ : Static	=	=	Outgoing calls
Net_B	Proxy_DMZ_NATed	*Any	=	Proxy_DMZ : Static	=	Incoming calls

7. As for all manual NAT rules, configure proxy-arp. To associate the translated IP address with the MAC address of the Check Point gateway interface that is on the same network as the translated addresses, use the arp command in Unix or the local.arp file in Windows.

The fw ctl arp command displays the ARP proxy table on Security Gateways that run on Windows. On Unix, use the arp -a command.

8. Select **Application Intelligence > VoIP > SIP** to configure IPS options (see “[IPS Application Intelligence for SIP](#)” on page 257 or the online help).
9. Install the security policy: **Policy > Install**.

## Configuring SIP-Based Instant Messenger Applications

For information on configuring MSN Messenger over SIP, refer to “[Configuring SIP-based Instant Messengers](#)” on page 315.

## Configuring SIP-T Support

To configure support for RFC 3372 Session Initiation Protocol for Telephones (SIP-T):

1. Add the \$FWDIR/lib/user.def line on the Security Management server:

```
sipt_hosts = { < first_ip, second_ip> , < first_ip, second_ip> , ....
.....< first_ip, second_ip> } ;
```

where `first_ip` and `second_ip` are the IP addresses between which (bi-directional) SIP-T are allowed. For example, to allow SIP-T between 192.1.1.1 and 192.1.1.2, and between 192.1.1.1 and 192.1.1.3 add the following line:

```
sipt_hosts = { < 192.1.1.1, 192.1.1.2> , < 192.1.1.1, 192.1.1.3> } ;
```

If the file does not exist, create it.

2. Save the file.
3. Install the security policy: **Policy > Install**.

## Troubleshooting SIP

To view a list of all of the online IP phones that Check Point Security Gateway has recorded as having registered:

Run the `fw tab -t sip_registration -f` command. The output of this command is a list in the username; IP address format.

To obtain information on current SIP calls:

Run the `fw tab -t sip_state -f` command. The following output is displayed:

- 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).

# Securing H.323-Based VoIP

## In This Section

H.323 Architectural Elements in the Security Rule Base	page 270
Supported H.323 RFCs and Standards	page 271
Secured H.323 Topologies and NAT Support	page 271
Application Intelligence for H.323	page 274
IPS Application Intelligence Settings for H.323	page 275
Gatekeeper and Gateway Call Routing	page 275
H.323 Services	page 277
Configuring H.323-Based VoIP	page 278



**Note** - Before reading this section, read “Introduction to the Check Point Solution for Secure VoIP” on page 243 to “Protocol-Specific Security” on page 252.

The H.323 protocol is described in this section only to the extent required to secure H.323 traffic using Check Point Security Gateway.

## ***H.323 Architectural Elements in the Security Rule Base***

Check Point Security Gateway supports the following H.323 architectural elements:

- **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.  
IP Phones are defined in SmartDashboard, usually as a network of IP Phones. There is normally no need to define network objects for individual IP Phones.
- **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 provides gateway services as well.
- A **Gateway** provides interoperability between different networks. It translates between the telephony protocol and IP.

The Gatekeeper and Gateway are handover devices. Handover devices are defined in SmartDashboard as host nodes which manage a VoIP domain. In order to limit handover locations, define a VoIP domain. A VoIP domain is typically 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 Security Gateway. There is no need to define a rule for the media that specifies which ports to open and which endpoints will talk. The Security Gateway derives this information from the signalling. Given a particular VoIP signalling rule, the firewall automatically opens ports for the endpoint-to-endpoint RTP/RTCP media stream.

### ***Supported H.323 RFCs and Standards***

- H.323 Versions 2, 3 and 4. Version 4.
- H.225 Versions 2, 3 and 4. Version 4.
- H.245 Versions 3, 5 and 7. Version 7.

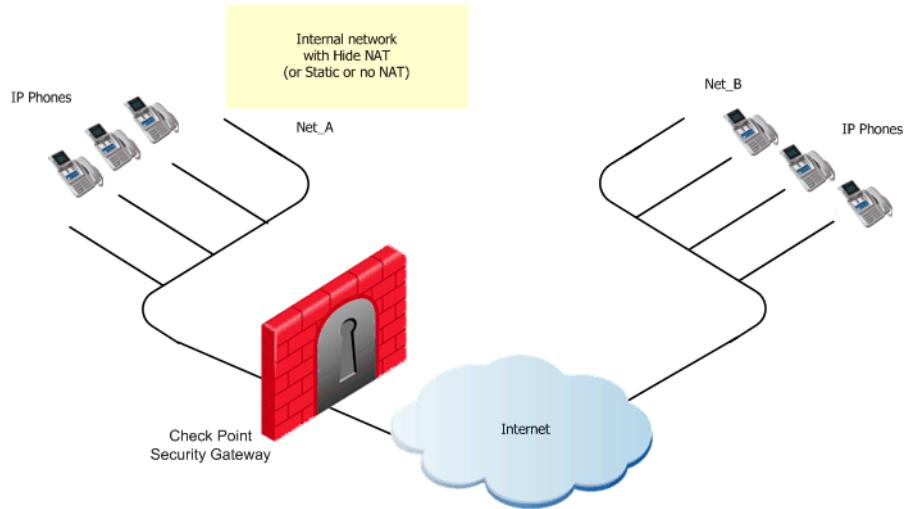
### ***Secured H.323 Topologies and NAT Support***

Check Point Security Gateway supports the H.323 deployments listed in [Table 10-12](#). NAT can be configured (either Hide or Static) for the phones in the internal network, and (where applicable) for the Gateway/Gatekeeper.

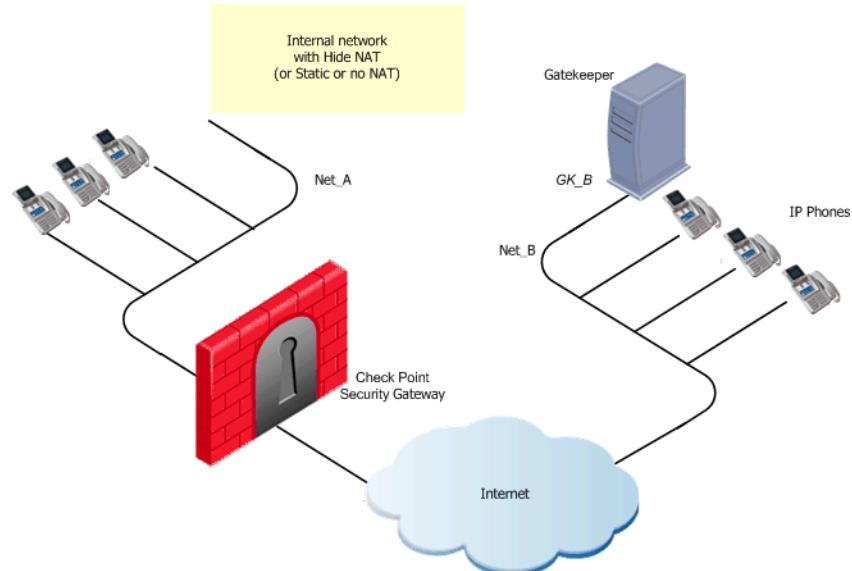
**Table 10-12** Supported H.323 Topologies

	No NAT	NAT for Internal Phones— Hide/Static NAT	NAT for Gateway/ Gatekeeper— Static NAT
Endpoint to Endpoint ( <a href="#">Figure 10-10</a> )	Yes	Yes	Not applicable
Gateway/Gatekeeper in External ( <a href="#">Figure 10-11</a> )	Yes	Yes	Not applicable
Gateway/Gatekeeper to Gateway/Gatekeeper ( <a href="#">Figure 10-12</a> )	Yes	Yes	Yes
Gateway/Gatekeeper in DMZ ( <a href="#">Figure 10-13</a> )	Yes	Yes	Yes

- **Endpoint to Endpoint:** The IP Phones communicate directly, without a Gatekeeper or a Gateway (refer to [Figure 10-10](#)). NAT (both hide and static mode) can be configured for the phones on the internal side of the Security Gateway. No incoming calls can be made when Hide NAT is configured for the internal phones.

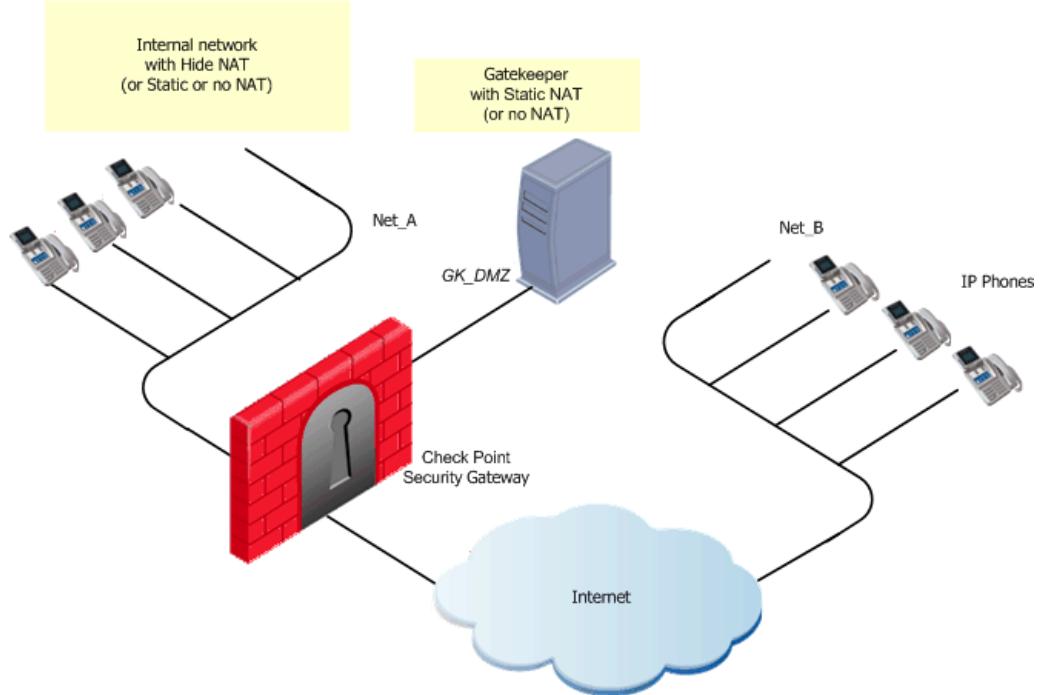
**Figure 10-10** H.323 Topology: Direct Endpoint-to-Endpoint Communication

- **Gatekeeper/Gateway in External Network:** The IP Phones use the services of a Gatekeeper on the external side of the Security Gateway (refer to [Figure 10-11](#)). This topology enables using the services of a Gatekeeper that is maintained by another organization. It is possible to configure Hide NAT (or Static NAT or no NAT) for the phones on the internal side of the Security Gateway.

**Figure 10-11** H.323 Topology: Gatekeeper/Gateway in External Network

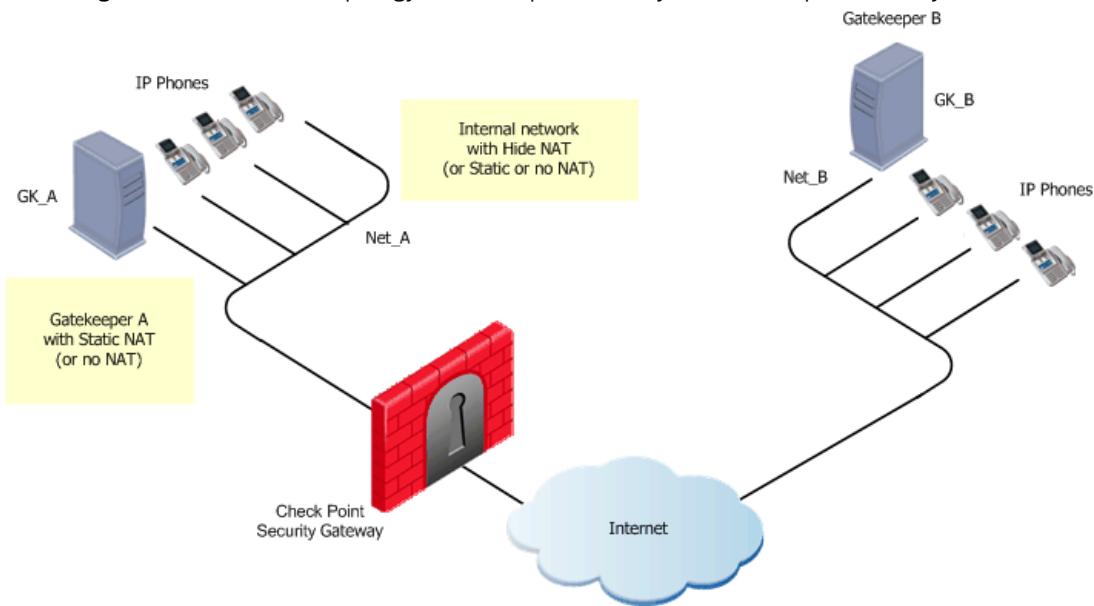
- **Gatekeeper/Gateway in the DMZ:** The same Gatekeeper/Gateway controls both endpoint domains. This topology makes it possible to provide Gatekeeper/Gateway services to other organizations (refer to [Figure 10-12](#)). Static NAT (or no NAT) can be configured for the Gatekeeper/Gateway. Hide NAT (or Static or no NAT) can be configured for the phones on the internal side of the Security Gateway.

**Figure 10-12** H.323 Topology: Gatekeeper/Gateway in the DMZ



- **Gatekeeper/Gateway to Gatekeeper/Gateway:** Each Gatekeeper/Gateway controls a separate endpoint domain (refer to [Figure 10-13](#)). Static NAT can be configured for one of the Gatekeepers/Gateways. For the phones, Hide NAT (or Static NAT) can be configured for the phones on the internal or the external side of the Security Gateway (but not both).

**Figure 10-13** H.323 Topology: Gatekeeper/Gateway to Gatekeeper/Gateway



## ***Application Intelligence for H.323***

Check Point Security Gateway supports H.323 version 4 and below, which includes H.225 version 4 and H.245 version 7. 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 are only 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 illegal use of well-known ports.

Check Point Security Gateway supports *Fast Connect*, an advanced H.323 capability that ensures that audio is available as soon as the phone is answered. This feature is active by default, and is always available.

## ***IPS Application Intelligence Settings for H.323***

The following additional Application Intelligence checks can be configured via IPS Application Intelligence > VoIP > H.323:

- **Block connections re-direction:** Prevents conversations being handed over on both sides. It must be unchecked in order to use Gatekeepers or Gateways.
- **Prevent blank source phone numbers for gatekeeper connections:** Rejects RAS 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.
- **Disable dynamic T.120:** Blocks application-sharing file transfer, used for white board, chat, and application sharing in applications such as Microsoft NetMeeting. T.120 is not allowed by default.
- **Block H.245 Tunneling:** Prevents the encapsulation a H.245 message in any Q.931 message. H.245 tunneling conserves resources, synchronizes call signaling and control, and reduces call setup time. H.245 Tunneling should be allowed, if the VoIP equipment supports it.
- **Disable dynamic opening of H.323 connections opened from RAS messages:** Controls the way the `H323_ras` service works. If the service is allowed in the Rule Base, this setting controls whether control connections required by all H.323 sessions will be dynamically opened by the firewall. If H.323 connections opened from RAS messages are blocked, it is necessary to allow the `H323` service in the Rule Base. This setting applies only to connections that start with RAS (that is allowed and inspected by the `H323_ras` service).
- **Drop H.323 calls that do not start with a SETUP message:** Ensures that if this option is selected, all H.323/Q.931 connections that do not start with a SETUP message are dropped.
- **T120 timeout:** Determines how long a dynamically opened T120 connection can be idle. After this time, the connection is deleted. The default timeout is 3600 seconds.

## ***Gatekeeper and Gateway Call Routing***

H.323 routing modes define which control protocols are allowed to pass between the Gatekeepers or Gateways, and which are allowed to pass directly between the endpoints. Check Point Security Gateway can be configured to allow one or more routing modes. To understand routing modes, a basic understanding of H.323 protocols and the sequence in which they are used is required.

## Signaling and Media Protocols for H.323

The media in H.323 uses the RTP/RTCP and/or T.120 protocols. Signalling is handled by the following H.323 protocols:

- RAS manages registration, admission and status. RAS uses a fixed port: UDP1719.
- Q.931 manages call setup and termination. Q.931 uses a fixed port: TCP1720.
- H.245 negotiates channel usage and capabilities. H.245 uses a dynamically assigned port.

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.

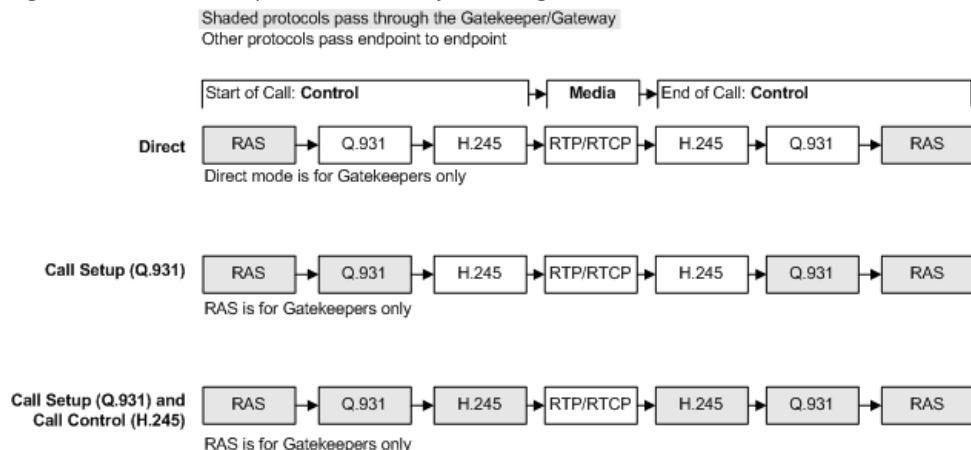
The protocol sequence for a Gateway is the same, except that an endpoint does not use RAS when it connects to the Gateway.

## Routing Modes

H.323 routing modes define which control protocols should pass between the Gatekeepers or Gateways, and which between the endpoints. Check Point Security Gateway can be configured to allow one or more of the routing modes. At least one of the routing modes *must* be selected. If the Security Gateway is configured to allow more than one routing mode, the Gatekeeper/Gateway is free to decide which routing mode to use.

[Figure 10-14](#) illustrates the three routing modes that can be selected.

**Figure 10-14** Gatekeeper and Gateway Routing Modes



The following routing modes are illustrated in [Figure 10-14](#):

- **Direct** mode is for Gatekeepers only, and not for Gateways. 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:



**Note** - The services *H323* and *H323\_any* cannot be used in the same rule because they contradict each other. Similarly, the services *H323\_ras* and *H323\_ras\_any* cannot be used in the same rule.

- **H323\_ras\_only** allows only RAS. Cannot be used to make calls. If this service is used, no Application Intelligence checks (payload inspection or modification) are made. Do not use in the same rule as the *H323\_ras* service.
- **H323\_ras** allows a RAS port to be opened, followed by a Q.931 port. Q.931 then opens a H.245 port if needed, which in turn opens ports for RTP/RTCP or T.120. Use this service to do NAT on RAS messages. Do not use in the same rule as the *H323\_ras\_only* service.
- **H323** allows a Q.931 to be opened (and if needed, a H.245 port,) which in turn opens ports for RTP/RTCP or T.120. Do not use in the same rule as the *H323\_any* service.
- **H323\_any** is like the *H323* service, but also allows the Destination in the rule to be ANY rather than a network object. Only use *H323\_any* if you do not know the VoIP topology, and are not enforcing handover using a VoIP domain. Do not use in the same rule as the *H323* service.

# Configuring H.323-Based VoIP

## In This Section

<a href="#">Choosing the Type of H.323-VoIP Domain</a>	page 278
<a href="#">H.323 Rule for an Endpoint-to-Endpoint Topology</a>	page 278
<a href="#">H.323 Rules for a Gatekeeper-to-Gatekeeper Topology</a>	page 280
<a href="#">H.323 Rules for a Gateway-to-Gateway Topology</a>	page 282
<a href="#">H.323 Rules for a Gatekeeper in the External Network</a>	page 284
<a href="#">H.323 Rules for a Gateway in the External Network</a>	page 286
<a href="#">H.323 Rules for a Gatekeeper in DMZ Topology</a>	page 288
<a href="#">H.323 Rules for a Gateway in DMZ Topology</a>	page 291

## ***Choosing the Type of H.323-VoIP Domain***

Configure a VoIP domain for H.323 phones if they use the Gateway or Gatekeeper to make calls. Select either a Gateway or Gatekeeper object according to the following criteria:

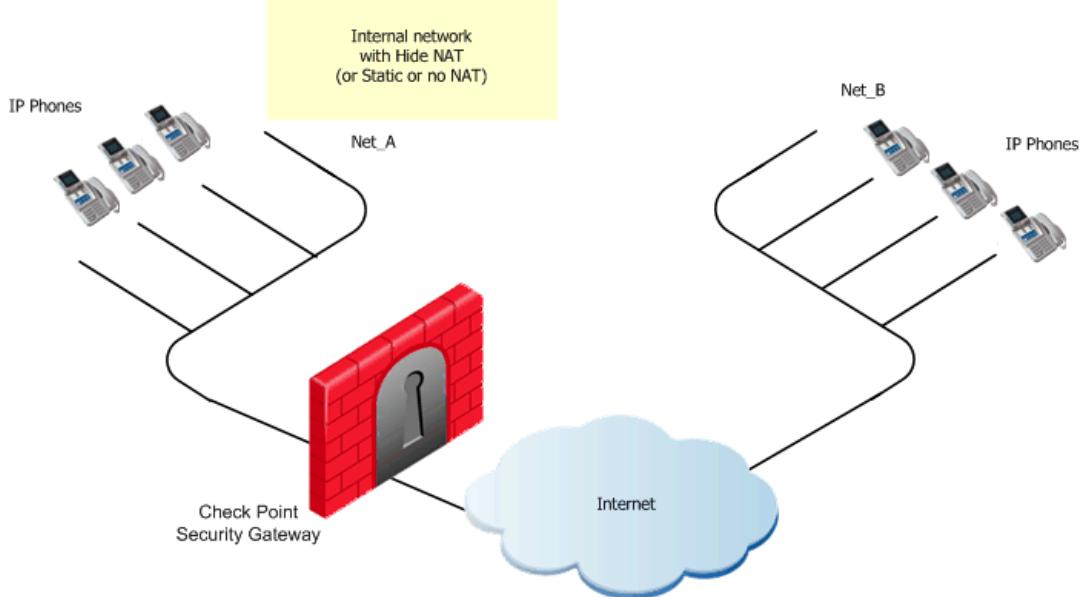
- **Use a VoIP Domain H.323 Gateway** if the first packet that the device sees when a call is initiated is a Q.931/H.225 packet, and not an RAS packet.
- **Use a VoIP Domain H.323 Gatekeeper** if the first packet that the device sees when a call is initiated is an RAS/H.225 packet.

For an H.323 Gatekeeper, the VoIP domain corresponds to the zone of that Gatekeeper. A zone is a collection of terminals that are managed by a single Gatekeeper. A zone has one and only one Gatekeeper.

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.

## ***H.323 Rule for an Endpoint-to-Endpoint Topology***

An endpoint-to-endpoint topology is shown in [Figure 10-15](#), with Net\_A and Net\_B on opposite sides of the Security Gateway. The following procedure explains how to allow bidirectional calls between the phones in the internal network (Net\_A) and phones in an external network (Net\_B), and how to define NAT for the internal phones. No incoming calls can be made when Hide NAT is configured for the internal phones.

**Figure 10-15** H.323 Topology: Direct Endpoint-to-Endpoint Communication

To define an H.323 rule for endpoint-to-endpoint topology:

1. Define the following rule:

**Table 10-13**

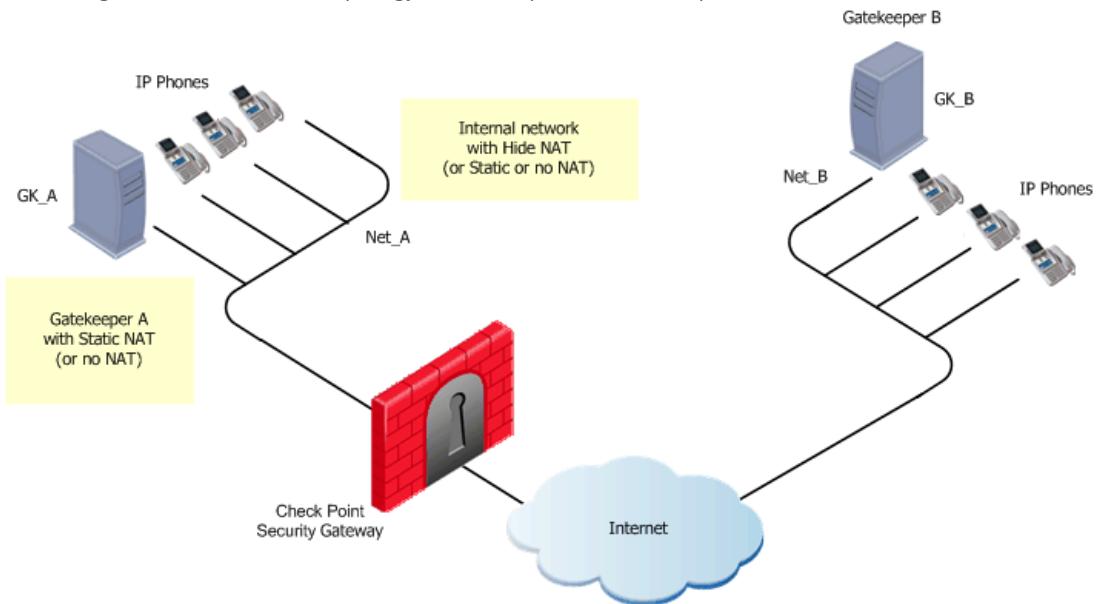
Source	Destination	Service	Action
Net_A	Net_B	H323	Accept
Net_B	Net_A		

2. To define Hide NAT (or Static NAT) for the phones in the internal network, edit the network object for the internal network (Net\_A). In the **NAT** tab, check **Add Automatic Address Translation Rules**, and select the **Translation method (Hide or Static)**.
3. Configure the IPS options under **Application Intelligence > VoIP > H.323** as required. For details, refer to "[IPS Application Intelligence Settings for H.323](#)" on page 275, or the online help.
4. Install the security policy: **Policy > Install**.

## H.323 Rules for a Gatekeeper-to-Gatekeeper Topology

A Gatekeeper-to-Gatekeeper topology is shown in [Figure 10-16](#), with Net\_A and Net\_B on opposite sides of the Security Gateway. The following procedure explains how to allow bidirectional calls between the phones in the internal network (Net\_A) and phones in an external network (Net\_B), and how to define NAT for the internal phones and the internal Gatekeeper (GK\_A).

**Figure 10-16** H.323 Topology: Gatekeeper-to-Gatekeeper



To define an H.323 rule for gatekeeper-to-gatekeeper topology:

1. Define the network objects (Nodes or Networks) for the phones which use the Gatekeeper for registration, and are allowed to make calls, and whose calls are tracked by the Security Gateway.  
In the example in [Figure 10-16](#), these are Net\_A and Net\_B.
2. Define the Network object for the Gatekeeper objects (GK\_A and GK\_B)
3. Define Security Rule Base rules either with or without a VoIP domain.

To enforce handover, define VoIP domains. Right-click the Network Objects tree, and select **New... > VoIP Domains > VoIP Domain H.323 Gatekeeper**. Define two VoIP domains, as follows:

**Table 10-14** VoIP Domains for Gatekeeper-to-Gatekeeper

Name	VoIP_Domain_A	VoIP_Domain_B
<b>Related endpoints domain</b>	Group containing Net_A	Group containing Net_B
<b>VoIP installed at</b>	GK_A	GK_B

4. In the **Routing Mode** tab, define permitted routing modes for the Gatekeepers. For an explanation of the modes, refer to “[Routing Modes](#)” on page 276. It is important to select at least one option.
5. Now define the rules. To enforce handover, define the following rule with VoIP domains:

**Table 10-15** VoIP Handover Enforced

Source	Destination	Service	Action	Comment
VoIP_Domain_A	VoIP_Domain_B	H323_ras	Accept	Bidirectional calls.
VoIP_Domain_B	VoIP_Domain_A			Handover enforced.

If you do not want to enforce handover, define the following rules:

**Table 10-16** VoIP Handover Not Enforced

Source	Destination	Service	Action	Comment
GK_A	GK_B	H323_ras_only	Accept	No handover.
Net_A	Net_A	H323	Accept	No handover.
Net_B	Net_B			

When rules without a VoIP domain are defined, all connections other than H323\_ras must be peer to peer.

For an explanation of the H.323 services, refer to “[H.323 Services](#)” on page 277.

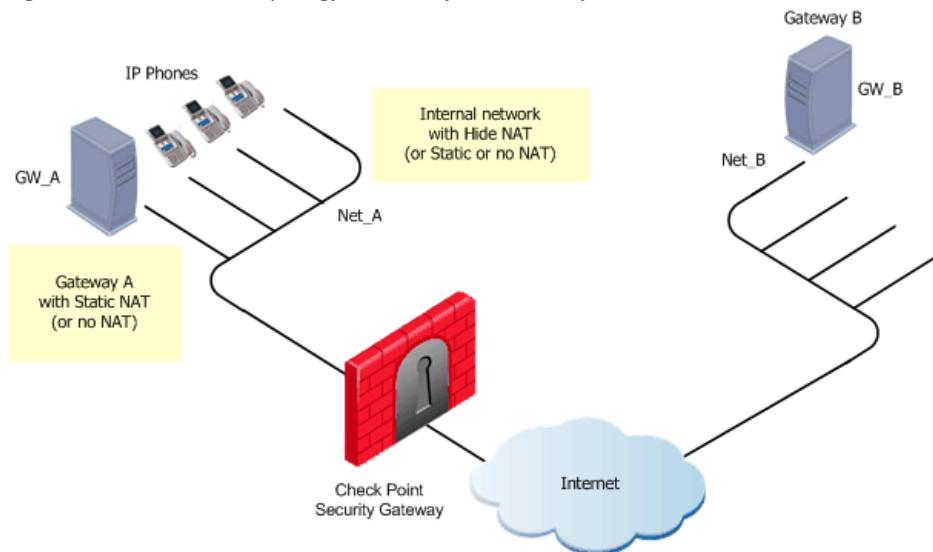
6. To define Hide NAT (or Static NAT) for the phones in the internal network, edit the network object for the internal network (Net\_A). In the **NAT** tab, select **Add Automatic Address Translation Rules**, and select the **Translation method** (Hide or Static).

7. To define Static NAT for the Gatekeeper/Gateway in the internal network, repeat [step 6](#) for the Gatekeeper object (GK\_A).
8. It is recommended to make the time-out of the H323\_ras service equal to or greater than the Gatekeeper registration time-out. Configure the time-outs in the **Advanced Properties** window of the Service object.
9. Configure the IPS options under **Application Intelligence > VoIP > H.323** as required. For details, refer to [“IPS Application Intelligence Settings for H.323” on page 275](#), or the online help.
10. Install the security policy: **Policy > Install**.

## **H.323 Rules for a Gateway-to-Gateway Topology**

A Gateway-to-Gateway topology is shown in [Figure 10-17](#), with Net\_A and Net\_B on opposite sides of the Security Gateway. The following procedure explains how to allow bidirectional calls between the phones in the internal network (Net\_A), and phones in an external network (Net\_B), and how to define NAT for the internal phones and the internal gateway (GW\_A).

**Figure 10-17** H.323 Topology: Gateway-to-Gateway



To define an H.323 rule for gateway-to-gateway topology:

1. Define the network objects (Nodes or Networks) for the phones which are allowed to make calls, and whose calls are tracked by the Security Gateway.  
For the example in [Figure 10-17](#), these are Net\_A and Net\_B.
2. Define the network object for the gateway objects (GW\_A and GW\_B)

3. Define Security Rule Base rules with a VoIP domain to enforce handover. Right-click the Network Objects tree, and select **New... > VoIP Domains > VoIP Domain H.323 Gateway**.
4. Define two VoIP domains, as follows:

**Table 10-17** VoIP Domains for Gateway-to-Gateway

Name	VoIP_Domain_A	VoIP_Domain_B
Related endpoints domain	Group containing Net_A	Group containing Net_B
VoIP installed at	GW_A	GW_B

5. In the **Routing Mode** tab, define permitted routing modes for the Gateways. For an explanation of the modes, refer to “[Routing Modes](#)” on page 276. It is important to select at least one option.
6. Now define the rules. To enforce handover, define the following rule with VoIP domains:

**Table 10-18** VoIP Handover Enforced

Source	Destination	Service	Action	Comment
VoIP_Domain_A	VoIP_Domain_B	H323	Accept	Bidirectional calls.
VoIP_Domain_B	VoIP_Domain_A			Handover enforced.

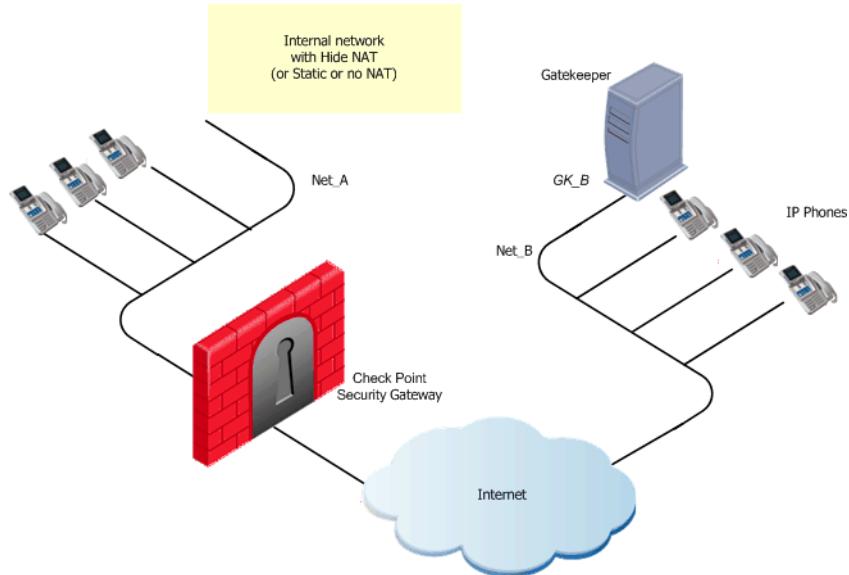
For an explanation of the H.323 services, refer to “[H.323 Services](#)” on page 277.

7. To define Hide NAT (or Static NAT) for the phones in the internal network, edit the network object for the internal network (Net\_A). In the **NAT** tab, select **Add Automatic Address Translation Rules**, and select the **Translation method (Hide or Static)**
8. To define Static NAT for the Gatekeeper/Gateway in the internal network, repeat step 6 for the Gatekeeper/Gateway object (GK\_A).
9. Configure the IPS options under **Application Intelligence > VoIP > H.323** as required. For details, refer to “[IPS Application Intelligence Settings for H.323](#)” on page 275, or the online help.
10. Install the security policy: **Policy > Install**.

## H.323 Rules for a Gatekeeper in the External Network

An H.323 topology with a Gatekeeper in the Internet is shown in [Figure 10-18](#), with Net\_A and Net\_B on opposite sides of the Security Gateway. The following procedure explains how to allow bidirectional calls between the phones in the internal network (Net\_A) and phones in an external network (Net\_B), and how to define NAT for the internal phones.

**Figure 10-18** H.323 Topology: Gatekeeper In External Network



To define an H.323 rule for a gatekeeper in the external network:

1. Define the network objects (Nodes or Networks) for the phones which use the Gatekeeper for registration, and that are allowed to make calls, and whose calls are tracked by the Security Gateway.

For the example in [Figure 10-18](#), these are Net\_A and Net\_B.

2. Define the network object for the Gatekeeper (GK\_B)
3. Define Security Rule Base rules either with or without a VoIP domain.

To enforce handover, define a VoIP domain. Right-click the Network Objects tree, and select **New... > VoIP Domains > VoIP Domain H.323 Gatekeeper**.

- 
4. Define a VoIP domain, as follows:

**Table 10-19** VoIP Domains for External Gatekeeper

<b>Name</b>	VoIP_Domain
<b>Related endpoints domain</b>	Group containing Net_A and Net_B
<b>VoIP installed at</b>	GK_A

5. In the **Routing Mode** tab, define permitted routing modes for the Gatekeeper. For an explanation of the modes, refer to “[Routing Modes](#)” on page 276. It is important to select at least one option.
6. Now define the rules. To enforce handover, define the following rule with a VoIP domain:

**Table 10-20** VoIP Handover Enforced

Source	Destination	Service	Action	Comment
Net_A	VoIP_Domain	H323_ras	Accept	Bidirectional calls.
Net_B	Net_A	H323		Handover enforced.
VoIP_Domain				

If you do not want to enforce handover, define the following rules:

**Table 10-21** VoIP Handover Not Enforced

Source	Destination	Service	Action	Comment
Net_A	GK_B	H323_ras_only	Accept	No handover.
Net_A	Net_A	H323	Accept	No handover.
Net_B	Net_B			

When rules without a VoIP domain are defined, all connections other than RAS connections must be peer to peer.

For an explanation of the H.323 services, refer to “[H.323 Services](#)” on page 277.

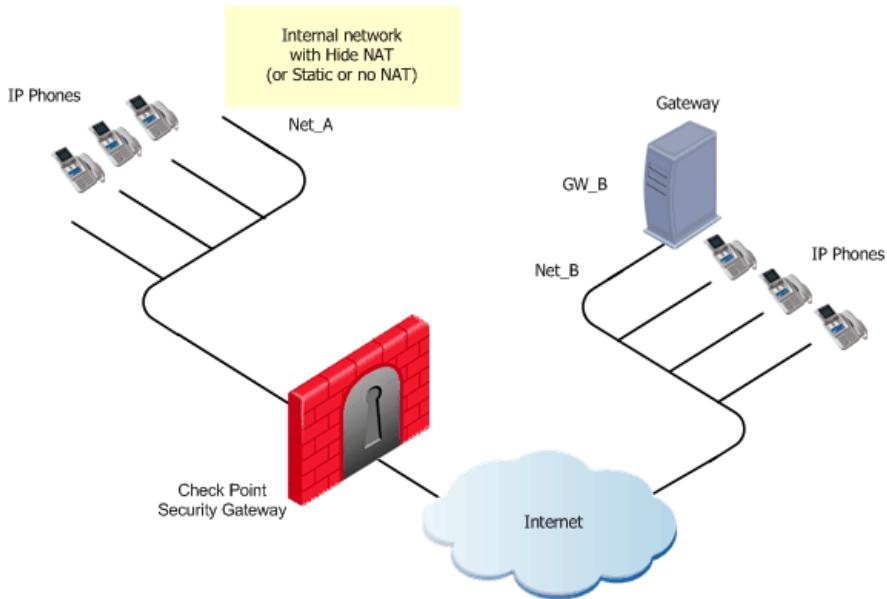
7. To define Hide NAT (or Static NAT) for the phones in the internal network:
- Edit the network object for the internal network (Net\_A). In the **NAT** tab, check **Add Automatic Address Translation Rules**, and select the **Translation method** (*Hide* or *Static*)
  - If defining Hide NAT, add a Node object with the Hide NAT IP address to the **Destination** of the rule(s) defined in step 6.

8. It is recommended to make the time-out of the `H323_ras` service greater or equal to the Gatekeeper registration time-out. Configure the time-outs in the **Advanced Properties** window of the Service object.
9. Configure the IPS options under **Application Intelligence > VoIP > H.323** as required. For details, refer to “[IPS Application Intelligence Settings for H.323](#)” on page 275, or the online help.
10. Install the security policy: **Policy > Install**.

## ***H.323 Rules for a Gateway in the External Network***

An H.323 topology with a Gateway in the Internet is shown in [Figure 10-19](#), with Net\_A and Net\_B on opposite sides of the Security Gateway. The following procedure explains how to allow bidirectional calls between the phones in the internal network (Net\_A) and phones in an external network (Net\_B), and how to define NAT for the internal phones.

**Figure 10-19** H.323 Topology: Gateway In External Network



To define an H.323 rule for a gateway in the external network:

1. Define the network objects (Nodes or Networks) for the phones that are allowed to make calls, and whose calls are tracked by the Security Gateway.  
For the example in [Figure 10-19](#), these are Net\_A and Net\_B.
2. Define the network object for the Gateway (GW\_B)

3. Define Security Rule Base rules with a VoIP domain to enforce handover. Right-click the Network Objects tree, and select **New... > VoIP Domains > VoIP Domain H.323 Gateway**. Define a VoIP domain, as follows:

**Table 10-22** VoIP Domains for External Gateway

<b>Name</b>	VoIP_Domain
<b>Related endpoints domain</b>	Group containing Net_A and Net_B
<b>VoIP installed at</b>	GW_B

4. In the **Routing Mode** tab, define permitted routing modes for the Gateway. For an explanation of the modes, refer to "["Routing Modes" on page 276](#)". It is important to select at least one option.
5. Now define the rules. To enforce handover, define the following rule with a VoIP domain:

**Table 10-23** VoIP Handover Enforced

Source	Destination	Service	Action	Comment
Net_A	VoIP_Domain	H323	Accept	Bidirectional calls.
Net_B	Net_A			Handover enforced.
VoIP_Domain				

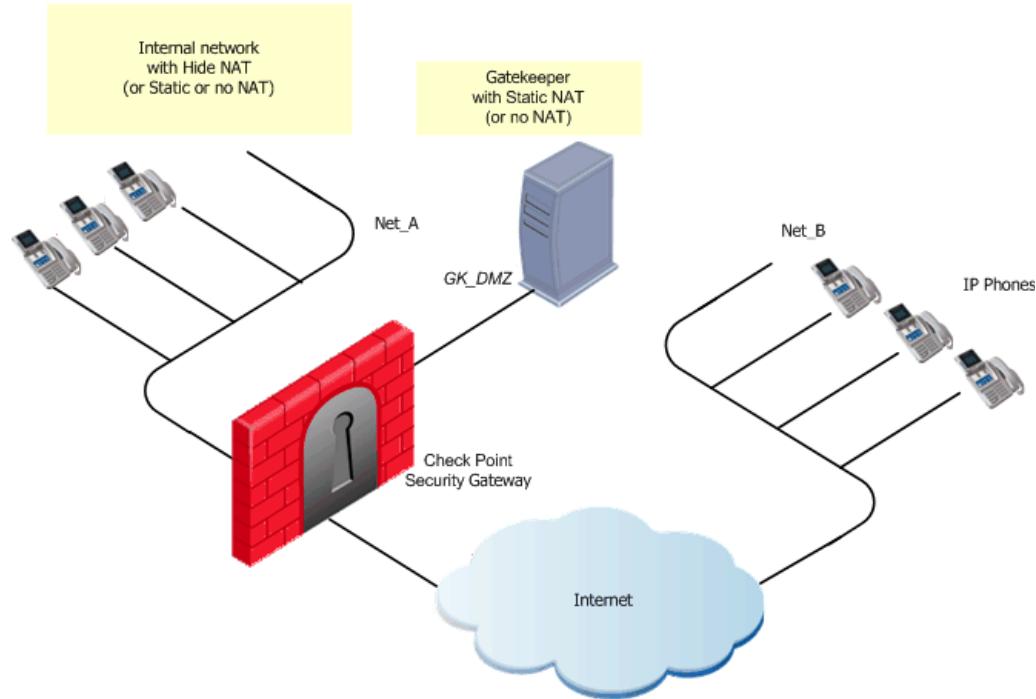
For an explanation of the H.323 services, refer to "["H.323 Services" on page 277](#)".

6. To define Hide NAT (or Static NAT) for the phones in the internal network:
  - Edit the network object for the internal network (Net\_A). In the **NAT** tab, select **Add Automatic Address Translation Rules**, and select the **Translation method** (Hide or Static).
  - If using Hide NAT, you must add a Node object with the Hide NAT IP address to the **Destination** of the rule(s) defined in step 5.
7. Configure the IPS options under **Application Intelligence > VoIP > H.323** as required. For details, refer to "["IPS Application Intelligence Settings for H.323" on page 275](#)", or the online help.
8. Install the security policy: **Policy > Install**.

## H.323 Rules for a Gatekeeper in DMZ Topology

A H.323-based VoIP topology where a Gatekeeper is installed in the DMZ is shown in [Figure 10-20](#). The following procedure explains how to allow bidirectional calls between the phones in the internal network (Net\_A) and phones in an external network (Net\_B), and how to define NAT for the internal phones and the Gatekeeper in the DMZ (GK\_DMZ).

**Figure 10-20** H.323 Topology: Gatekeeper in the DMZ



To define an H.323 rule for a gatekeeper in the DMZ:

1. Define the network objects (Nodes or Networks) for the phones which use the Gatekeeper for registration, and that are allowed to make calls, and whose calls are tracked by the Security Gateway.

For the example in [Figure 10-20](#), these are Net\_A and Net\_B.

2. Define the network object for the Gatekeeper (GK\_DMZ).
3. Define Security Rule Base rules either with or without a VoIP domain.

To enforce handover, define VoIP domains. Right-click the Network Objects tree, and select **New > VoIP Domains > VoIP Domain H.323 Gatekeeper**.

The definition of the VoIP domain depends on whether or not you want to enforce handover locations for phones in the external network. For phones in the internal network, handover should always be enforced.

**Table 10-24** VoIP Domains for Gatekeeper in DMZ

VoIP Domain Definition	With Handover	No Handover for External Phones
Name	VoIP_Domain	VoIP_Domain_A
Related endpoints domain	Group containing Net_A and Net_B	Net_A
VoIP installed at	GK_DMZ	GK_DMZ

4. In the **Routing Mode** tab, define permitted routing modes for the Gatekeeper. For an explanation of the modes, refer to “[Routing Modes](#)” on page 276. It is important to select at least one option.
5. Now define the rules. For full handover enforcement, define the following rule:

**Table 10-25** VoIP Handover Enforced

Source	Destination	Service	Action	Comment
VoIP_Domain	Net_A	H323_ras	Accept	Bidirectional calls. Handover enforced.
Net_A	Net_B			
Net_B	VoIP_Domain			

If you do not want to enforce handover for the external phones (in Net\_B), define the following rules:

**Table 10-26** VoIP Handover Not Enforced

Source	Destination	Service	Action	Comment
Net_A, Net_B, GK_DMZ	Net_A, Net_B, GK_DMZ	H323_ras_only	Accept	Outgoing calls. No handover enforced.
Net_A Net_B	Net_A Net_B	H323	Accept	No Handover enforced.

When rules without a VoIP domain are defined, all connections other than H323\_ras are only allowed to be peer to peer.

For an explanation of the H.323 services, refer to “[H.323 Services](#)” on page 277.

6. To define Hide NAT (or Static NAT) for the phones in the internal network:
  - Edit the network object for Net\_A. In the **NAT** tab, select **Add Automatic Address Translation Rules**, and select the **Translation method** (Hide or Static).
  - If using Hide NAT, you must select the **Hide behind IP address** option, and type the IP address of the Hiding address of the phones in the internal network.
  - If using Hide NAT, you must add a Node object with the Hide NAT IP address to the **Destination** of the rule(s) defined in [step 5](#).
7. To define Static NAT for the Gatekeeper in the DMZ, add manual NAT rules, as follows:
  - Create a Node object for the Static address of the Gatekeeper (for example: GK\_DMZ\_NATed).
  - Define the following manual NAT rules:

**Table 10-27** Manual NAT

Original			Translated			Comment
Source	Destination	Service	Source	Destination	Service	
GK_DMZ	Net_B	*Any	GK_DMZ: Static	=	=	Outgoing calls
Net_B	GK_DMZ_N ATed	*Any	=	GK_DMZ: Static	=	Incoming calls

- As for all manual NAT rules, configure proxy-ARPs. In other words, you must associate the translated IP address with the MAC address of the Check Point Gateway interface that is on the same network as the translated addresses. Use the `arp` command in Unix or the `local.arp` file in Windows.

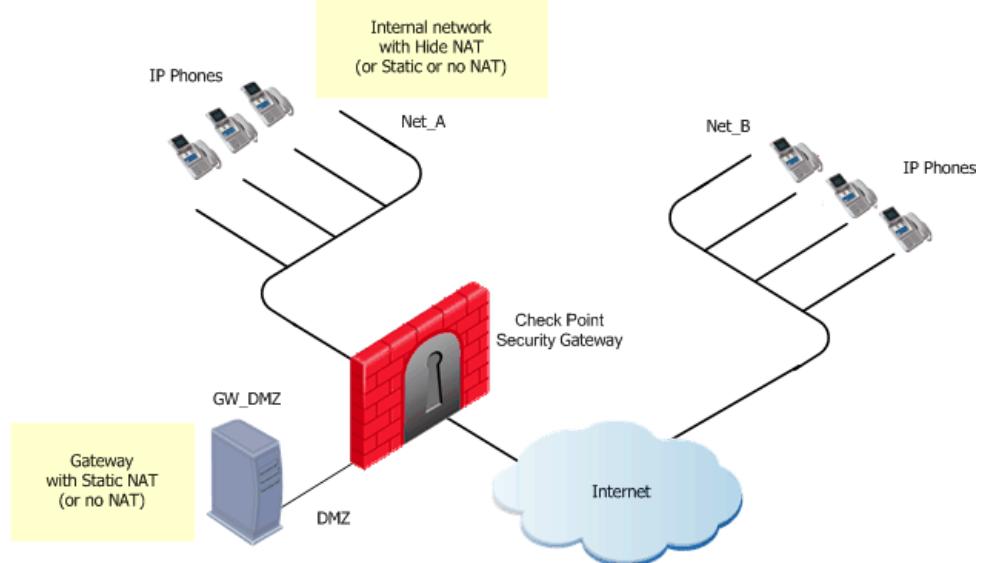
The command `fw ctl arp` displays the ARP proxy table on Security Gateways that run on Windows. On Unix, use the `arp -a` command.

8. It is recommended to make the time-out of the `H.323_ras` service greater than or equal to the Gatekeeper registration time-out. Configure the time-outs in the **Advanced Properties** window of the Service object.
9. Configure the IPS options under **Application Intelligence > VoIP > H.323** as required. For details, refer to [“IPS Application Intelligence Settings for H.323” on page 275](#), or the online help.
10. Install the security policy: **Policy > Install**.

## H.323 Rules for a Gateway in DMZ Topology

A H.323-based VoIP topology where a Gateway is installed in the DMZ is shown in [Figure 10-21](#). The following procedure explains how to allow bidirectional calls between the phones in the internal network (Net\_A) and phones in an external network (Net\_B), and how to define NAT for the internal phones and the Gateway in the DMZ (GK\_DMZ).

**Figure 10-21** H.323 Topology: Gateway in the DMZ



To define an H.323 rule for a gateway in the DMZ:

1. Define the network objects (Nodes or Networks) for the phones that are allowed to make calls, and whose calls are tracked by the Security Gateway.  
For the example in [Figure 10-21](#), these are Net\_A and Net\_B.
2. Define the network object for the Gateway (GW\_DMZ).
3. Define Security Rule Base rules with or without a VoIP domain to enforce handover. Right-click the Network Objects tree, and select **New > VoIP Domains > VoIP Domain H.323 Gateway**.

**Table 10-28** H.323 Gateway in DMZ

VoIP Domain Definition	With Handover
Name	VoIP_Domain
Related endpoints domain	Group containing Net_A and Net_B
VoIP installed at	GK_DMZ

4. In the **Routing Mode** tab, define permitted routing modes for the Gateway. For an explanation of the modes, refer to “[Routing Modes](#)” on page 276. It is important to select at least one option.
5. Now define the rules for full handover enforcement:

**Table 10-29** VoIP Handover Enforced

Source	Destination	Service	Action	Comment
VoIP_Domain	Net_A	H323	Accept	Bidirectional calls.
Net_A	Net_B			Handover enforced.
Net_B	VoIP_Domain			

For an explanation of the H.323 services, refer to “[H.323 Services](#)” on page 277.

6. To define Hide NAT (or Static NAT) for the phones in the internal network:
  - Edit the network object for Net\_A. In the **NAT** tab, check **Add Automatic Address Translation Rules**, and select the **Translation method** (*Hide* or *Static*).
  - If using Hide NAT, you must select the **Hide behind IP address** option, and type the IP address of the Hiding address of the phones in the internal network.
  - If using Hide NAT, you must add a Node object with the Hide NAT IP address to the **Destination** of the rule(s) defined in step 5.
7. To define Static NAT for the Gateway in the DMZ, add manual NAT rules, as follows:
  - Create a Node object for the Static address of the Gateway (for example: GW\_DMZ\_NATed).
  - Define the following manual NAT rules:

**Table 10-30** Manual NAT

Original			Translated			Comment
Source	Destination	Service	Source	Destination	Service	
GW_DMZ	Net_B	*Any	GW_DMZ: Static	=	=	Outgoing calls
Net_B	GW_DMZ_NATed	*Any	=	GW_DMZ: Static	=	Incoming calls

- As for all manual NAT rules, configure proxy-arps. In other words, you must associate the translated IP address with the MAC address of the Check Point Gateway interface that is on the same network as the translated addresses. Use the arp command in Unix or the local.arp file in Windows.  
The command fw ctl arp displays the ARP proxy table on Security Gateways that run on Windows. On Unix, use the arp -a command.
8. Configure the IPS options under **Application Intelligence > VoIP > H.323** as required. For details, refer to "[IPS Application Intelligence Settings for H.323 on page 275](#), or the online help.
  9. Install the security policy: **Policy > Install**.

# Securing MGCP-Based VoIP

The Need for MGCP	page 294
MGCP Protocol and Devices	page 294
MGCP Network Security and Application Intelligence	page 296
Secured MGCP Topologies and NAT Support	page 298
Synchronizing User Information	page 299
Configuring MGCP-Based VoIP	page 300



**Note** - Before reading this section, read “Introduction to the Check Point Solution for Secure VoIP” on page 243 to “Protocol-Specific Security” on page 252.

The MGCP protocol is described in this section only to the extent required to secure MGCP traffic using Check Point Security Gateway.

## ***The Need for MGCP***

Regular phones are relatively inexpensive because they do not 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***

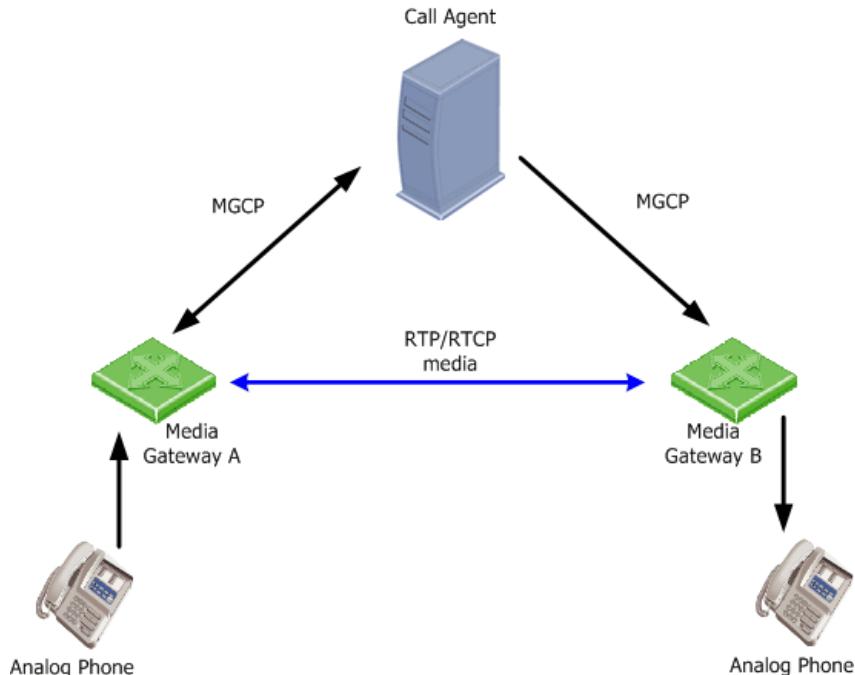
MGCP is a protocol for controlling telephony gateways from external call control devices called *Call Agents* (also known as *Media Gateway Controllers*).

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 10-22](#) shows the MGCP elements and a simplified call control process.

**Figure 10-22** MGCP Elements



The Call Agent and Media Gateways are defined in SmartDashboard, usually as Node objects.

To allow MGCP conversations you need only create rules to allow the MGCP control signals through the Security Gateway. There is no need to define a rule for the media that specifies which ports to open and which endpoints will talk. Check Point Security Gateway derives this information from the signalling. Given a particular VoIP signalling rule, the firewall 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 Check Point Security Gateway MGCP services (MGCP-CA and MGCP-MG).

## **MGCP IP Phones**

An MGCP IP Phone is a network device that:

- Provides conversion between the audio signals carried over the Internet or over other packet networks.
- Sends notification to the call agent about its events.
- Executes commands from the call agents.

MCGP IP Phones normally support features such as conference calls, three-way brokering, and supervisor inspection. All of these features are supported by the predefined Check Point Security Gateway MGCP services (MGCP-CA and MGCP-MG).

## ***MGCP Network Security and Application Intelligence***

Check Point Security Gateway provides full network level security for MGCP. The Security Gateway enforces strict compliance with RFC-2705, RFC-3435 (version 1.0), and ITU TGCP specification J.171. In addition, all Check Point capabilities are supported, such as inspection of fragmented packets, anti-spoofing, and protection against DoS attacks.

Check Point Security Gateway restricts handover locations and controls signalling and data connections, as described in “[VoIP Application Intelligence](#)” on [page 247](#).

IPS can perform additional content security checks for MGCP connections, thereby providing a greater level of protection. MGCP-specific Application Intelligence security is configured via IPS, 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 predefined MGCP commands. Some commands are made by the Call Agent, and others by the Gateway, as shown in [Table 10-31](#). It is possible to allow or disallow any command as dictated by the security needs.

**Table 10-31** MGCP commands

Call Agent Commands	Gateway Commands
EndpointConfiguration (EPCF)	Notify (NTFY)
NotificationRequest (RQNT)	DeleteConnection (DLXC)
CreateConnection (CRCX)	RestartInProgress (RSIP)
ModifyConnection (MDCX)	
DeleteConnection (DLCX)	
AuditEndpoint (AUEP)	
AuditConnection (AUCX)	

In addition, it is possible to define additional proprietary commands, as well as whether to allow or block those commands. By default, all undefined commands are blocked.

The firewall 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. The firewall knows how to parse the header and check it has the correct syntax. If the destination address and port in the header are allowed, The firewall 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 a 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.

## **Secured MGCP Topologies and NAT Support**

Check Point Security Gateway supports the MGCP deployments listed in [Table 10-1](#). It is possible to configure NAT (either Hide or Static) for the phones in the internal network.

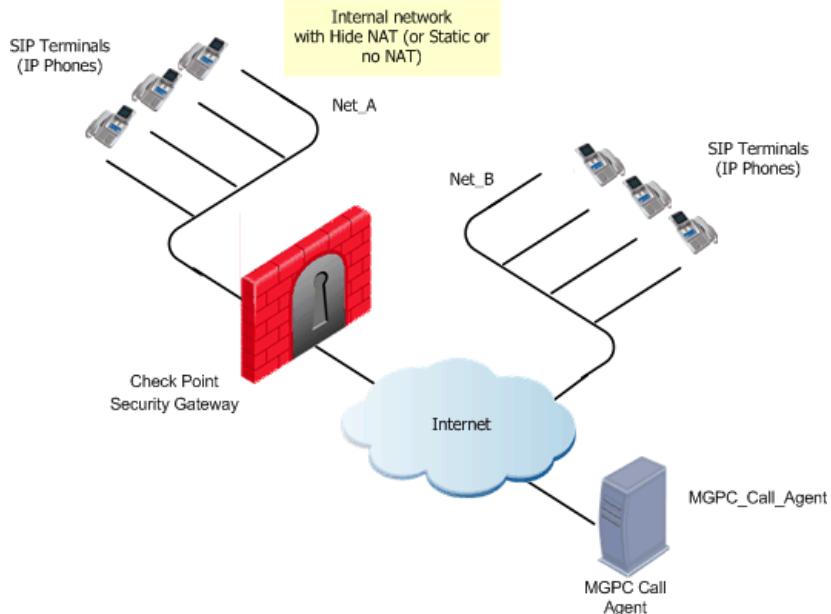
**Table 10-32** Supported MGCP Topologies

	No NAT	NAT for Phones - Hide/Static NAT	NAT for the Call Agent - Static NAT
Peer-to-Peer ( <a href="#">Figure 10-4</a> )	Yes	Yes	Not applicable
Proxy in External ( <a href="#">Figure 10-5</a> )	Yes	Yes	Not applicable

The “Call Agent” is any MGCP handover device.

Where there is one or more handover devices, the signalling passes through one or more Call Agents. Once the call has been set up, the media can pass peer to peer.

The SmartDashboard configuration depends on the topology, as described in [“Configuring MGCP-Based VoIP” on page 300](#) which includes diagrams showing the most widely used deployment topologies.

**Figure 10-23** MGCP Call Agent in Internet with NAT for Internal phones

## ***Additional Conditions for Using NAT in MGCP Networks***

MGCP can be used with Network Address Translation (NAT), subject to the following conditions:

- Hide NAT can be used for all types of calls (incoming, outgoing, internal and external). 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 Security Gateway, 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.
- Bidirectional NAT of VoIP calls is not supported.

## ***Synchronizing User Information***

The user IP Phone sends MGCP messages to the Call Agent in order to register itself on the network. Once a phone is registered, it can make calls. These MGCP messages cross the firewall, and are then stored in the user database.

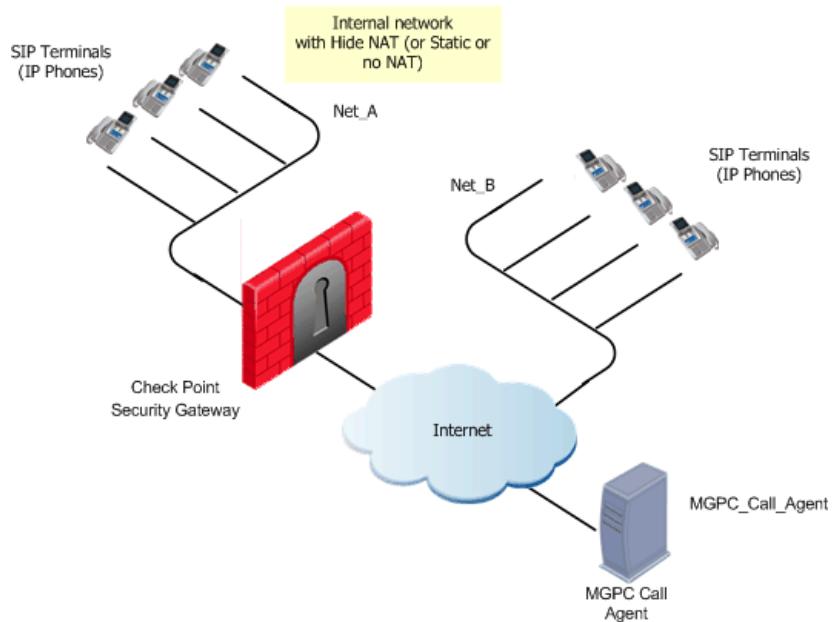
Registration makes it possible to initiate calls from outside the Security Gateway to phones whose addresses are translated using Hide NAT.

If the Check Point Security Gateway machine is rebooted, the VoIP user database is deleted. The `cpstop/cpstart` commands do not delete the user database.

## ***Configuring MGCP-Based VoIP***

An MGCP topology with a Call Agent in the external network is shown in [Figure 10-7](#). The following procedure explains how to allow bidirectional calls between the MGCP phones in the internal network (Net\_A) and phones in an external network (Net\_B), and how to define NAT for the internal phones.

**Figure 10-24** MGCP Call Agent in External Network



To define an MGCP rule for a call agent in the external network:

1. Define the network objects (Nodes or Networks) for the IP Phones that are managed by the Handover device (MGCP Call Agent) and are allowed to make calls, and whose calls are tracked by the Security Gateway. For the example in [Figure 10-24](#), these are Net\_A and Net\_B.
2. Define the network object for the Handover device (MGCP\_Call\_Agent).
3. Define the VoIP domain object. If the Call Agent (MGCP\_Call\_Agent) is on one machine with a single IP address, define only one VoIP domain. If there are different IP addresses, define a VoIP domain for each IP address.

Right-click the Network Objects tree, and select **New... > VoIP Domains > VoIP Domain MGCP Call Agent**.

**Table 10-33** VoIP Domains with MGCP Call Agent

VoIP Domain Definition	With Handover
Name	VoIP_Domain
Related endpoints domain	Group containing Net_A and Net_B
VoIP Gateway installed at	MGCP_Call_Agent

4. Now define the rules. With full handover enforcement, define the following rule:

**Table 10-34** VoIP Handover Enforced

Source	Destination	Service	Action
VoIP_Domain Net_A	Net_A VoIP_Domain	mgcp_CA or mgcp_MG or mgcp_dynamic_ports	Accept

The services are:

- **mgcp\_CA** is Call Agent service. It uses port 2727.
- **mgcp\_MG** is the Media Gateway service. It uses port 2427.
- **mgcp\_dynamic\_ports** - is the MGCP service and uses ports that are not predefined. For example, ports that were identified in the NotifiedEntity field in previous MGCP packets.

5. To define Hide NAT (or Static NAT) for the phones in the internal network, edit the network object for Net\_A. In the **NAT** tab, check **Add Automatic Address Translation Rules**, and select the **Translation method** (*Hide* or *Static*)
6. Configure IPS options under **Application Intelligence > VoIP > MGCP** as required.
7. Install the security policy: **Policy > Install**.

# Securing SCCP-Based VoIP



**Note** - Before reading this section, read “[Introduction to the Check Point Solution for Secure VoIP](#)” on page 243 to “[Protocol-Specific Security](#)” on page 252.

The SCCP protocol is described in this section only to the extent required to secure SCCP traffic using Check Point Security Gateway.

## In This Section

<a href="#">The SCCP Protocol</a>	page 302
<a href="#">SCCP Devices</a>	page 302
<a href="#">SCCP Network Security and Application Intelligence</a>	page 303
<a href="#">ClusterXL Support for SCCP</a>	page 304
<a href="#">Configuring SCCP-Based VoIP</a>	page 304

## ***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 information, such as the button template and the date/time, to the VoIP endpoints.

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 Security Gateway. There is no need to define a rule for the media that specifies which ports to open and which endpoints will talk. Check Point Security Gateway derives this information from the signalling. Given a particular VoIP signalling rule, the firewall automatically opens ports for the endpoint-to-endpoint RTP/RTCP media stream.

## ***SCCP Network Security and Application Intelligence***

Check Point Security Gateway 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 Check Point capabilities are supported, such as anti-spoofing and protection against DoS attacks. Fragmented packets are examined and secured using kernel-based streaming. However, NAT on SCCP devices is not supported.

Check Point Security Gateway restricts handover locations, and controls signalling and data connections, as described in “[VoIP Application Intelligence](#)” on [page 247](#).

The Security Gateway 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.

IPS 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** blocks various potentially dangerous control characters, and the null character.
- **Block Multicast RTP Connections** blocks SCCP multicasts. 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.

## ***ClusterXL Support for SCCP***

SCCP calls can be made across a ClusterXL Gateway cluster. However, calls do not survive failover if the failover occurs while the call is being set up.

## ***Configuring SCCP-Based VoIP***

To configure SCCP-Based VoIP:

1. Configure the IPS 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**, select the Group object defined in [step 3](#). For the **VoIP installed at** option, select 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.

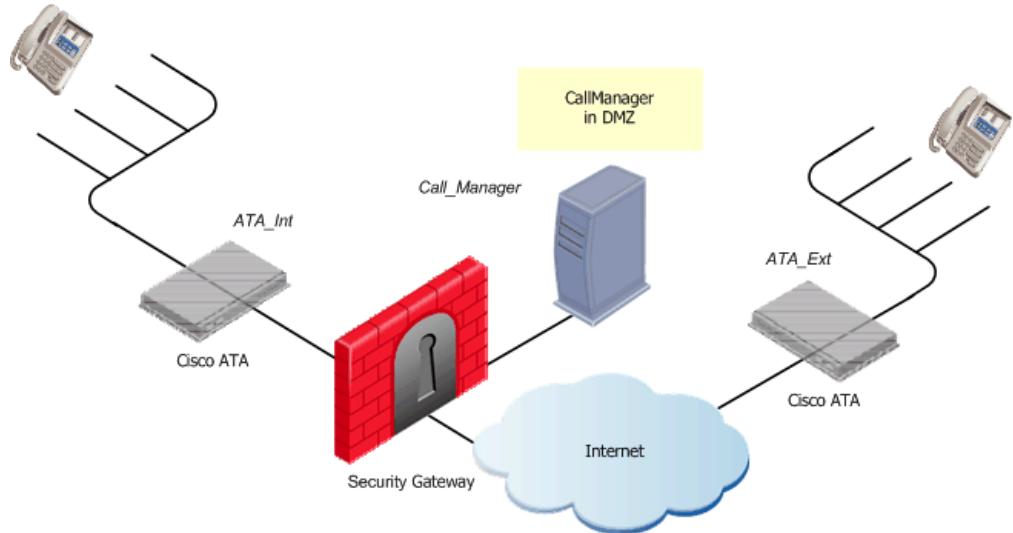
The rules depend on the network topology. For details, refer to the following sections:

- “[SCCP Rules for a CallManager in the DMZ](#)” on page 305.
  - “[SCCP Rules for a CallManager in the Internal Network](#)” on page 306.
  - “[SCCP Rules for a CallManager in an External Network](#)” on page 307.
7. Install the security policy: **Policy > Install**.

## SCCP Rules for a CallManager in the DMZ

In a DMZ topology shown in [Figure 10-25](#), 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 Security Gateway.

**Figure 10-25** SCCP CallManager in the DMZ



The rules in [Table 10-35](#) allows any telephone managed by ATA\_Int and ATA\_Ext to make calls to each other.

**Table 10-35** SCCP rules for a CallManager in the DMZ

Source	Destination	Service	Action
ATA_Int ATA_Ext	VoIP_Call_Manager	SCCP	Accept
VoIP_Call_Manager	ATA_Int ATA_Ext	SCCP	Accept

VoIP\_Call\_Manager is the VoIP domain object with endpoint domain that includes both ATA\_Int and ATA\_Ext.

To create the VoIP domain object:

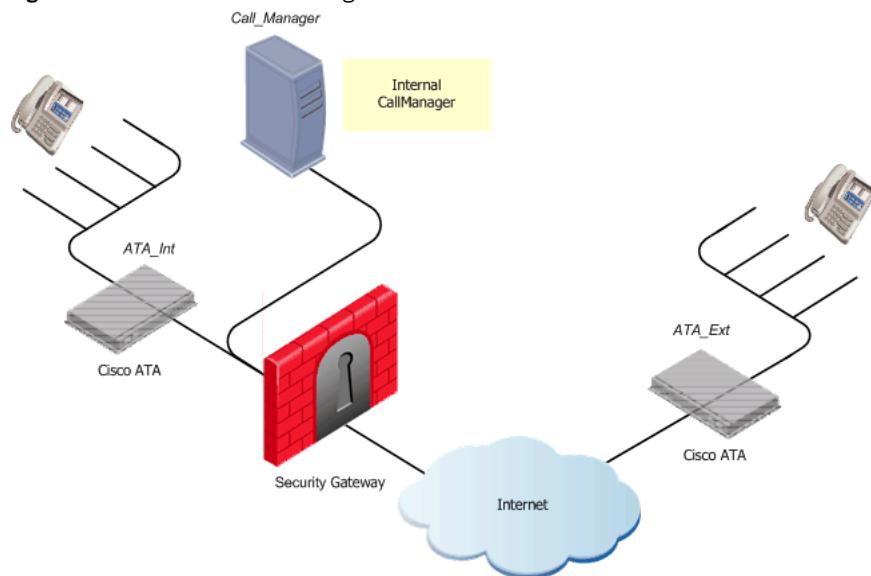
1. In SmartDashboard, select **Manage > Network Objects**.
2. Click **New > Group > Simple Group**.
3. In the Group Properties window, add the Cisco ATA devices or the IP Phone objects and give the group a name.

4. Click **OK**.
5. In the Network Objects window, click **New > VoIP Domains > VoIP Domain SCCP CallManager**.
6. Give the Call Manager object a name.
7. In **Related endpoints domain** select the group of phone devices that you created earlier.
8. In **VoIP installed at** select the CallManager object (or click **New** and define it).

### SCCP Rules for a CallManager in the Internal Network

In the topology shown in [Figure 10-26](#), 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 10-26** SCCP CallManager in an Internal Network



The rules in [Table 10-36](#) allow any telephone managed by ATA\_Int and ATA\_Ext to make calls to each other. Each rule allows calls in one direction.

**Table 10-36** SCCP Rules for a CallManager in the internal Network

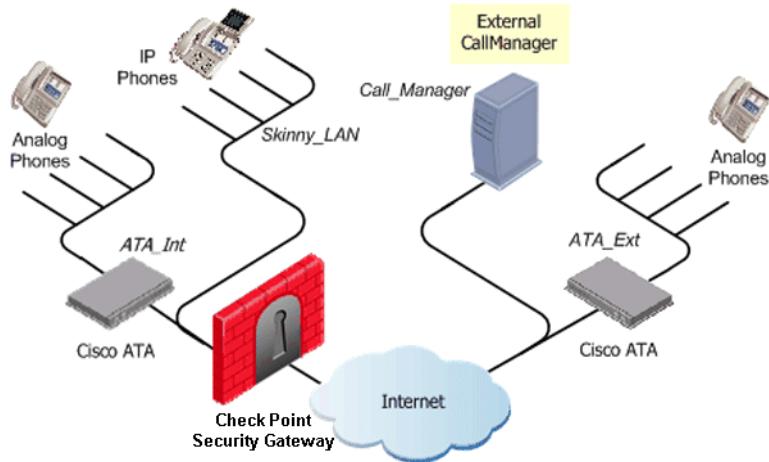
Source	Destination	Service	Action	Comment
VoIP_Call_Manager	ATA_Ext	SCCP	Accept	Outgoing calls
ATA_Ext	VoIP_Call_Manager	SCCP	Accept	Incoming calls

VoIP\_Call\_Manager is the VoIP domain object with an endpoint domain that includes both ATA\_Int and ATA\_Ext. Create the VoIP domain object as shown in [Figure 10-26 on page 306](#). 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 10-27](#), 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 10-27** SCCP CallManager in an External Network



The first rule in [Table 10-37](#) 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 Security Gateway object **Topology** page, the interface that faces the Internet is defined as *External*.

**Table 10-37** SCCP rules for a CallManager in the internal network

Source	Destination	Service	Action	Comment
ATA_Int Skinny_LAN	Call_Manager	SCCP	Accept	Outgoing calls
Call_Manager	ATA_Int Skinny_LAN	SCCP	Accept	Incoming calls

## Allowing Internal Calls with External CallManager

If the CallManager is in an external network, and you want to allow internal calls between phones managed by different Cisco ATA devices or IP Phones behind the same interface of the Security Gateway, you must define a VoIP domain. This configuration is illustrated in [Figure 10-27 on page 307](#). The rules in [Table 10-38](#) allow calls between ATA\_Int and the IP Phones in Skinny\_LAN.

**Table 10-38** SCCP rules for a CallManager in the internal network

Source	Destination	Service	Action	Comment
ATA_Int Skinny_LAN	VoIP_Call_Manager	SCCP	Accept	Outgoing calls
VoIP_Call_Manager	ATA_Int Skinny_LAN	SCCP	Accept	Incoming calls

VoIP\_Call\_Manager is the VoIP domain object with an endpoint domain that includes both ATA\_Int and Skinny\_LAN. Create the VoIP domain object as shown in [Figure 10-26 on page 306](#). 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.

# Chapter

# Securing Instant Messaging Applications

## In This Chapter

The Need to Secure Instant Messenger Applications	page 310
Introduction to Instant Messenger Security	page 311
Understanding Instant Messenger Security	page 312
NAT Support for MSN Messenger over SIP	page 313
NAT Support for MSN Messenger over MSNMS	page 314
Logging Instant Messenger Applications	page 314
Configuring SIP-based Instant Messengers	page 315
Configuring MSN Messenger over MSNMS	page 317
Configuring Skype, Yahoo, ICQ and More	page 318

# The Need to Secure Instant Messenger Applications

Common Instant Messenger capabilities include 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 Instant Messenger 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 service and reduce MIS costs. However, it can also be used by hackers to take control of a remote computer.

Instant Messaging protocols themselves have vulnerabilities that can be exploited to cause a Denial of Service attack. For example, passing an overly long user name and password for authorization for some applications may cause a buffer overflow that could bring down the Instant Messenger server.

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 they are used in the enterprise.

# Introduction to Instant Messenger Security

Instant Messenger applications allow communication and collaboration between users employing various communication modes, such as Instant Messaging, Voice and Video, Application Sharing, White board, File Transfer, and Remote Assistance.

Firewall and IPS provide powerful and flexible security for Instant Messengers. MSN Messenger in particular, both in its SIP mode of operation, and using the native MSNMS protocol, can be secured with an extra level of granularity.

It is possible to selectively block audio, video or other selected capabilities of MSN Messenger. In addition, the audio and video streams of any SIP-based Instant Messaging application can be blocked. The Security Rule Base can be used to allow communication to and from specified locations.

Firewall and IPS secure 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 Messenger Security

To understand the principles of securing SIP-based Instant Messenger communication, refer to [Chapter 10, “Securing Voice Over IP”](#): “Introduction to the Check Point Solution for Secure VoIP” on page 243 to “Securing SIP-Based VoIP” on page 252 (inclusive).

The firewall dynamically opens ports for the services used by Instant Messenger applications. It keeps those ports open only for as long as required, and closes them as soon as the call ends, without waiting for a time-out. The order and direction of the packets is also enforced.

For detailed information about MSN Messenger and the protocols it uses, visit the following Microsoft Web pages:

- <http://www.microsoft.com/technet/prodtechnol/winxppro/evaluate/insid01.mspx>
- <http://www.microsoft.com/technet/prodtechnol/winxppro/plan/rtcprot.mspx>  
(recommended for technical reference)

Some peer-to-peer applications also have Instant Messenger capabilities, which can be blocked or allowed. For details, see the HTML pages and online help for the IPS **Application Intelligence > Peer to Peer** category.

# NAT Support for MSN Messenger over SIP

The firewall and IPS 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 other MSN Messenger applications, some Hide NAT operations are not supported due to the inconsistent behavior of MSN Messenger. [Table 11-1](#) shows how Hide NAT can be used with SIP-based MSN Messenger applications.

**Table 11-1** Support for Hide NAT with SIP-Based MSN Messenger Capabilities

Hide NAT	Instant Messaging	Application Sharing and Whiteboard	File Transfer and Remote Assistance	Audio	Video and Audio
Internal → External (outbound traffic)	Yes	Yes	No	Yes	No
External → Internal (inbound traffic)	Yes	No	Yes	Yes	No
Internal → Internal (internal traffic)	Yes	Yes	Yes	Yes	Yes

# NAT Support for MSN Messenger over MSNMS

For MSN Messenger over MSNMS, Static and Hide Network Address Translation (NAT) are supported for the Instant Messenger and File Transfer applications.

## Logging Instant Messenger Applications

SmartView Tracker provides detailed protocol-specific logs for Instant Messenger conversations. The following events are logged.

**Table 11-2** Logged MSN Messenger over SIP Events in SmartView Tracker

Event or Application	SmartView Tracker Field name	Value
Call registration	registered IP-phones	SIP address
Instant message	media type	instant messaging
Audio	media type	Audio
Video	media type	Video
Application sharing and Whiteboard (MSN Messenger only)	media type	Application
File transfer (MSN Messenger only)	media type	File_Transfer
Remote Assistant (MSN Messenger only)	media type	Remote_Assistance

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 show the port numbers used.

# Configuring SIP-based Instant Messengers

The firewall and IPS components make it possible to block or to allow all SIP-based Instant Messenger applications. For MSN Messenger over SIP, additional granular control is possible.



**Note** - To understand how to configure SmartDashboard for a SIP Proxy topology, it is recommended to first read “[Configuring SIP-Based VoIP](#)” on page 261.

To completely block MSN Messenger over SIP and other SIP-based Instant Messenger applications, including the core instant messaging capabilities, do not allow the **SIP** service in the Security Rule Base.

To selectively block SIP-based Instant Messenger applications (while allowing the core instant Messaging capabilities):

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 11-3](#) includes all the relevant services, and allows calls in both directions.

**Table 11-3** Example rule allowing SIP-based Instant Messengers

Source	Destination	Service	Action	Action
allowed_phones SIP_domain	SIP_domain allowed_phones	sip sip_dynamic_ports T.120 MSN_Messenger_File_Transfer	Accept	Log

The relevant services are:

- **sip** allows the use of a proxy server and enforces handover via a VoIP Domain. See “[SIP Services](#)” on page 259.
- **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.

4. If required, configure Static and/or Hide NAT for MSN Messenger, taking into account the limitations described in “[NAT Support for MSN Messenger over SIP](#)” on page 313.
5. Configure the IPS SIP options in the following protections:
  - **Application Intelligence > VoIP > SIP Filtering**
  - **Application Intelligence > VoIP > SIP Protections**
  - **Application Intelligence > VoIP > SIP Custom Properties**
  - **Application Intelligence > Instant Messengers > MSN Messenger over SIP**

# Configuring MSN Messenger over MSNMS

To completely block MSN Messenger over MSNMS, including its core instant messaging capabilities, do not allow the MSNMS service in the Security Rule Base.

To selectively block MSNMS-based Instant Messenger applications (while allowing its core instant messaging capabilities), define the rules and select settings for IPS MSN Messenger protections.

1. Define a Security Rule Base rule that allows the following services:
  - MSNMS, DNS (group), Microsoft-ds, https.
  - To allow MSN Messenger games, also allow http.
2. If required, configure Static and/or hide NAT for MSN Messenger, taking into account the limitations described in “[NAT Support for MSN Messenger over MSNMS](#)” on page 314.
3. On the IPS tab > Protections, define the settings for:
  - **MSN Messenger - Chat**
  - **MSN Messenger - Files**
  - **MSN Messenger - Application**
  - **MSN Messenger - General Settings**
4. To block MSN messenger communication that uses HTTP, open the **IPS > By Protocol > HTTP Protocol Inspection > Header Rejection** protection. In the Protection Settings window, select all headers from the list that contain **Msn Messenger** and **MSN Web Messenger**.

## Configuring Skype, Yahoo, ICQ and More

- To allow Skype, Yahoo and ICQ and other Instant Messenger applications, follow the instructions provided by the application vendors.
- To block Skype, Yahoo! Messenger and ICQ, configure the IPS options under **Application Intelligence > Instant Messengers**.
- Some peer-to-peer applications also have instant messaging capabilities. Block or allow peer-to-peer applications using the options in **Application Intelligence > Peer to Peer**.

## Chapter

# Microsoft Networking Services Security

### In This Chapter

Securing Microsoft Networking Services (CIFS)	page 320
Restricting Access to Servers and Shares (CIFS Resource)	page 321

# 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. CIFS 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 is therefore an easy target for internal attacks, such as brute-force password attacks on file servers.

Check Point Security Gateway 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:

- Verifying the 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)

To restrict access to servers and shares:

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. Select **Add**, **Edit** or **Delete** to modify the list.

For example, to allow access to the disk share PAUL on the CIFS server BEATLES:

- a. Click **Add** and type BEATLES in the **Server Name** field and IPC\$ in the **Share Name** field. Click **OK**.
- b. 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.



**Warning** - Do not delete or change the protocol type of the service objects that perform content inspection. If the service is altered in this way, the protection will not work.

4. Install the security policy: **Policy > Install**.



# Chapter

# FTP Security

## In This Chapter

Introduction to FTP Content Security	page 324
FTP Enforcement by the Firewall Kernel	page 324
FTP Enforcement by the FTP Security Server	page 325
Configuring Restricted Access to Specific Directories	page 326

# Introduction to FTP Content Security

Content Security for FTP connections is provided both by the firewall kernel and the FTP Security server (the Check Point process for FTP security integrated into the firewall).

The Content Vectoring Protocol (CVP) is an API specification developed by Check Point. CVP checking can be performed on FTP traffic by redirecting the FTP traffic to a CVP server. This is configured in the FTP Resource object.

## FTP Enforcement by the Firewall Kernel

The firewall kernel enforces RFC-compliant use of the PORT commands issued by the client to ensure that no arbitrary syntax is sent. The firewall enforces additional security limitations, including:

- Proper use of the IP field in the PORT command. This verifies that an IP address presented in 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 IPS (**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 described in the following sections.

## Control Allowed Protocol Commands

Only a predefined list of FTP commands is allowed, providing full control over the character of the FTP traffic. Certain seldom-used FTP commands may compromise FTP application security and integrity, and may be blocked accordingly. These include the SITE, REST, and MACB commands, as well as 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 IPS (**Application Intelligence > FTP > FTP Security Server > Allowed FTP Commands**).

Check Point Security Gateway 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 by the FTP client or by the FTP Security server in the PORT command. This prevents the random selection of a port 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 attack 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 via the FTP Resource

FTP connections can be inspected for viruses and malicious content through integration with third-party, OPSEC-certified CVP and UFP applications. see also “[Using CVP for Virus Scanning on FTP Connections](#)” on page 337.

# 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 allows files to be downloaded from anywhere on the FTP server to the internal network.

Two resources must be created. One for upload, and another for download.

To restrict access:

1. Create an FTP Resource to allow file downloads (from **Manage > Resources**, click **New > FTP**).

In the **General** tab, name the resource (for example, Download), and select 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 (for example, Upload), and select a **Tracking Option**.

In the **Match** tab, type the allowed directory path and filename, using wildcards. For example /uploads/\*. Under **Methods**, select **PUT**.

Define one 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 resemble those listed in [Table 13-1](#).

**Table 13-1** Example Rules for FTP Upload and Download

Source	Destination	Service	Action	Track	Install On	Time	Comment
Alaska_Lan	Alaska.DMZ.ftp	ftp->Upload	Accept	Log	*Policy Targets	Any	ftp upload to /uploads/*
Alaska_Lan	Alaska.DMZ.ftp	ftp->Upload	Accept	Log	*Policy Targets	Any	ftp download from*

3. Install the security policy: **Policy > Install**.



# Chapter

# Content Security

## In This Chapter

The Need for Content Security	page 330
Check Point Solution for Content Security	page 331
Configuring Content Security	page 343
Advanced CVP Configuration: CVP Chaining and Load Sharing	page 352

# The Need for Content Security

Protecting corporate resources is a major concern for most businesses. Blocking undesirable content is an important part of a corporate security policy for a variety of reasons, including::

- 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 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.

# Check Point Solution for Content Security

## In This Section

Introduction to Content Security	page 331
Security Servers	page 332
Deploying OPSEC Servers	page 333
CVP Servers for Anti-Virus and Malicious Content Protection	page 335
Using URL Filtering to Limit Web Surfers	page 338
TCP Security Server	page 342

## Introduction to Content Security

The firewall integrates Content Security capabilities with best-of-breed, OPSEC-certified applications. OPSEC applications enable organizations to select content screening applications that best meet their needs, while managing Content Security centrally. 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 from browsing to undesirable websites, by filtering URLs.
- Provide auditing capabilities and detailed reports.

For a listing of OPSEC Content Security solutions, refer to:

[http://www.opsec.com/solutions/sec\\_content\\_security.html](http://www.opsec.com/solutions/sec_content_security.html).

Content security applications, like virus scanners, inspect the content of individual packets for specific services.

The Content Vectoring Protocol (CVP) is an API specification developed by Check Point used for integration with Anti-Virus servers. This API defines an asynchronous interface to server applications that validate file content. An important feature of CVP is scanning files for viruses or harmful applets as they pass through firewalls. CVP defines a client/server relationship that enables different Security Gateways to share a common content validation server.

The URL Filtering protocol (UFP) blocks user access to forbidden websites, allowing administrators to define undesirable or inappropriate types of websites. No configuration is required at the client machine. UFP is useful for companies that 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.

## Security Servers

Security servers are Check Point processes that are integrated into the firewall. They are user mode processes that provide content security for:

- HTTP
- FTP
- SMTP

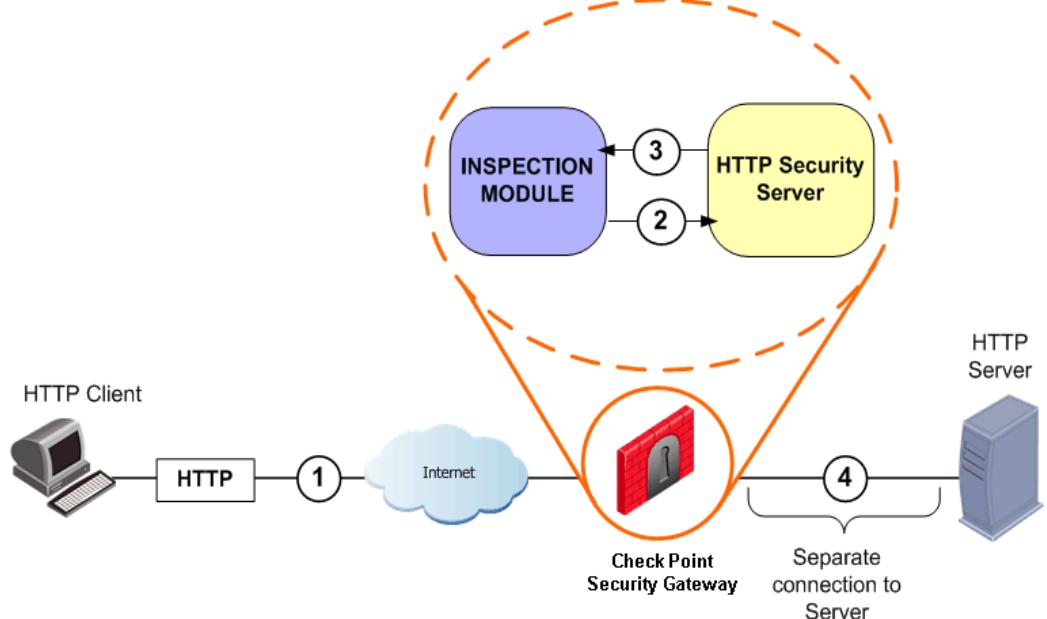
There is also a generic TCP Security server. Security servers employ many ways of enforcing Content Security, including, checking whether the connections for these protocols are well formed, stripping script tags for HTTP, email address translation for SMTP, and file name matching for FTP.

In addition to Content Security, Security servers also perform authentication. For additional information on the authentication functions of the Security servers, refer to [“Authentication” on page 59](#).

### ***How a Security Server Mediates a Connection***

[Figure 14-1](#) 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 that contains a resource, the Inspection Module on a Check Point Security Gateway diverts 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 14-1** How the Security Server Mediates a Connection

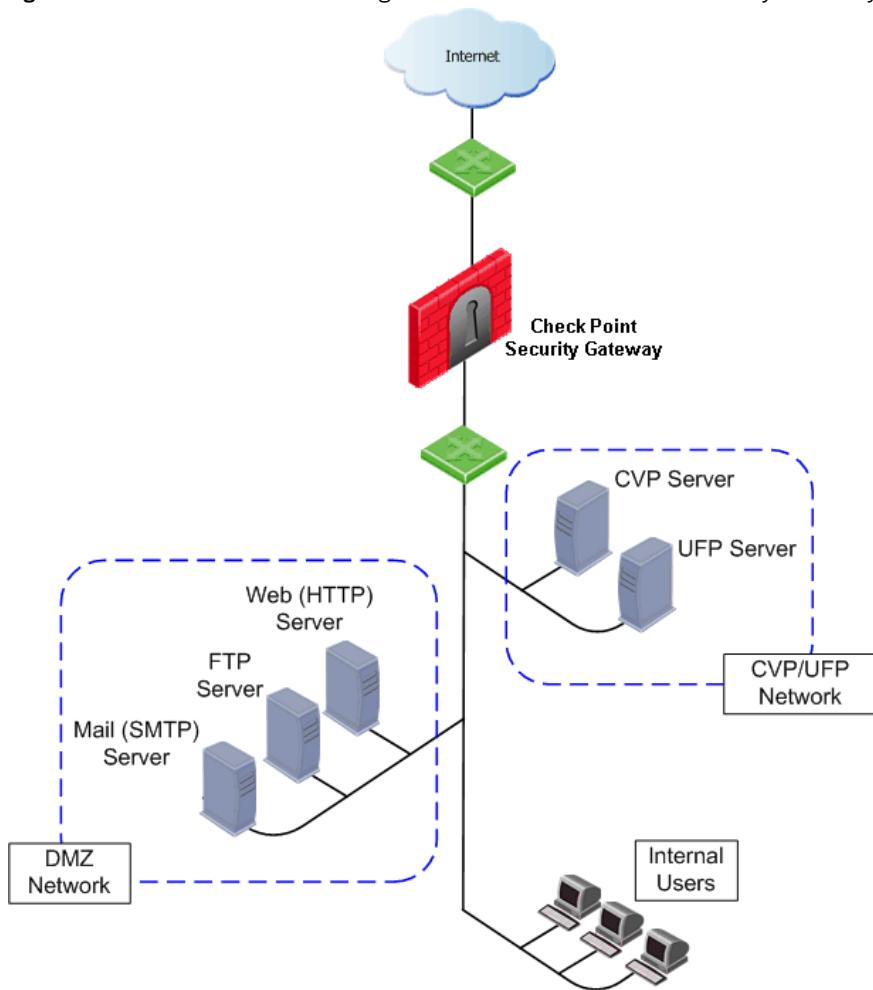
The source IP address that appears to the destination server is the IP address of the client that originally opened the connection. The connection leaves the Security server with the source IP address of the Security Gateway, and the outbound kernel performs NAT so that the source IP address is that of the original client.

## Deploying OPSEC Servers

OPSEC solutions, such as CVP and UFP servers, are deployed on dedicated servers ([Figure 14-2](#)). These servers are typically placed in the DMZ or on a private network segment. This allows fast secure connections between the CVP servers and the Security Gateway.

Performing scanning at the network perimeter is both safer and more efficient than performing the scanning at the desktop or on the application servers.

**Figure 14-2** OPSEC Server Integration with Check Point Security Gateway



# CVP Servers for Anti-Virus and Malicious Content Protection

## In This Section

<a href="#">CVP and Anti-Virus Protection for SMTP and HTTP Traffic</a>	page 335
<a href="#">How a Connection is Handled by the HTTP Security Server</a>	page 335
<a href="#">Improving CVP Performance for Web Traffic</a>	page 336
<a href="#">Using CVP for Virus Scanning on FTP Connections</a>	page 337

## ***CVP and Anti-Virus Protection for SMTP and HTTP Traffic***

To perform virus scanning, the HTTP or SMTP security server transfers packets from the Security 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 Security Gateway with the offending content removed (if the CVP server is configured 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***

This section describes how the HTTP Security server handles a connection where CVP checking is performed. The Security 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 that needs to be checked is carried in the response that comes from the Web server. Therefore, 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 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 number of connections opened with the CVP server. Nonetheless, sending all content for CVP checking provides better protection.

Check Point Security Gateway considers non-executable picture and video files to be safe because they do not normally contain viruses.

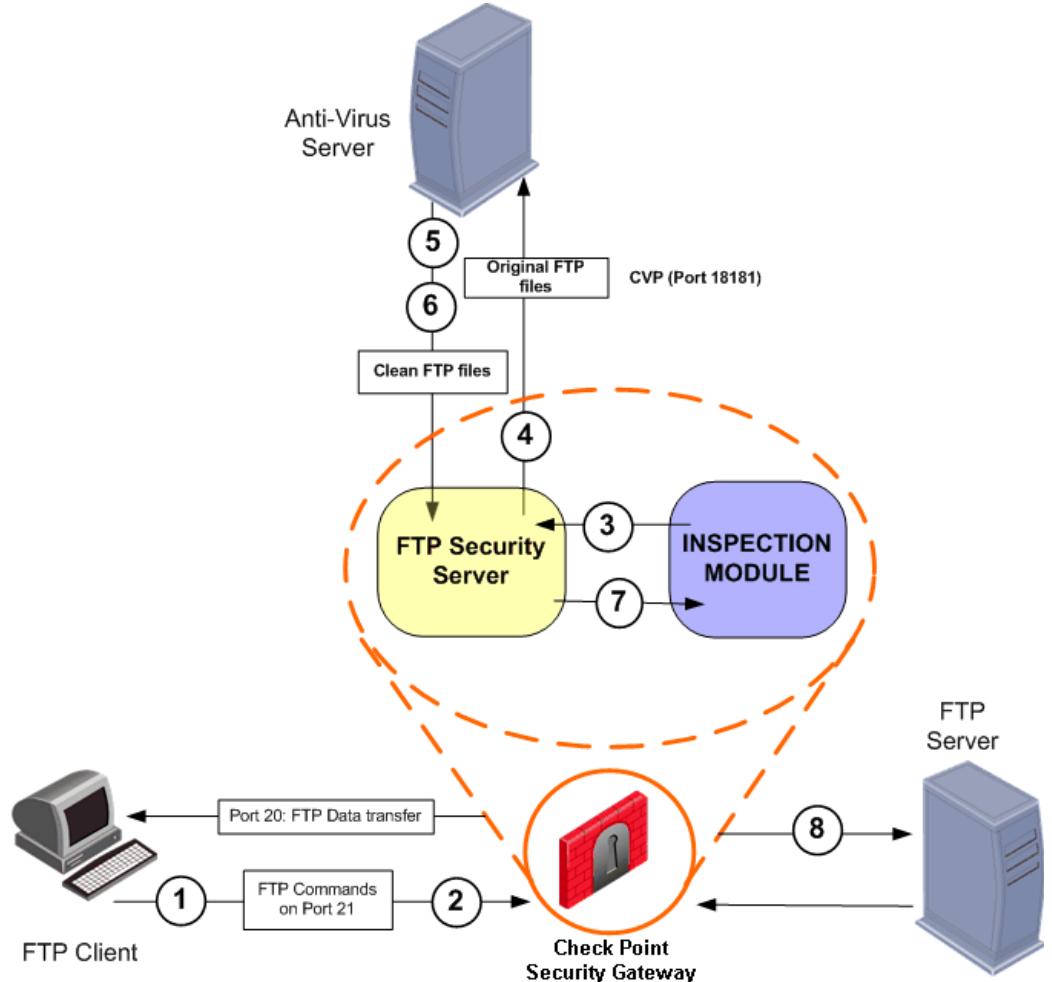
The HTTP Security server identifies safe content by actually examining the contents of a file. It does not rely on examining the URL (for file extensions such as \*.GIF) nor does it rely on checking the MIME type (such as image/gif) in the server response.

For configuration details, refer to “[Configuring CVP for Web Traffic Performance](#)” on page [347](#).

## Using CVP for Virus Scanning on FTP Connections

Virus scanning on FTP connections can be performed by transferring the file to a third-party Anti-Virus application using the CVP protocol.

**Figure 14-3** CVP Inspection Process during 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 data transfer over port 20, the gateway diverts 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. Based on the Validation Result message, the FTP Security server determines whether to transfer the file, 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 to Limit Web Surfers

### In This Section

<a href="#">Understanding URL Filtering</a>	page 338
<a href="#">URL Filtering Using the HTTP Security Server</a>	page 340
<a href="#">Enhanced UFP Performance Mode</a>	page 341
<a href="#">Choosing the URL Filtering Mode</a>	page 342

### ***Understanding URL Filtering***

The security administrator can prevent access to specific destinations on the Internet, allow access only to appropriate Web pages, and make it impossible to access particular websites or download certain file types.

This is done using third-party, OPSEC-certified URL Security Management applications. The security administrator can define a corporate security policy that includes URL screening to block undesirable Web pages and to record the types of URLs accessed for internal analysis and reporting needs.

A URL Filtering Protocol (UFP) server maintains a list of URLs and their categories. When a user requests a URL, Check Point Security Gateway 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.

By default, UFP uses TCP port 18182.



**Note** - A basic URL filtering capability is built in to Check Point Security Gateway. It can be used to block a specific list of URLs without a UFP server. For details, refer to “[Basic URL Filtering](#)” on page 370.

Check Point Security Gateway can integrate with OPSEC-certified solutions in different ways:

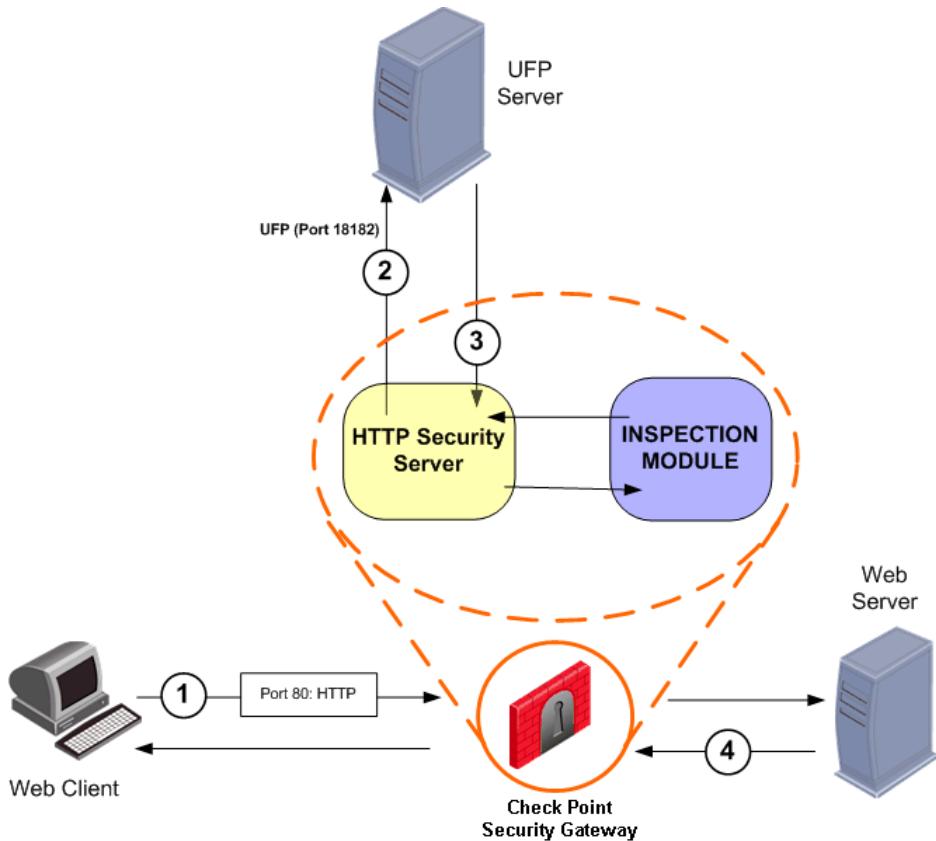
- Enhanced UFP Performance mode (called **Enhanced UFP Performance** in the URI Resource) uses kernel inspection together with a dedicated UFP daemon (aufpd). However, in this mode, it is not possible to use CVP and UFP checking on the same connection.
- The standard UFP checking mode uses the HTTP Security server to mediate UFP connections. This can add significantly to the response time experienced by clients that browse websites, in comparison to the Enhanced UFP Performance mode.

For configuration details, refer to “[Configuring URL Filtering with a UFP Server](#)” on page 348.

## ***URL Filtering Using the HTTP Security Server***

Figure 14-4 illustrates how Check Point Security Gateway performs URL Filtering of an HTTP connection using the HTTP Security server and a UFP server.

**Figure 14-4** URL Filtering (UFP) Process for an HTTP Connection

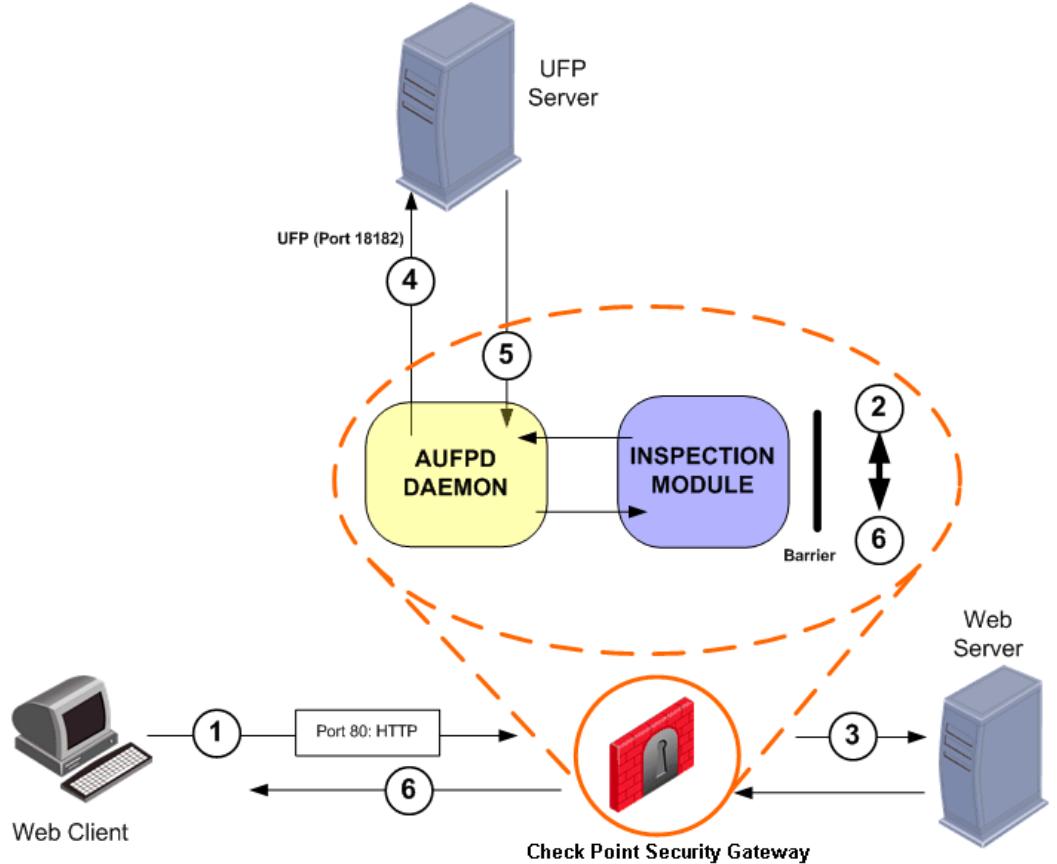


1. The client invokes a connection through the Inspection Module.
2. The HTTP Security server uses UFP to send the URL to be categorized to the third-party UFP server.
3. The UFP server inspects the file and returns a Validation Result message, notifying the Security server of the result of the inspection.
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 14-5 illustrates how enhanced URL Filtering (UFP) performance of an HTTP connection works.

**Figure 14-5** Enhanced URL Filtering (UFP) Process, Using Kernel Inspection



1. The Web client invokes a connection through the Check Point Security Gateway 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 Security Gateway 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 Security Gateway.
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 performing UFP Filtering. When deciding the method to employ, you must balance performance against security.

When the Enhanced UFP Performance mode is used, users browsing websites experience significantly improved response times, as compared to UFP checking using the 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.

## **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, refer to “[Performing CVP/UFP Inspection on any TCP Service](#)” on page 351.

# Configuring Content Security

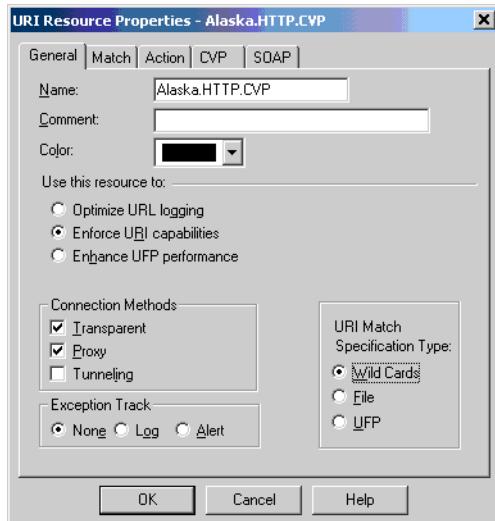
## In This Section

Resources: What They Are and How to Use Them	page 343
Creating a Resource and Using it in the Rule Base	page 344
Configuring Anti-Virus Checking for Incoming Email	page 345
Configuring CVP for Web Traffic Performance	page 347
Configuring URL Filtering with a UFP Server	page 348
Performing CVP/UFP Inspection on any TCP Service	page 351
Advanced CVP Configuration: CVP Chaining and Load Sharing	page 352

## 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 14-6). 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.

**Figure 14-6** A URI Resource, Showing the General Tab



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

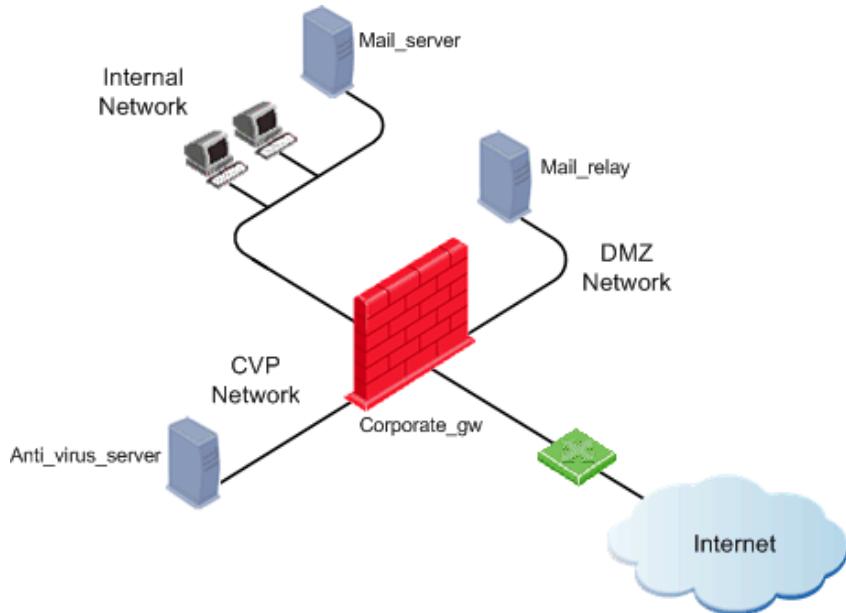
1. To create a resource, select the Resources tab in the objects tree. Select the Resource Type, right-click, select a resource type, such as **New URI** or **New SMTP**.
2. Define the resource parameters in the **General** tab, and in the other tabs as required.
3. To use a service with a resource in 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 14-7](#). 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 by the Anti-Virus server (Anti\_virus\_server). Outgoing mail is sent from the mail server to the Internet.

**Figure 14-7** Sample Configuration - Illustrating Anti-Virus Checking for Incoming Email



To configure Anti-Virus checking for incoming email:

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 performed.
4. Define rules that use the resource.

To implement Anti-Virus checking for incoming email:

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 Security Management server. In the **CVP Options** tab, verify that FW1\_cvps 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 performed.
  - a. In the **General Tab**, give the Resource a **Name** (such as virus\_check). Select both the **Mail Delivery** and the **Error Mail Delivery** options, as well as **Exception Tracking**.
  - b. In the **Match** tab, for the **Sender** put \*, and for the **Recipient** put \*@*your\_domain*, (for example \*@company.com).
  - c. In the **Action1** tab, define the **Rewriting Rules**, if any.
  - d. 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**.
5. Click **OK**. A message may appear regarding stripping MIME of type “message/partial”. Accepting the MIME strip of type “message/partial” changes configuration 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.
6. Define a pair of rules that will perform virus checking on incoming mail, and a rule to allow outbound email.

- 
7. Install the security policy: **Policy > Install**.

**Table 14-1**

Source	Destination	Service	Action	Track	Install On	Comment
Any	mail_relay	smtp	Accept	Log	Corporate_gw	Incoming to mail relay
mail_relay	mail_server	smtp->virus_check	Accept	Log	Corporate_gw	Incoming virus scan
mail_server	Any	smtp	Accept	Log	Corporate_gw	Outgoing email

## Configuring CVP for Web Traffic 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, refer to “[Improving CVP Performance for Web Traffic](#)” on page 336.

To configure CVP checking for Web traffic:

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 performed.
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. Refer to the sample rule shown in [Table 14-2](#).

**Table 14-2** Sample URI Resource in a Rule Base

Source	Destination	Service	Action
Internal_LAN	Any	http->Internal.HTTP.CVP	Accept

## Configuring URL Filtering with a UFP Server

Check Point Security Gateway 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 Check Point Security Gateway and the URL Filtering server uses the UFP.

### **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 additional information on these two modes, refer to “[Using URL Filtering to Limit Web Surfers](#)” on page 338.

- 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 all of these rules, 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 the connection matches the UFP category, the action specified 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.

This means that you can only have one rule with an **Enhance UFP Performance** resource, for a given Source, Destination, or 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.

When 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, or Service. However, to maintain a simpler and less error-prone Rule Base, it is recommended to use only one resource, as for the **Enhance UFP Performance** mode.

For example, consider the following rules:

**Table 14-3** Enforce URL Filtering Rules

No.	Source	Destination	Service	Action
1	Any	Any	Resource with UFP Category “Drugs”	Drop
2	Any	Any	Resource with UFP Category “Alcohol”	Drop

If a connection fits the UFP category of “Alcohol”:

- In **Enhance UFP Performance** mode, the connection matches Rule 1 and the connection is Accepted — which is not the desired behavior.
- In **Enforce URI Capabilities** mode, the connection matches Rule 2 and the connection is Dropped.

The correct way to build this rule so that it will work in all modes, and for greater simplicity, is as follows:

**Table 14-4** Optimal Enforce URL Filtering Rule

No.	Source	Destination	Service	Action
1	Any	Any	Resource with UFP Categories “Drugs” and “Alcohol”	Drop

## **Configuring URL Filtering**

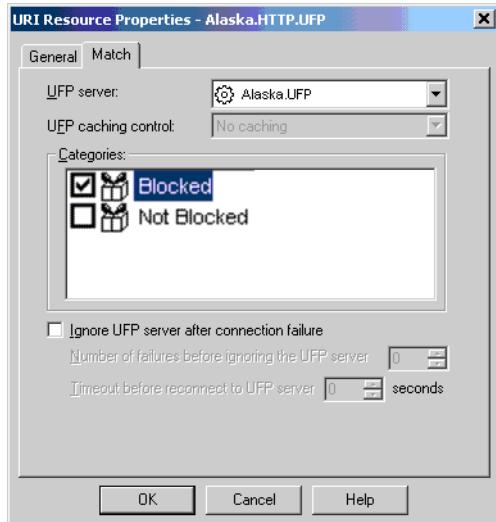
This procedure describes how to configure a URL Filtering using the Check Point Security Gateway kernel or using the Security server. For background information, refer to [“Using URL Filtering to Limit Web Surfers” on page 338](#).

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 Check Point Security Gateway 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 14-8** Match tab for a URI Resource for UFP



- Associate the Resource with the HTTP Service, and place it in a rule in the Security Rule Base. Refer to the sample rules shown in [Table 14-5](#).

The Action in Rule 1 is *Drop* because the resource matches the Blocked categories. If the resource matched the 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 14-5** Sample UFP Rule Base Policy

No.	Source	Destination	Service	Action
1	Any	Any	http->Alaska_HTTP_UFP	Drop
2	Any	Any	http	Accept

## Performing CVP/UFP Inspection on any TCP Service

In this procedure, you will create and configure a TCP service and a TCP resource. These steps are done with the Firewall tab open, by selecting different tabs in the left panel.

To configure CVP or UFP inspection on any TCP service:

1. Open the **Services** tab.
2. Right-click **TCP** and choose **New TCP**. Fill in the general properties of the new TCP service.
3. Click **Advanced**.
4. In the **Advanced TCP Service Properties** window, check **Enable for TCP Resource** and then click **OK**.
5. Open the **Servers and OPSEC Applications** tab, right-click **OPSEC Applications**, and choose **New > OPSEC Applications**.
6. In the **OPSEC Application Properties** window, name the server and select **Server Entities > CVP and UFP**.
7. Select a host to act as the CVP and UFP server.
8. In the **UFP Options** and **CVP Options** tabs, select the TCP service configured in the Services tab.
9. Click **OK**.
10. Open the **Resources** tab, right-click **Resources**, and choose **New > TCP**.
11. In the **TCP Resource Properties** window, provide a name for the resource and choose **UFP** or **CVP**.
12. The tab that appears in this window depends on whether you chose UFP or CVP. In this tab, select the CVP/UFP server you configured in OPSEC Applications.
13. Click **OK**.
14. Add a rule to the Rule Base: in the **Service** column, select **Add with Resource**.
15. In the **Service with Resource** window, select the configured TCP service.
16. In the **Resource** drop-down list, select the configured TCP resource.
17. Install the security policy: **Policy > Install**.

# Advanced CVP Configuration: CVP Chaining and Load Sharing

## In This Section

Introduction to CVP Chaining and Load Sharing	page 352
CVP Chaining	page 352
CVP Load Sharing	page 354
Combining CVP Chaining and Load Sharing	page 355
Configuring CVP Chaining and Load Sharing	page 355

## Introduction to CVP Chaining and Load Sharing

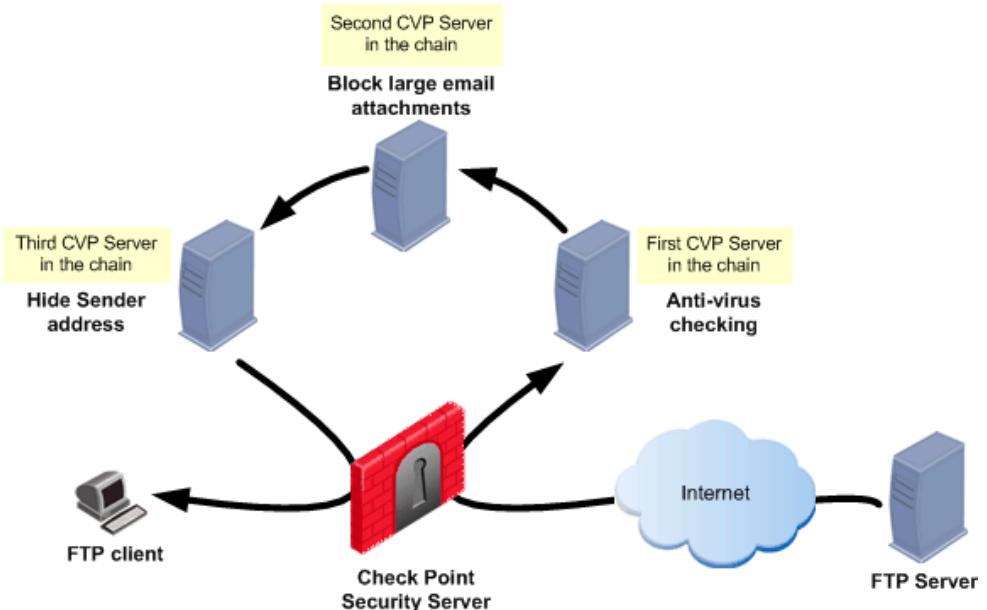
Traffic that crosses the Security Gateway can be checked using CVP servers. CVP checking is available for Web, Mail, FTP and TCP traffic. For detailed explanations, see:

- “CVP and Anti-Virus Protection for SMTP and HTTP Traffic” on page 335.
- “Using CVP for Virus Scanning on FTP Connections” on page 337.

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 14-9, the Check Point Security Gateway server invokes the first, second, and third CVP servers in turn.

**Figure 14-9** CVP Server Chain

Chained CVP servers are invoked in the order set 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 14-9](#), you may want 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 Security Gateway or on the protected (internal interface) side.

For example, in [Figure 14-9](#), consider a user at an internal FTP client who is downloading a file from an external FTP server. CVP checking is performed 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 performed 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.

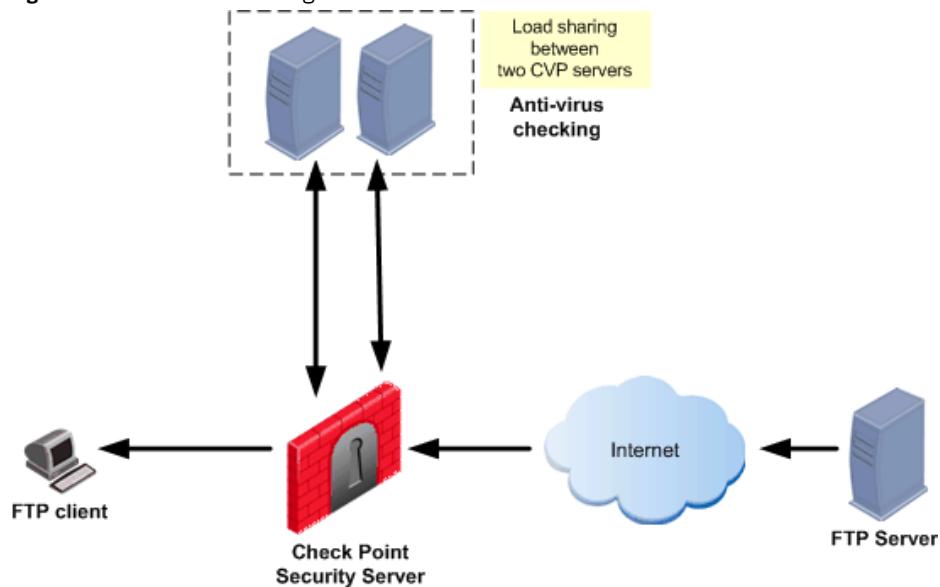
Two load-sharing methods are available:

- **Round robin:** The Security server sends each new CVP session to a different CVP server in turn.
- **Random:** The 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 14-10** Load Sharing between CVP Servers

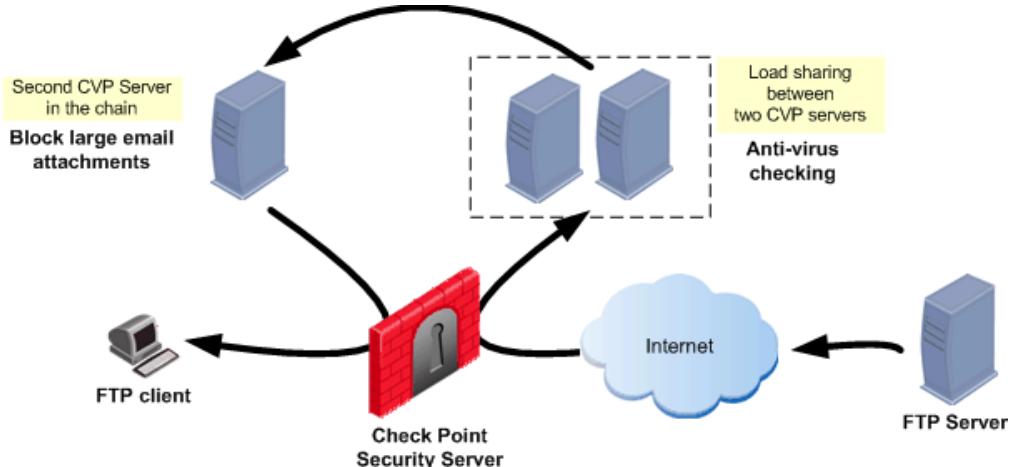


## Combining CVP Chaining and Load Sharing

It is possible to combine CVP chaining and load sharing. [Figure 14-11](#) 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.

**Figure 14-11** A Chained Load-Sharing CVP Server Group



## 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. Select the **Work distribution method**: Either Load sharing or Chaining.
5. If you select **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: **Policy > Install**.

# Chapter

# Services with Application Intelligence

## In This Chapter

Introduction to Services with Application Intelligence	page 358
DCE-RPC	page 358
SSLv3 Service	page 359
SSHv2 Service	page 359
FTP_BASIC Protocol Type	page 359
Domain_UDP Service	page 360
Point-to-Point Tunneling Protocol (PPTP)	page 361
Blocking Visitor Mode (TCPT)	page 363

# Introduction to Services with Application Intelligence

There are a number of TCP services for which the firewall can perform content inspection, in addition to checking port numbers.

Services that support content inspection are those services having a defined Protocol Type in the **TCP Service Properties > Advanced** window, either nbsession or Microsoft-DS together with the configured Resource.



**Warning** - Do not delete or change the protocol type of the service objects that perform content inspection. If the service is altered in this way, the content inspection may not work.

## DCE-RPC

DCE-RPC (Distributed Computing Environment- Remote Procedure Call) is a technology that calls 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 (the default RPC Endpoint Mapper port) and provides the Endpoint Mapper with a UUID number interface. In return, the Endpoint Mapper provides the client with a port to which the client can connect.

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

## SSLv3 Service

To prevent security problems associated with earlier versions of SSL, it is possible to verify that SSL client connections are using version 3 or higher of the SSL protocol. 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 the firewall, use the **HTTPS** service in the Rule Base.

## SSHv2 Service

To prevent security problems associated with earlier versions of SSH, it is possible to verify that SSH connections are using version 2 or higher of the protocol. 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 enforces a reduced set of the FTP security checks performed 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:

- Every packet must be 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. Check Point Security Gateway normally maintains virtual DNS connections for the period of the UDP timeout. DNS verification speed can be improved by telling the firewall 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).

# Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol (PPTP) is a network protocol for creating Virtual Private Networks (VPNs) over the Internet. It was developed jointly by Microsoft Corporation and several remote access vendor companies.

PPTP sets up a secure client-to-client connection via a PPTP server. The connection is made up of TCP/PPTP control connections and the GRE data connections, GRE being the actual VPN tunnel.

Check Point Security Gateway secures PPTP while allowing Hide NAT as well as Static NAT for PPTP connections. The Security Gateway can also enforce compliance to the PPTP protocol. If enforcement is turned on, PPTP packets are checked for compliance with RFC 2637, including message type, and packet length. In addition, if the PPTP control connection closes, the GRE tunnel is also closed.

## Configuring PPTP

To configure PPTP:

1. Define an object for the PPTP client that originates the connection, and an object for the PPTP server (not the destination client).
2. To allow PPTP connections through the Security Gateway, you must define a PPTP rule in the Security Rule Base using the `pptp_tcp` service. In the service column, set either `pptp_tcp` or `Any` (by default the `pptp_tcp` Service object is set to **Match for Any** in the Advanced Service Properties).

Source	Destination	Service	Action
<code>pptp_client</code>	<code>pptp_server</code>	TCP: <code>pptp_tcp</code>	Accept

3. To enforce compliance to the PPTP protocol and allow Hide NAT, turn on enforcement in IPS **Application Intelligence > VPN Protocols > Point to Point Tunneling Protocol**. Static NAT is supported even with the enforcement turned off. IPS enforcement is turned on by default for new installations. For upgrades it is turned off.

4. For gateways of version NGX R60 or lower, or if enforcement is turned off, an additional rule is required to allow the GRE tunnel:

Source	Destination	Service	Action
pptp_client	pptp_client	?:GRE	Accept
pptp_server	pptp_server		

## Advanced Configuration

It is possible to configure strict enforcement of the PPTP protocol using the `pptp_strict_enforcement` database property. However, this may cause connectivity problems because many PPTP applications do not rigorously conform to RFC 2637.

Using the GUIdbedit database tool, go to: **Table > Managed Objects > asm > AdvancedSecurityObject**. Open this object, look for the line containing `pptp_strict_enforcement` in the **value** column, and change the value from **false** (the default setting) to **true**.

# Blocking Visitor Mode (TCPT)

## 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 a 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 firewall 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. Refer to the *Advanced Configuration* chapter of the *Check Point Security Gateway Administration Guide* for details.

## How the Firewall Identifies TCPT

The firewall 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. (Refer to “[Changing the Port Used to Block Outgoing TCPT](#)” on page 364.)

## 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 perform content inspection have a defined Protocol Type in the **TCP Service Properties>Advanced** window.

## **Blocking Visitor Mode (Blocking Outgoing TCPT)**

To block outgoing TCPT, use the Database Tool on the Security Management server to locate and change the following property for every Security Gateway for which you wish to block outgoing TCPT:

`disable_outgoing_tcpt (false)`

Change the value of the property to true.

## **Changing 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 Security Management server:

`tcpt_outgoing_port (443)`

Change the value of the property to the required port number.

# **Web Security**

This section describes the firewall Web Content capabilities that provide high performance attack protection for Web servers and applications.



# Chapter

# Web Content Protection

## In This Chapter

Introduction to Web Content Protection	page 368
Web Content Security in the Rule Base	page 369
Securing XML Web Services (SOAP)	page 372
Understanding HTTP Sessions, Connections and URLs	page 373
Connectivity or Security: Web Surfers	page 376
HTTP Security Server Performance	page 378
Configuring Web Content Protection	page 380

# Introduction to Web Content Protection

This chapter discusses the following firewall Web Security capabilities:

- Integrated Web security capabilities configured via the firewall Security Rule Base. These include a number of URL-based protections.
- The ability to secure XML Web Services (SOAP) on Web servers.

# Web Content Security in the Rule Base

## In This Section

<a href="#">What is a URI Resource?</a>	page 369
<a href="#">Filtering URLs</a>	page 369
<a href="#">Basic URL Filtering</a>	page 370
<a href="#">URL Logging</a>	page 370
<a href="#">Java and ActiveX Security</a>	page 371

Check Point Security Gateway provides Web security capabilities configured through the Security Rule Base, rather than IPS. These include a number of URL-based protections.

## What is a URI Resource?

Web security is implemented via the Security Rule Base by defining a SmartDashboard object called a URI Resource, and using it in the Security Rule Base. For a description of Resource objects, refer to “[Resources: What They Are and How to Use Them](#)” on page 343.

URI stands for Uniform Resource Identifier. A URI is more or less identical to the familiar URL (Uniform Resource Locator).

## Filtering URLs

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, refer to “[Blocking URL-Based Attacks Using URI Resources](#)” on page 380.

## Basic URL Filtering

Basic URL Filtering capability is integrated into the firewall. 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, refer to [“Configuring Basic URL Filtering” on page 381](#).

More comprehensive URL Filtering is available using third-party, OPSEC-certified applications (refer to [“Using URL Filtering to Limit Web Surfers” on page 338](#)).

## 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 details on configuring the logging of URLs, either by performing kernel inspection on the HTTP connection or using a URI Resource, refer to [“Configuring URL Logging” on page 381](#).

## Java and ActiveX Security

Check Point Security Gateway can protect Web surfers by controlling incoming Java and ActiveX code according to specific conditions, such as host, URL, or authenticated user name.

Java and ActiveX screening capabilities 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. Refer to “[Creating a Resource and Using it in the Rule Base](#)” on page 344.

# Securing XML Web Services (SOAP)

Check Point Security Gateway provides certain Web security capabilities configurable via the Security Rule Base, rather than Web Intelligence. These include securing SOAP-based XML Web Services.

XML Web services, using XML Schema and SOAP, facilitate application to application communication. This is an important emerging communicating protocol using Internet protocols and standards. This is in contrast to Web pages (using HTML and DHTML), which are intended for person-to-program communication, and email and Instant Messaging (using protocols such as SMTP and MIME), which are also intended 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 run on the destination computer.

Check Point Security Gateway uses a Security server to prevent potential attacks by verifying that the HTTP, XML, and methods in SOAP requests conform to the RFC. Check Point Security Gateway also ensures that only methods contained in a predefined white-list of acceptable methods are allowed in a SOAP packet. The manner in which the firewall treats SOAP packets is defined in a URI resource that specifies whether a SOAP packet passing through the gateway is always accepted, or limited to methods specified in the white list.

SOAP processing defined in the URI resource is performed only if the HTTP connection carrying the SOAP message has already been 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, refer to the online help in the URI Resource Properties **SOAP** tab.

# Understanding HTTP Sessions, Connections and URLs

To understand how to best use Check Point Security Gateway Power Web security and IPS 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
```

### ***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**

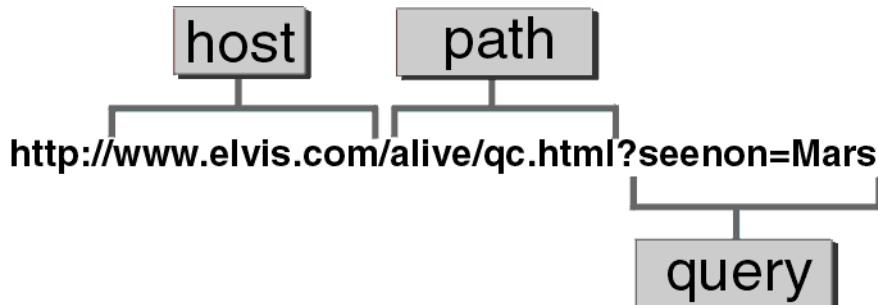
HTTP/1.1 encourages the transmission of multiple requests over a single TCP connection. Each request must still be sent in one contiguous message, and a server must send responses (on a given connection) in the order that it received the corresponding requests.

**Table 16-1** HTTP Request Connection Example

<b>Request # 1 Header section</b>	Post /Hello/ HTTP/1.1 Host: www.walla.co.il User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT5.0) Pragma: no-cache Content-length: 20 Connection: Keep-alive
<b>Request #1 - Body</b>	This my example body
<b>Request # 2 Header section</b>	Get /scripts/ HTTP/1.1 Host: www.walla.co.il User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT5.0) Pragma: no-cache Content-length: 0 Connection: Keep-alive

## Understanding URLs

A URL is made up of the **Host**, **Path** and **Query** parameters. In the URL in [Figure 16-1](#), the **Host** is `http://www.elvis.com`, the **Path** is `/alive/qc.html`, and the **Query** is everything else. Check Point Security Gateway and IPS can filter the URL on these parameters and decide whether to allow the HTTP request containing a particular URL.

**Figure 16-1** Example URL showing Host, Path and Query components

# Connectivity or Security: Web Surfers

To tune connectivity versus security for Web surfers, you need to adjust certain database properties.

## Allowing or Restricting Content

### ***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.

To ensure the Content-Disposition header is allowed:

1. From the SmartDashboard main menu, select **Policy > Global Properties**. The Global Properties window opens.
2. Open the **SmartDashboard Customization** page and click **Configure**. The Advanced Configuration window opens.
3. Open **Firewall > Web Security > Security**.
4. Select `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.

To allow ranges:

1. From the SmartDashboard main menu, select **Policy > Global Properties**. The Global Properties window opens.
2. Open the **SmartDashboard Customization** page and click **Configure**. The Advanced Configuration window opens.

3. Open **Firewall > Web Security > Security > Content Security**.
4. Select `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, 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 its 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 tune content compression:

1. From the SmartDashboard main menu, select **Policy > Global Properties**. The Global Properties window opens.
2. Open the **SmartDashboard Customization** page and click **Configure**. The Advanced Configuration window opens.
3. Select **Firewall > Web Security > Security > Content Security**.
4. Change the values of the compression properties as needed:
  - `http_disable_content_enc` If selected, compression of the content encoding data is allowed.
  - `http_disable_content_type` If selected, compression of the content type data is allowed.

# HTTP Security Server Performance

On multiple CPU machines, running more than one instance of the HTTP Security server increases the performance experienced by users. This is because each Security server uses a different CPU. Run at least one Security server instance for each CPU (refer to “[Running Multiple Instances of HTTP Security Server](#)” on page 379).

To allow more concurrent connections, it may well be worthwhile to run more than one Security server, even on a single CPU machine. However, this will increase the memory usage.

## 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 Check Point Security Gateway, as follows:

1. Web client to Security Gateway to Web server (request).
2. Web server to Security Gateway 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 Check Point Security Gateway three times:

1. Web client to Security Gateway to Web server (request).
2. Web server to Security Gateway to CVP/UFP server (response).
3. CVP/UFP server to Security Gateway to Web client (response).

Therefore, the available file descriptors are split three ways, so that a total of 341 simultaneous connections are possible.

## Running Multiple Instances of 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. Run the cpstart command to restart the Check Point Security Gateway.

# Configuring Web Content Protection

## In This Section

Blocking URL-Based Attacks Using URI Resources	page 380
Configuring URL Logging	page 381
Configuring Basic URL Filtering	page 381

## Blocking URL-Based Attacks Using URI Resources

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. See also “[Securing XML Web Services \(SOAP\)](#)” on page 372.

To block URL-based attacks:

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. (Optional) To specify a replacement URL to which 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.

**Table 16-2** Sample URI Resource in a Rule Base

No.	Source	Destination	Service	Action
1	Any	Any	http->Alaska.Web.Protection	Drop
2	Any	Any	http	Accept

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 the 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** specified as Accept.
4. Select **Log** in the **Track** column. This logs the URL of all connections that match this rule.

See also “[URL Logging](#)” on page 370.

## Configuring Basic URL Filtering

To prevent access to selected forbidden websites:

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

- 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 Security Gateway.
- /path is optional. Use it to restrict a particular directory in a site.
- category is an optional parameter that can be any hexadecimal number. It is not currently used.

Make sure that 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 1,000 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.

See also “[Basic URL Filtering](#)” on page 370.

# **Appendices**

This section describes how the Check Point Security Gateway machine protects itself and the networks behind it upon activation, and the command line interface.



# Appendix Security Before Firewall Activation

## In This Appendix

Achieving Security Before Firewall Activation	page 386
Boot Security	page 386
The Default Filter	page 387
The Initial Policy	page 390
Managing Default Filter and Initial Policy	page 393

# Achieving Security Before Firewall Activation

There are several scenarios in which a computer does not yet have a 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 a result, there is no point in 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, the firewall Boot Security feature protects both the internal networks behind the Security Gateway, and the computer itself. Boot Security is provided by two elements working together:

- Control of IP Forwarding on boot
- Default Filter

The Default Filter also provides protection in a scenario where firewall processes are stopped for maintenance.

## Control of IP Forwarding on Boot

For networks protected by a Security Gateway, 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 and no security policy is enforced. This ensures that networks behind the gateway are safe.

Disabling IP Forwarding protects networks behind the Check Point Security Gateway computer, but it does not protect the Security Gateway computer itself. For this purpose, the Security Gateway implements a Default Filter during the period of vulnerability.

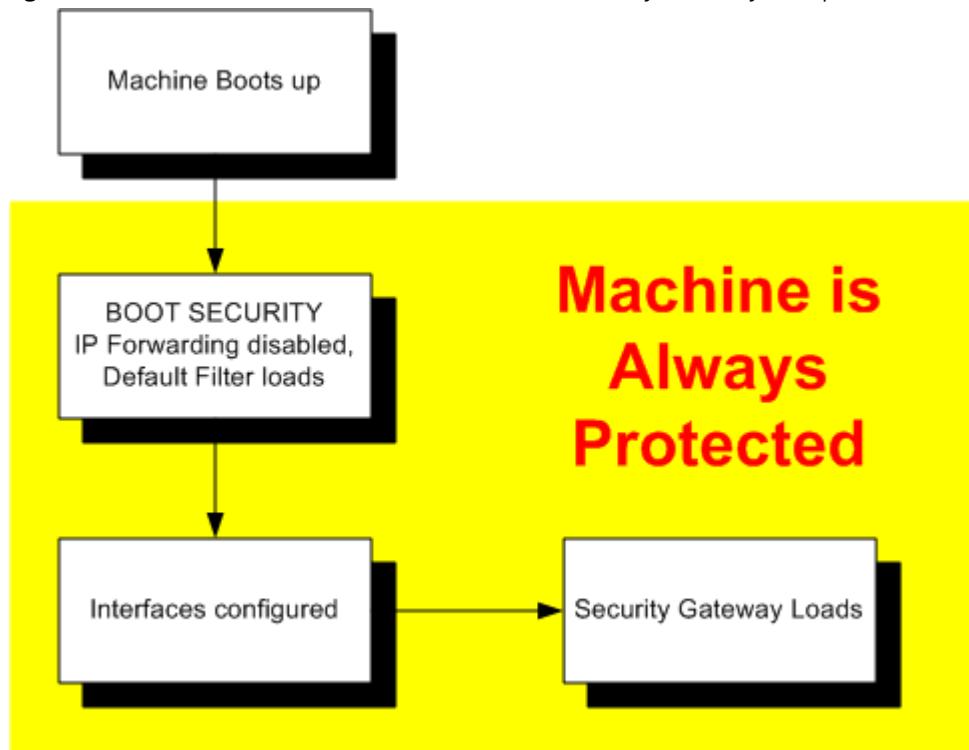
# The Default Filter

When a Security Gateway boots with the Default Filter, the following sequence is performed:

1. Computer boots up.
2. Boot security takes effect (Default Filter loads and IP Forwarding is disabled).
3. Interfaces are configured.
4. Check Point Security Gateway services start.

The computer is protected as soon as the Default Filter loads.

**Figure A-1** How a Default Filter Protects the Security Gateway Computer



There are several Default Filters:

- General Filter 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 Security Gateway. It ensures that packets whose source are the Security Gateway computer itself have not come from one of its interfaces.

## Changing 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`.

To change the Default Filter:

1. Copy over and rename the relevant desired Default Filter Inspect file (`defaultfilter.boot` or `defaultfilter.drop`) to `$FWDIR/conf/defaultfilter.pf`
2. Compile the Default Filter by running the command:  
`fw defaultgen`  
The output will be in `$FWDIR/state/default.bin`
3. Run `fwboot bootconf get_def` to print the Default Filter file path.
4. Copy `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.

## Defining a Custom Default Filter

For administrators with Inspect knowledge, you can define your own Default Filter.

To define a Default Filter:

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 from [step 2 of “Changing the Default Filter to a Drop Filter” on page 388.](#)

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 firewall processes for maintenance, and it is impractical to disconnect the Security 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 Check Point Security Gateway processes to be temporarily stopped for remote maintenance without exposing the computer to attack.

During maintenance, the Default Filter allows open connections to the gateway to remain open, without dropping them.

# The Initial Policy

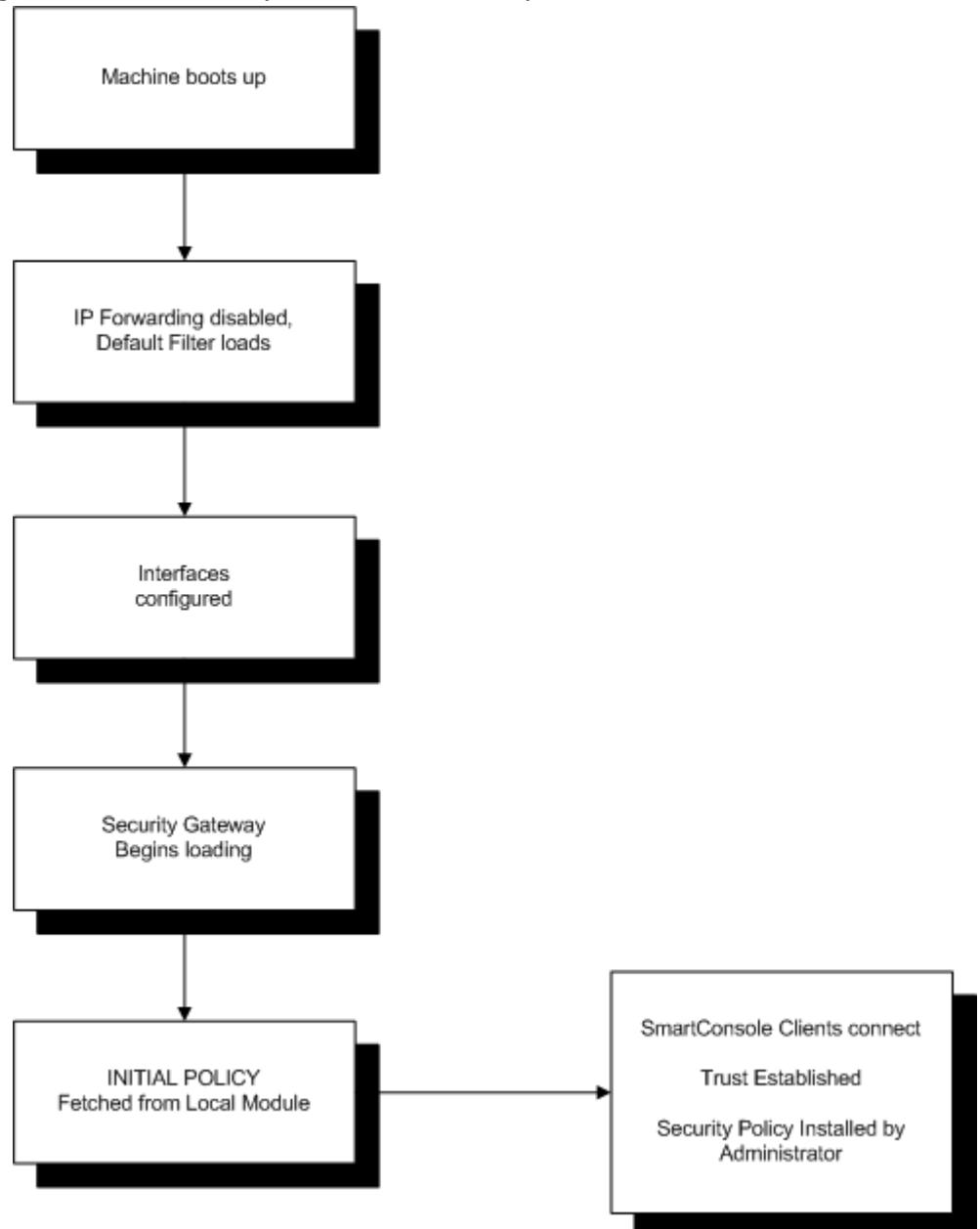
Until the Security Gateway administrator installs the security policy on the gateway for the first time, security is enforced by an Initial Policy. The Initial Policy operates by adding “implied rules” to the Default Filter. These rules forbid most communication yet allows the communication needed for the installation of the security policy. The Initial Policy also protects a gateway during Check Point product upgrades, when a SIC certificate is reset on the gateway, 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 Security Gateway computer until a security policy is loaded for the first time:

1. The computer boots up.
2. The Default Filter loads and IP Forwarding is disabled.
3. The Interfaces are configured.
4. Check Point Security Gateway services start.
5. The Initial policy is fetched from the local gateway.
6. 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 standalone and distributed setups. In a standalone configuration, where the Security Management server and Security Gateway are on the same computer, the Initial Policy allows CPMI communication only. This permits SmartConsole clients to connect to the Security Management server.

In a distributed configuration, where the Primary Security Management server is on one computer and the Security Gateway is on a different computer, the Initial Policy allows the following:

- Primary Security Management server computer — allows CPMI communication for SmartConsole clients.
- Security 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 Security Gateway does not allow CPMI connections. The SmartConsole will not be able to connect to the Security Management server if the SmartConsole must access the Security Management server through a gateway running the Initial Policy.

There is also an Initial Policy for a Secondary Security Management 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.

# Managing Default Filter and Initial Policy

## In This Section

Verifying Default Filter or Initial Policy Loading	page 393
Unloading Default Filter or Initial Policy	page 393
Troubleshooting: Cannot Complete Reboot	page 394
Command Line Reference	page 394

## Verifying Default Filter or Initial Policy Loading

You can verify that the Default Filter and/or Initial Policy are loaded.

To verify loading of the Default Filter or Initial Policy:

1. Boot the system.
2. Before installing another security policy, type the following command:

```
$FWDIR/bin/fw stat
```

The command's output should show that `defaultfilter` is installed for the Default Filter status. It should show that `InitialPolicy` is installed for the Initial Policy.

## Unloading Default Filter or 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 Security Management machine, run the following command on the Security Management server:

```
fwm unload <hostname>
```

where `hostname` is the SIC\_name of the gateway.

## Troubleshooting: Cannot Complete Reboot

In certain configurations the Default Filter may prevent the Security Gateway computer from completing the reboot following installation.

First, examine the Default Filter and verify that the Default Filter allows traffic that the computer needs in order 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

### In This Section

<a href="#">control_bootsec</a>	<a href="#">page 394</a>
<a href="#">fwboot bootconf</a>	<a href="#">page 395</a>
<a href="#">comp_init_policy</a>	<a href="#">page 396</a>
<a href="#">cpstop -fwflag -default and cpstop -fwflag -proc</a>	<a href="#">page 397</a>

### ***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

Options	Meaning
-r	Removes boot security
-g	Enables boot security

## ***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

Options	Meaning
Get_ipf	Reports whether firewall controls IP Forwarding. <ul style="list-style-type: none"> <li>• Returns 1 if IP Forwarding control is enabled on boot.</li> <li>• Returns 0 if IP Forwarding is not controlled on boot.</li> </ul>
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>	Loads <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.) <b>Note</b> - 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, for example, at `cpstart`, or with the `fw fetch localhost` command. After running this command, `cpconfig` adds an Initial Policy if there is no previous Policy installed.

### **Usage**

```
$FWDIR/bin/comp_init_policy [-u | -g]
```

**Table A-3** options `comp_init_policy`

Options	Meaning
<code>-u</code>	Removes the current Initial Policy, and ensures that it will not be generated in future when <code>cpconfig</code> is run.
<code>-g</code>	Generates the Initial Policy and ensures that it is loaded the next time a policy is fetched (at <code>cpstart</code> , or at next boot, or via the <code>fw fetch localhost</code> command). After running this command, <code>cpconfig</code> adds an Initial Policy when needed.

The `comp_init_policy -g` command will only work if there is no previous policy. If there is a policy, 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. `cpstart`. `comp_init_policy` creates the initial policy, but has a safeguard so 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 the existing user policy 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 firewall processes but leave the Default Filter running, use `cpstop -fwflag -default`. To stop all Check Point Security Gateway 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

Options	Meaning
-default	Kills firewall processes (fwd, fwm, vpnd, snmpd etc.). Logs, kernel traps, resources, and all security server connections stop working. The security policy in the kernel is replaced with the Default Filter.
-proc	Kills firewall 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, or drop rules that do not use resources, but only services, continue to work.



# Appendix

# Command Line Interface

The following firewall commands are also documented in the *Command Line Interface (CLI) Administration Guide*.

**Table B-1** Firewall-related Command Line Interface

Command	Description
comp_init_policy	Generates and loads (or removes) the Initial Policy.
fw	Various actions for the Check Point Security Gateway.
fw_isp_link	Takes down (or up) one of the redundant ISP links.
fw_monitor	Simplifies the task of capturing network packets at multiple capture points within the firewall chain.
fw_tab	Displays kernel table contents and enables you to change the contents of dynamic tables. Static tables cannot be changed.
fw_stat	Displays the content of state tables on target hosts in various formats. For each host, the default format displays the host name and a list of all tables with their elements.
fw_ver	Displays the firewall major and minor version number and build number.
sam_alert	Executes SAM (Suspicious Activity Monitoring) actions according to information received from standard input, used with the User Defined alerts mechanism. It is normally run on the Security Management server.
svr_webupload_config	Provides configuration options for the Eventia Reporter Web upload script.

