Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=22913

For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

For more about this release, see the R76 home page (http://supportcontent.checkpoint.com/solutions?id=sk91140).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 February 2013</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Firewall R76 Administration Guide).
Contents

Important Information ............................................................................................................. 3
Check Point Firewall Security Solution ................................................................................ 7
 Overview of Firewall Features .................................................................................................. 7
 Components of the Check Point Solution ................................................................................. 7
 Dual Stack (IPv4 and IPv6) Network Configuration ................................................................. 8
 Access Control and the Rule Base ............................................................................................ 9
 How to Use this Guide .............................................................................................................. 9
 SmartDashboard Toolbar ......................................................................................................... 11
 Creating a Strong Firewall Security Policy ............................................................................. 12
 Using the Firewall Rule Base ................................................................................................. 12
 Managing the Firewall Rule Base ........................................................................................... 12
 Explicit and Implied Rules ....................................................................................................... 13
 Order of Rule Enforcement ...................................................................................................... 13
 Creating a Secure Firewall Rule Base ..................................................................................... 14
 Basic Rules ............................................................................................................................ 14
 Sample Firewall Rule Base ...................................................................................................... 14
 Defining Security Zones ......................................................................................................... 15
 Perimeter ................................................................................................................................ 15
 DMZ ....................................................................................................................................... 16
 Preventing IP Spoofing ........................................................................................................... 16
 Configuring Anti-Spoofing ........................................................................................................ 17
 Excluding Specific Internal Addresses ...................................................................................... 18
 Analyzing the Rule Base (Hit Count) ...................................................................................... 19
 Enabling or Disabling Hit Count ............................................................................................. 19
 Configuring the Hit Count Display .......................................................................................... 19
 Remote Access to the Network .............................................................................................. 21
 Overview .................................................................................................................................. 21
 Check Point Mobile Access Solutions ..................................................................................... 21
 Client-Based vs. Clientless ......................................................................................................... 21
 Mobile Access Clients ............................................................................................................... 22
 Mobile Access Web Portal ......................................................................................................... 22
 SSL Network Extender ............................................................................................................ 22
 Configuring Remote Access to Network Resources ............................................................... 22
 Sample Mobile Access Workflow ............................................................................................ 22
 Sample Mobile Access Deployment .......................................................................................... 23
 Using the Mobile Access Configuration Wizard ...................................................................... 23
 Allowing Mobile Connections .................................................................................................. 25
 Defining Access to Applications ............................................................................................... 25
 Activating Single Sign On ......................................................................................................... 26
 Connecting to a Citrix Server .................................................................................................... 26
 Citrix Services .......................................................................................................................... 26
 Sample Deployment with Citrix Server ..................................................................................... 27
 Configuring Citrix Services for Mobile Access ....................................................................... 27
 Endpoint Compliance Check .................................................................................................... 28
 Compliance Policy Rules ......................................................................................................... 28
 Creating an Endpoint Compliance Policy .................................................................................. 29
 Configuring Compliance Settings for a Security Gateway ...................................................... 30
 Using Secure Workspace ......................................................................................................... 31
 Creating VPN Policies ............................................................................................................. 32
 Overview .................................................................................................................................. 32
 Site to Site VPN ....................................................................................................................... 32
 Remote Access VPN ................................................................................................................. 35
Chapter 1

Check Point Firewall Security Solution

In This Chapter

- Overview of Firewall Features
- How to Use this Guide
- SmartDashboard Toolbar

Overview of Firewall Features

Firewalls control the traffic between the internal and external networks and are the core of a strong network security policy. Check Point Software Blades are a set of security features that makes sure that the Security Gateway or Security Management server gives the correct functionality and performance. The Check Point Firewall is part of the Software Blade architecture that supplies "next-generation" firewall features, including:

- VPN and mobile device connectivity
- Identity and computer awareness
- Internet access and filtering
- Application control
- Intrusion and threat prevention
- Data Loss Prevention

Components of the Check Point Solution
These are the primary components of the Check Point solution:

- **Security Gateway** - The security engine that enforces the organization’s security policy and acts as a security enforcement point. The Security Gateway is managed by the Security Management server and sits on the network as an entry point to the LAN.

- **Security Management server** - The server used by the system administrator to manage the security policy. The organization’s databases and security policies are stored on the Security Management server and downloaded to the Security Gateway.

- **SmartDashboard** - A SmartConsole GUI application that is used by the system administrator to create and manage the security policy.

### Dual Stack (IPv4 and IPv6) Network Configuration

You can easily configure the Firewall to support a dual stack network that uses IPv4 and IPv6 addresses. Configure one or more interfaces with the applicable IPv4 and IPv6 addresses.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internet and external networks</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway</td>
</tr>
<tr>
<td>3</td>
<td>SmartDashboard</td>
</tr>
<tr>
<td>4</td>
<td>Security Management server</td>
</tr>
<tr>
<td>5</td>
<td>Internal network</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IPv4 network traffic</td>
</tr>
<tr>
<td>2</td>
<td>IPv6 network traffic</td>
</tr>
<tr>
<td>3</td>
<td>Security Gateway for dual stack network</td>
</tr>
<tr>
<td>4</td>
<td>Internal network (IPv6 traffic)</td>
</tr>
<tr>
<td>5</td>
<td>Dual stack web server in the DMZ</td>
</tr>
<tr>
<td>6</td>
<td>Security Gateway for IPv4 network</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>5</td>
<td>Security Gateway for IPv6 network</td>
</tr>
<tr>
<td>6</td>
<td>Mobile device (IPv4 traffic)</td>
</tr>
<tr>
<td>7</td>
<td>Mobile devices (IPv6 traffic)</td>
</tr>
</tbody>
</table>

**Note** - For R76 Security Gateways, you can configure the interfaces to use only IPv6 addresses.

### Access Control and the Rule Base

A primary goal of a firewall is to control access and traffic to and from the internal and external networks. The Firewall lets system administrators securely control access to computers, clients, servers and applications. The Firewall Rule Base defines the quality of the access control and network performance. Rules that are designed correctly make sure that a network:

- Only allows authorized connections and prevents vulnerabilities in a network
- Gives authorized users access to the correct internal networks
- Optimizes network performance and efficiently inspects connections

### How to Use this Guide

When you configure a Firewall, it is necessary that you understand how it is connected to the other Software Blades. For example, you must add a rule for the Firewall to allow remote users to connect to the internal network. In addition, you can enable Software Blades to supply advanced protection for the network, such as IPS and Anti-Bot.

Some of the sections in this guide tell you how to enable a sample configuration of a Software Blade. Make sure that you read the applicable Administration Guide for the Software Blade before you configure the feature for a production environment. Each section also explains rules that you must add to the Firewall Rule Base to complete the configuration for that feature.

### Software Blades in this Guide

<table>
<thead>
<tr>
<th>Software Blade</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Creating a Strong Firewall Security Policy (on page 12)</td>
</tr>
<tr>
<td></td>
<td>Configuring the NAT Policy (on page 88)</td>
</tr>
<tr>
<td>Mobile Access</td>
<td>Remote Access to the Network (on page 21)</td>
</tr>
<tr>
<td>IPsec VPN</td>
<td>Creating VPN Policies (on page 32)</td>
</tr>
<tr>
<td>Identity Awareness</td>
<td>Adding Users to the Security Policy (on page 39)</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>Defining an Internet Access Policy (on page 50)</td>
</tr>
<tr>
<td>Application Control</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td>Blade</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Anti-Bot</td>
<td></td>
</tr>
<tr>
<td>Anti-Virus</td>
<td></td>
</tr>
<tr>
<td>Anti-Spam</td>
<td></td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td></td>
</tr>
<tr>
<td>Advanced Networking &amp; Clustering</td>
<td></td>
</tr>
<tr>
<td>SmartEvent</td>
<td></td>
</tr>
<tr>
<td>SmartLog</td>
<td></td>
</tr>
</tbody>
</table>
## SmartDashboard Toolbar

You can use the SmartDashboard toolbar to do these actions:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📄</td>
<td>Open the SmartDashboard menu. When you are instructed to select menu options, click this button first. For example, if you are instructed to select Manage &gt; Users and Administrators, click this button to open the Manage menu and then select the Users and Administrators option.</td>
</tr>
<tr>
<td>📄</td>
<td>Save current policy and all system objects.</td>
</tr>
<tr>
<td>📄</td>
<td>Open a policy package, which is a collection of policies saved together with the same name.</td>
</tr>
<tr>
<td>🔄</td>
<td>Refresh policy from the Security Management Server.</td>
</tr>
<tr>
<td>🔄</td>
<td>Open the Database Revision Control window.</td>
</tr>
<tr>
<td>🍀</td>
<td>Change global properties.</td>
</tr>
<tr>
<td>🍀</td>
<td>Verify rule base consistency.</td>
</tr>
<tr>
<td>🛠️+</td>
<td>Install the policy on Security Gateways or VSX Gateways.</td>
</tr>
<tr>
<td>🛠️+</td>
<td>Open SmartConsoles.</td>
</tr>
</tbody>
</table>
Chapter 2

Creating a Strong Firewall Security Policy

In This Chapter

- Using the Firewall Rule Base
- Creating a Secure Firewall Rule Base
- Defining Security Zones
- Preventing IP Spoofing
- Analyzing the Rule Base (Hit Count)

Using the Firewall Rule Base

The firewall is the core of a well-defined network security policy. The goal of the Check Point Firewall Rule Base is to create rules that only allow the specified connections.

Managing the Firewall Rule Base

Use SmartDashboard to easily create and configure Firewall rules for a strong security policy.

These are the fields that manage the rules for the Firewall security policy.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Rule number in the Firewall Rule Base. Implied rules do not have a number.</td>
</tr>
<tr>
<td>Hits</td>
<td>Number of connections that match this rule.</td>
</tr>
<tr>
<td>Name</td>
<td>Name that the system administrator gives this rule.</td>
</tr>
<tr>
<td>Source</td>
<td>Network object that starts the connection.</td>
</tr>
<tr>
<td>Destination</td>
<td>Network object that completes the connection.</td>
</tr>
</tbody>
</table>
Creating a Strong Firewall Security Policy

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN</td>
<td>Definitions of the allowed or blocked traffic between VPN sites.</td>
</tr>
<tr>
<td>Service</td>
<td>Type of network service that is allowed or blocked.</td>
</tr>
<tr>
<td>Action</td>
<td>Firewall action that is done when traffic matches the rule.</td>
</tr>
<tr>
<td>Track</td>
<td>Tracking and logging action that is done when traffic matches the rule.</td>
</tr>
<tr>
<td>Install On</td>
<td>Network objects that will get the rule(s) of the security policy. The Policy Targets option installs the rule(s) on all Security Gateways.</td>
</tr>
<tr>
<td>Time</td>
<td>Time period that the Firewall enforces this rule.</td>
</tr>
<tr>
<td>Comment</td>
<td>An optional field that lets you summarize the rule.</td>
</tr>
</tbody>
</table>

**Note** - The X11 (X Window System Version 11) graphics display system is the standard graphics system for the Unix environment. To enable X11, create a specific rule that allows the X11 service. If you select Any as the Source or Destination, the X11 service is not included.

### Explicit and Implied Rules

These are the types of rules in the Rule Base:

- **Explicit rules** - Rules that you create to configure which connections the Firewall allows
- **Implied rules** - Rules that are based on settings in the Global Properties menu

Implied rules allow connections for different services that the Security Gateway uses. For example, the Accept Control Connections option allows packets that control these services:

- Installing the security policy on a Security Gateway
- Sending logs from a Security Gateway to the Security Management server
- Connecting to third party applications, such as RADIUS and TACACS authentication servers

#### To show the implied rules in the Policy window:

1. Make sure there is at least one rule in the Rule Base.
2. Click View > Implied Rules.
   
   The Policy window in the Firewall tab shows the Rule Base with the explicit and implied rules.

#### To configure the implied rules:

1. Click Policy > Global Properties.
2. From the navigation tree, click Firewall.
3. Select a rule to enable it, or clear a rule to disable it.
4. For the enabled rules, select the position of the rules in the Rule Base ("Order of Rule Enforcement" on page 13).
5. Click OK and install the policy.

### Order of Rule Enforcement

The Firewall inspects connections and enforces the Rule Base in a sequential manner. The Firewall inspects each connection that comes to the network and compares the data (source, destination, service, etc.) to the first rule. If the connection matches the rule, the Firewall applies the action of that rule. If the connection does not match the rule, the Firewall continues with the next rule in the Rule Base.
Creating a Strong Firewall Security Policy

Creating a Secure Firewall Rule Base

Basic Rules

These are basic access control rules we recommend for all Rule Bases:

- Stealth rule that prevents direct access to the Security Gateway.
- Cleanup rule that drops all traffic that is not allowed by the earlier rules.
  There is also an implied rule that drops all traffic, but you can use the Cleanup rule to log the traffic.

Sample Firewall Rule Base

This table shows a sample Firewall Rule Base for a typical security policy. (The Hits and VPN columns are not shown.)

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Stealth</td>
<td>NOT Corporate-</td>
<td>GW-group</td>
<td>Any</td>
<td>Drop</td>
<td>Alert</td>
<td>Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>internal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Targets</td>
</tr>
<tr>
<td>2</td>
<td>Critical subnet</td>
<td>Corporate-internal</td>
<td>Corporate-finance Corporate-hr Corporate-rnd</td>
<td>Any</td>
<td>Accept</td>
<td>Log</td>
<td>Corporate-gw</td>
</tr>
</tbody>
</table>
### Creating a Strong Firewall Security Policy

#### Firewall Administration Guide R76

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Tech support</td>
<td>Tech-Support</td>
<td>Remote-1-web</td>
<td>HTTP</td>
<td>Accept</td>
<td>Alert</td>
<td>Remote-1-gw</td>
</tr>
<tr>
<td>4</td>
<td>DNS server</td>
<td>Any</td>
<td>Corporate-dns</td>
<td>domain-udp</td>
<td>Accept</td>
<td>None</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>5</td>
<td>Mail and Web servers</td>
<td>Any</td>
<td>Corporate-dmz</td>
<td>HTTP HTTPS SMTP</td>
<td>Accept</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>6</td>
<td>SMTP</td>
<td>Corporate-mail</td>
<td>NOT Internal-net-group</td>
<td>SMTP</td>
<td>Accept</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>7</td>
<td>DMZ and Internet</td>
<td>Internal-net-group</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>8</td>
<td>Clean up rule</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

1. **Stealth** - All traffic that is NOT from the internal company network to one of the Security Gateways is dropped. When a connection matches the Stealth rule, an alert window opens in SmartView Monitor.
2. **Critical subnet** - Traffic from the internal network to the specified resources is logged. This rule defines three subnets as critical resources: Finance, HR, and RnD.
3. **Tech support** - Allows the Technical Support server to access the Remote-1 web server which is behind the Remote-1 Security Gateway. Only HTTP traffic is allowed. When a packet matches the Tech support rule, the Alert action is done.
4. **DNS server** - Allows UDP traffic to the external DNS server. This traffic is not logged.
5. **Mail and Web servers** - Allows incoming traffic to the mail and web servers that are located in the DMZ. HTTP, HTTPS, and SMTP traffic is allowed.
6. **SMTP** - Allows outgoing SMTP connections to the mail server. Does not allow SMTP connections to the internal network, to protect against a compromised mail server.
7. **DMZ and Internet** - Allows traffic from the internal network to the DMZ and Internet.
8. **Clean up rule** - Drops all traffic. All traffic that is allowed matched one of the earlier rules.

#### Defining Security Zones

Networks use different security zones to protect very important resources and to defend against malware. Create rules that allow only the applicable traffic in and out of a security zone. Make sure that there are different rules in the Firewall Rule Base that define traffic to and from the security zones. These are the key elements that define security zones:

- **External network** - Insecure data, such as the Internet
- **Internal network** - Company data that is only used by trusted and authenticated users
- **Perimeter** - The border between the internal and external networks.
- **DMZ** - Company servers that can be accessed from insecure sources, such as the Internet

#### Perimeter

The Firewall on the perimeter of the network is responsible for all the incoming and outgoing traffic. These are some of the connections that are usually allowed by a Firewall on the perimeter:

- **Outgoing connections to the Internet**
- **Connections to the DNS server**
- **Specified external connections**
- **Connections to servers in the DMZ**
• Connections from the internal network to the internal network
• VPN connections

**DMZ**

Servers that are accessed by the Internet are usually located in a DMZ (demilitarized zone). The DMZ makes sure that these servers cannot connect to the internal network. Make sure that the Rule Base contains rules for DMZ traffic. For example, these are rules for a web server in the DMZ:
• A rule that allows HTTP and HTTPs traffic to the DMZ network object
• A rule that allows traffic from the internal network group object to any destination (the destination includes the DMZ)

**Preventing IP Spoofing**

Firewall rules can be based on **Source** and **Destination** IP addresses. Attackers use IP spoofing to change a packet's IP address and make a packet look like it is from a trusted source. If your network is not protected against IP spoofing, attackers can exploit the vulnerability in the Firewall rules and gain access to the network.

Anti-spoofing protection makes sure that the source IP address is the same as the Security Gateway interface. The Firewall blocks a packet that comes to an external interface with a spoofed internal IP address. Check Point Anti-spoofing makes sure that packets go to the correct interface according to the destination IP address.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Interface IF1</td>
<td>6</td>
<td>Florida_LAN</td>
</tr>
<tr>
<td>2</td>
<td>Interface IF2</td>
<td>7</td>
<td>Alaska_RND_LAN</td>
</tr>
<tr>
<td>3</td>
<td>Interface IF3</td>
<td>8</td>
<td>Internet</td>
</tr>
<tr>
<td>4</td>
<td>Interface IF4</td>
<td>9</td>
<td>Alaska_GW</td>
</tr>
<tr>
<td>5</td>
<td>Alaska_LAN</td>
<td>10</td>
<td>Alaska_RND_GW</td>
</tr>
</tbody>
</table>

For the Alaska_GW, the Firewall makes sure that:
• All incoming packets to IF1 come from the Internet.
• All incoming packets to IF2 come from Alaska_LAN or, Alaska_RND_LAN or Florida_LAN.

For the Alaska_RND_GW, the Firewall makes sure that:
• All incoming packets to IF3 come from Alaska_LAN, Florida_LAN or the Internet.
• All incoming packets to IF4 come from Alaka_RND_LAN.

When you configure Anti-spoofing for a Security Gateway, specify if the interfaces go to the Internet (External) or an internal network (Internal).

**Configuring Anti-Spoofing**

Use the Topology page to configure Anti-spoofing for the external and internal interfaces on the Security Gateway. Configure Anti-spoofing protection on all the interfaces of the Security Gateway, including internal interfaces.

SmartDashboard attempts to automatically retrieve the topology from the Security Gateway. If it cannot retrieve the topology information, make sure that:

- The details in the Security Gateway **General Properties** window are correct.
- The Security Gateway, the Security Management server, and the SmartDashboard can communicate with each other.

When you configure an internal interface, select the option for the IP addresses that are connected to the interface. These are the network options:

- **Not Defined** - All IP addresses are considered as part of the internal network that connects to this internal interface.
- **Network defined by the interface IP and Net Mask** - There is only one network that connects to this internal interface.
- **Specific** - There is more than one network that connects to this internal interface. Select the group network object that contains all the appropriate networks.

**To configure Anti-Spoofing for an interface:**

1. In SmartDashboard, from the **Network Objects** tree, double-click the Security Gateway. The **General Properties** window opens.
2. From the navigation tree, click **Topology**.
3. Click **Get > Interfaces**.
4. Click **Accept**.
5. Select the interface that connects to the Internet and click **Edit**. The **Interface Properties** window opens.
6. Click the **Topology** tab.

![Topology tab](image)

7. Select **External** or **Internal**.

8. For **Internal** interfaces, do these steps:
   a) Select the option for the network **IP Addresses behind this interface**.
   b) If the internal interface connects to a DMZ, select **Interface leads to DMZ**.

9. Select **Perform Anti-Spoofing based on interface topology**.

10. Select an **Anti-Spoofing action**.
    - **Prevent** - Drops spoofed packets.
    - **Detect** - Allows spoofed packets.

    We recommend that you use the **Detect** option to monitor traffic. You can use it with a **Spoof Tracking** option to learn about the network topology without rejecting packets.

11. **Optional for External Interfaces**: Configure the IP addresses that are not included in Anti-spoofing ("Excluding Specific Internal Addresses" on page 18).
    a) Select **Don't check packets from**.
    b) Click the field, and select the Group or Network object that you are not including in Anti-spoofing.

        You can click **New** to create a new Group or Network object.

12. From **Spoof Tracking**, select the tracking action that is done when Anti-Spoofing is detected.

13. Click **OK** and configure Anti-spoofing for all the interfaces on the Security Gateway.

14. Click **OK** and install the policy.

---

**Excluding Specific Internal Addresses**

In some configurations, the Firewall must allow connections with an internal IP address from an external source. For example, an external application can assign internal IP addresses to external clients. You can configure the Anti-spoofing protection on the external interfaces to ignore connections from these IP addresses. The Firewall allows these connections and does not inspect them.
Analyzing the Rule Base (Hit Count)

Use the Hit Count feature to track the number of connections that each rule matches. You can show Hit Count for the rules in these options:

- The percentage of the rule's hits from total hits
- The indicator level (very high, high, medium, low, or zero)

These options are configured in the Firewall Rule Base and also changes how Hit Count is shown in other supported Software Blades.

When you enable Hit Count, the Security Management server collects the data from supported Security Gateways (from version R75.40 and up). Hit Count works independently from logging and tracks the hits even if the Track option is None.

You can use the Hit Count data to:

- Analyze a Rule Base - You can delete rules that have no matching connections

  Note - If you see a rule with a zero hit count it only means that in the Security Gateways enabled with Hit Count there were no matching connections. There can be matching connections on other Security Gateways.

- Better Firewall performance - You can move a rule that has a high hit count to a higher position in the Rule Base
- Better understand the behavior of the security policy

Enabling or Disabling Hit Count

By default, Hit Count is globally enabled for all supported Security Gateways (from R75.40). The timeframe setting that defines the data collection time range is configured globally. If necessary, you can disable Hit Count for one or more Security Gateways.

After you enable or disable Hit Count you must install the policy for the Security Gateway to start or stop collecting data.

To enable or disable Hit Count globally:
1. From the Policy menu, select Global Properties.
2. Select Hit Count from the tree.
3. Select the options:
   - Enable Hit Count - Select to enable or clear to disable all Security Gateways to monitor the number of connections each rule matches.
   - Keep Hit Count data up to - Select one of the time range options. The default is 6 months. Data is kept in the Security Management Server database for this period and is shown in the Hits column.
4. Click OK and then install the policy.

To enable or disable Hit Count on each Security Gateway:
1. From the Gateway Properties of the Security Gateway, select Hit Count from the navigation tree.
2. Select Enable Hit Count to enable the feature or clear it to disable Hit Count.
3. Click OK and then install the policy.

Configuring the Hit Count Display

These are the options you can configure for how matched connection data is shown in the Hits column:

- Value - Shows the number of matched hits for the rule from supported Security Gateways. Connection hits are not accumulated in the total hit count for:
  - Security Gateways that are not supported (versions before R75.40)
  - Security Gateways that have disabled the hit count feature

The values are shown with these letter abbreviations:

- K = 1,000
- M = 1,000,000
• $G = 1,000,000,000$
• $T = 1,000,000,000,000$
For example, 259K represents 259 thousand connections and 2M represents 2 million connections.

• **Percentage** - Shows the percentage of the number of matched hits for the rule from the total number of matched connections. The percentage is rounded to a tenth of a percent.

• **Level** - The hit count level is a label for the range of hits according to the table.
The hit count range = Maximum hit value - Minimum hit value (does not include zero hits)

<table>
<thead>
<tr>
<th>Hit Count Level</th>
<th>Icon</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero</td>
<td><img src="image" alt="icon" /></td>
<td>0 hits</td>
</tr>
<tr>
<td>Low</td>
<td><img src="image" alt="icon" /></td>
<td>Less than 10 percent of the hit count range</td>
</tr>
<tr>
<td>Medium</td>
<td><img src="image" alt="icon" /></td>
<td>Between 10 - 70 percent of the hit count range</td>
</tr>
<tr>
<td>High</td>
<td><img src="image" alt="icon" /></td>
<td>Between 70 - 90 percent of the hit count range</td>
</tr>
<tr>
<td>Very High</td>
<td><img src="image" alt="icon" /></td>
<td>Above 90 percent of the hit count range</td>
</tr>
</tbody>
</table>

**To configure the Hit Count display:**
1. Right-click the **Hits** column header or the rule number in the row.
2. From the menu, select **Display**.
3. Select one or more options:
   • Percentage
   • Value
   • Level
Chapter 3

Remote Access to the Network

Overview

Check Point Mobile Access Software Blade extends the functionality of a Firewall and lets remote users easily and securely use the Internet to connect to internal networks. Remote users start a standard HTTPS request to the Mobile Access Security Gateway. They can then authenticate with multiple options such as: user name/password, certificates, or SecurID.

SmartDashboard lets you easily create user groups and give the users access to the applicable applications. These are some of the different corporate applications that users can access:

- Web applications - A set of URLs that are accessed with an Internet browser. For example: inventory management or HR management applications.
- File share - A collection of files that are available with a specified protocol, such as SMB for Windows. Users can read, write, and delete files that are stored on the network.
- Citrix clients - Users can connect to internal XenApp servers.
- Web mail services - Mobile Access provides a front end for email servers that support IMAP and SMTP protocols. You can also configure other Web-based mail services, such as OWA (Outlook Web Access) and iNotes (IBM Lotus Domino Web Access).

For more about using the Mobile Access Software Blade, see R76 Mobile Access Administration Guide.

Check Point Mobile Access Solutions

Check Point Mobile Access has a range of flexible clients and features that let users access internal resources from remote locations. All these solutions include these features:

- Enterprise-grade, secure connectivity to corporate resources
- Strong user authentication
- Granular access control

For more information about the newest versions of Mobile Access solutions and clients, go to sk67820 (http://supportcontent.checkpoint.com/solutions?id=sk67820).

Client-Based vs. Clientless

Check Point remote access solutions use IPSec and SSL encryption protocols to create secure connections. All Check Point clients can work through NAT devices, hotspots, and proxies in situations with complex topologies, such as airports or hotels. These are the types of installations for remote access solutions:
- **Client-based** - Client application installed on endpoint computers and devices. Clients are usually installed on a managed device, such as a company-owned computer. The client supplies access to most types of corporate resources according to the access privileges of the user.

- **Clientless** - Users connect through a web browser and use HTTPS connections. Clientless solutions usually supply access to web-based corporate resources.

- **On demand client** - Users connect through a web browser and a client is installed when necessary. The client supplies access to most types of corporate resources according to the access privileges of the user.

### Mobile Access Clients

- **Check Point Mobile** - An app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.

- **Mobile VPN** - A full L3 tunnel app that gives users network access to all mobile applications.

- **Check Point Mobile for Windows** - A Windows IPsec VPN client that supplies secure IPsec VPN connectivity and authentication.

### Mobile Access Web Portal

The Mobile Access Portal is a clientless SSL VPN solution that supplies secure access to web-based resources. After users authenticate to the portal, they can access Mobile Access applications such as Outlook Web App and a corporate wiki.

### SSL Network Extender

SSL Network Extender is an on-demand SSL VPN client and is installed on the computer or mobile device from an Internet browser. It supplies secure access to internal network resources.

### Configuring Remote Access to Network Resources

#### Sample Mobile Access Workflow

This is a high-level workflow to configure remote access to the internal applications and resources.

1. Use SmartDashboard to enable the Mobile Access Software Blade on the Security Gateway.
2. Follow the steps in the Mobile Access Configuration wizard to configure these settings:
   - Select mobile device access clients
   - Define the Mobile Access portal
   - Define the web applications, for example Outlook Web App
   - Connect to the AD server for user information
3. For VPN clients, add Firewall rules to allow the mobile device connections.
4. **Optional**: Distribute client certificates to authenticate the mobile users.
   For R76 and higher, use the Certificate Creation and Distribution Wizard.
5. Users download the Check Point Mobile app.
6. Users open the Check Point Mobile app and enter the Mobile Access Site Name and necessary authentication, such as user name and password.
Sample Mobile Access Deployment

This is a sample deployment of a Mobile Access Security Gateway with an AD and Exchange server in the internal network.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mobile devices</td>
</tr>
<tr>
<td>2</td>
<td>Mobile Access tunnels</td>
</tr>
<tr>
<td>3</td>
<td>Internet (external networks)</td>
</tr>
<tr>
<td>4</td>
<td>Mobile Access Security Gateway</td>
</tr>
<tr>
<td>5</td>
<td>Internal network resources, AD and Exchange servers</td>
</tr>
</tbody>
</table>

In this sample Mobile Access deployment, a mobile device uses a Mobile Access tunnel to connect to the internal network. The Mobile Access Security Gateway decrypts the packets and authenticates the user. The connection is allowed and the mobile device connects to the internal network resources.

Using the Mobile Access Configuration Wizard

This procedure describes how to enable and configure the Mobile Access Software Blade on a Security Gateway with the Configuration wizard. For this sample configuration, the AD user group **Mobile_Access** contains all the users that are allowed to connect to the internal network. The deployment is based on the Sample Mobile Access Deployment (on page 23).

This configuration lets these clients connect to internal resources:
Remote Access to the Network

- Android and iOS mobile devices
- Windows and Mac computers
- Internet browsers can open a SSL Network Extender connection to the internal network

To configure Mobile Access:
1. In SmartDashboard, from the **Network Objects** tree, double-click the Security Gateway. The **General Properties** window opens.

3. Configure the Security Gateway to allow connections from the Internet and mobile devices. Select these options:
   - Web
   - Mobile Devices - Business Secure Container and VPN Client
   - Desktops - With compliance check
4. Click **Next**. The **Web Portal** page opens.
5. Enter the primary URL for the Mobile Access portal. The default is `https://<IPv4 address of the gateway>/sslvpn`.
6. Click **Next**. The **Applications** page opens.
7. Configure the applications that are shown:
   a) In **Web Applications**, make sure **Demo web application** is selected.
   b) In **Mail/Calendar/Contacts**, enter the domain for the Exchange server and select these options:
      - Check Point Secure Mail
      - ActiveSync Applications
      - Outlook Web App
      The Mobile Access portal shows links to the Demo web and Outlook Web App applications. The client on the mobile device shows links to the other applications.
8. Click **Next**. The **Active Directory** page opens.
9. Select the AD domain and enter the user name and password.
10. Click **Connect**. The Security Gateway makes sure that it can connect to the AD server.
11. Click **Next**.
The Users page opens.

12. Click Add and then select the group Mobile_Access.
13. Click Next and then click Finish.

The Mobile Access Configuration Wizard closes.

Allowing Mobile Connections

The Mobile Access Configuration Wizard enables and configures the Mobile Access Software Blade. It is necessary to add Firewall rules to allow connections from the VPN clients on the computers and devices.

Create a Host Node object for the Exchange server, all of the other objects are predefined.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
<th>Track</th>
</tr>
</thead>
</table>

All connections from the RemoteAccess VPN community to the Exchange server are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and MSExchange. This rule is installed on the MobileAccess_Gateway Security Gateway.

Defining Access to Applications

Use the Policy page to define rules that let users access Mobile Access applications. The applications that are selected in the Configuration wizard are automatically added to this page. You can also create and edit the rules that include these SmartDashboard objects:

- Users and user groups
- Mobile Access applications
- Mobile Access Security Gateways

Sample Mobile Access Policy

The Mobile Access rule lets the users in the Mobile_Access AD group access these applications on the Tokyo_Gateway:

- OWA - Outlook Web Access
- Mobile Secure Mail - Check Point Mobile clients can connect to the Exchange mail server to use email applications
- Access_My_PC - Remote Desktop application
- Corporate_Portal - Connect to the internal corporate web portal
- ActiveSync App - Connect to the Exchange mail server to use email applications such as Outlook
Activating Single Sign On

Enable the SSO (Single Sign On) feature to let users authenticate one time for applications that they use during Mobile Access sessions. The credentials that users enter to log in to the Mobile Access portal can be re-used automatically to authenticate to different Mobile Access applications. SSO user credentials are securely stored on the Mobile Access Security Gateway for that session and are used again if users log in from different remote devices. After the session is completed, the credentials are stored in a database file.

By default, SSO is enabled on new Mobile Access applications that use HTTP. Most Web applications authenticate users with specified Web forms. You can configure SSO for an application to use the authentication credentials from the Mobile Access portal. It is not necessary for users to log in again to each application.

To configure SSO:

2. Select an application and click Edit. The application properties window opens and shows the Single Sign On page.

3. For Web form applications, do these steps:
   a) In the Application Single Sign On Method section, select Advanced and click Edit. The Advanced window opens.
   b) Select This application reuses the portal credentials. Users are not prompted.
   c) Click OK.
   d) Select This application uses a Web form to accept credentials from users.
   e) Click OK.

4. Install the policy.

Connecting to a Citrix Server

Citrix Services

The Mobile Access Software Blade integrates the Firewall Citrix clients and services. It is not necessary to use STA (Secure Ticketing Authority) servers in a Mobile Access Security Gateway deployment because Mobile Access uses its own STA engine. You can also use Mobile Access in a deployment with STA and CSG (Citrix Secure Gateway) servers.

The Mobile Access server certificate must use a FQDN (Fully Qualified Domain Name) that is issued to the FQDN of the Mobile Access Security Gateway.
**Sample Deployment with Citrix Server**

This is a sample deployment of a Mobile Access Security Gateway and a Citrix web server in the DMZ. The Citrix XenApp server is connected to the internal network.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Mobile devices</td>
</tr>
<tr>
<td>2</td>
<td>Mobile Access tunnels</td>
</tr>
<tr>
<td>3</td>
<td>Internet (external networks)</td>
</tr>
<tr>
<td>4</td>
<td>Security Gateway for the internal network</td>
</tr>
<tr>
<td>5</td>
<td>Mobile Access Security Gateway in the DMZ</td>
</tr>
<tr>
<td>6</td>
<td>Citrix web interface</td>
</tr>
<tr>
<td>7</td>
<td>Internal network resources</td>
</tr>
<tr>
<td>8</td>
<td>Citrix XenApp (MetaFrame) server</td>
</tr>
</tbody>
</table>

**Configuring Citrix Services for Mobile Access**

This procedure describes how to configure Mobile Access to let remote users connect to Citrix applications. The deployment is based on the Sample Deployment with Citrix Server (on page 27).

**To configure Citrix services:**

1. In the **Mobile Access** tab, select **Endpoint Security on Demand > Applications > Citrix Services**.
2. Click **New**.

   The **General Properties** page of the **Citrix Service** window opens.
3. Enter the **Name** for the Citrix server object.
4. From the navigation tree, click **Web Interface**.
5. Create a new object for the Citrix web interface server, in **Servers**, click **Manage > New > Host**. The **Host Node** window opens.
6. Enter the settings for the Citrix web interface server and the click **OK**.
7. In Services, select one or more of these services that the Citrix web interface server supports:
   - HTTP
   - HTTPS
8. From the navigation tree, click **Link in Portal**.
9. Configure the settings for the link to the Citrix services in the Mobile Access portal:
   - **Link text** - The text that is shown for the Citrix link
   - **URL** - The URL for the directory or subdirectory of the Citrix application
   - **Tooltip** - Text that is shown when the user pauses the mouse pointer above the Citrix link
10. From the navigation tree, select **Additional Settings > Single Sign On**.
11. Enable Single Sign On for Citrix services, select these options:
    - **Turn on single Sign On for this application**
    - **Prompt users for their credentials**
12. Click **OK**. The Citrix server object is added to **Defined Citrix Services**.
13. From the Mobile Access navigation tree, select **Policy**.
14. Add the Citrix services object to the applicable rules.
   a) Right-click on the Applications cell of a rule and select **Add Applications**.
   b) Select the Citrix services object.
15. Install the policy.

### Endpoint Compliance Check

The Mobile Access Software Blade lets you use the Endpoint Security on Demand feature to create compliance policies and add more security to the network. Mobile devices and computers are scanned one time to make sure that they are compliant before they can connect to the network.

The Endpoint Compliance scanner is installed on mobile devices and computers with ActiveX (for Internet Explorer on Windows) or Java. The scan starts when the Internet browser tries to open the Mobile Access Portal.

### Compliance Policy Rules

The Endpoint Compliance policy is composed of different types of rules. You can configure the security and compliance settings for each rule or use the default settings.

These are the rules for an Endpoint Compliance policy:

- **Windows security** - Microsoft Windows hotfixes, patches and Service Packs.
- **Anti-spyware protection** - Anti-spyware software.
- **Ant-virus protection** - Anti-virus software version and virus signature files.
- **Firewall** - Personal firewall software.
- **Spyware scan** - Action that is done for different types of spyware.
- **Custom** - Compliance rules for your organization, for example: applications, files, and registry keys.
- **OR group** - A group of the above rules. An endpoint computer is compliant if it meets one of the rules in the group.
Creating an Endpoint Compliance Policy

The default setting for Endpoint Security on Demand is that all endpoint computers cannot log in to the Mobile Access portal until they are compliant with the Endpoint Compliance policy. Use the Policies window to create or edit an Endpoint Compliance policy.

This procedure shows how to configure a sample policy for company laptop computers.

To create an Endpoint Compliance policy:

1. In the Mobile Access tab, select Endpoint Security on Demand > Endpoint Compliance.
2. Click Edit policies.
   The Policies window opens.

3. Click New Policy.
   The Policies > New Policy window opens.
4. Enter the Name and Description for the policy.
5. Click Add.
   The Add Enforcement Rules window opens.
6. Select the rules for the policy.
   These are the rules for the sample laptop computer policy:
   - Default Windows Security rule
   - High security Anti-Spyware applications check
   - High security Anti-Virus applications check
   - High security spyware scan
   - Medium security Firewall applications check
7. Click OK.
The Policies > Edit Policy window shows the rules for the policy.

**Policies > Edit Policy**

Specify the criteria for this policy
Name: Laptop Computer
Description: This is a sample Endpoint Compliance policy for laptop computers
[Bypass spyware scan if endpoint meets Anti-Virus or Anti-Spyware requirements.

**Rules selected for this policy**

<table>
<thead>
<tr>
<th>Enforcement Rule</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Windows Security rule</td>
<td>Requires endpoint to have latest service pack installed and Windows</td>
<td>Windows Security</td>
</tr>
<tr>
<td></td>
<td>automatic updates to be enabled</td>
<td>Anti-Spyware</td>
</tr>
<tr>
<td>High security Anti-Spyware applications check</td>
<td>Requires endpoint to have supported Anti-Spyware application running</td>
<td>Anti-Virus</td>
</tr>
<tr>
<td></td>
<td>and updated within last 2 weeks</td>
<td></td>
</tr>
<tr>
<td>High security Anti-Virus applications check</td>
<td>Requires endpoint to have supported Anti-Virus application active and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>updated within last 2 weeks, and restricts user on inaccuracy</td>
<td></td>
</tr>
<tr>
<td>High security spyware scan</td>
<td>Spyware scan with high security - restricts all spyware categories except</td>
<td>Spyware Scan</td>
</tr>
<tr>
<td></td>
<td>of cookies</td>
<td></td>
</tr>
<tr>
<td>Medium security Firewall applications check</td>
<td>Requires endpoint to have supported Firewall application running and</td>
<td>Firewall</td>
</tr>
<tr>
<td></td>
<td>warns user on inaccuracy</td>
<td></td>
</tr>
</tbody>
</table>

8. Select **Bypass spyware scan**.
   When this feature is selected, the scan for endpoint computers that are compliant with the Anti-Virus or Anti-Spyware settings is changed. These computers do not scan for spyware when they connect to a Mobile Access Security Gateway.

9. Click **OK**.
   The Policies window opens.

10. Click **OK**.

**Configuring Compliance Settings for a Security Gateway**

The Firewall on a Mobile Access Security Gateway only allows access to endpoint computers that are compliant with the Endpoint Compliance policy.

This procedure shows how to configure the Laptop Computer policy ("Compliance Policy Rules" on page 28) for a Security Gateway.
To configure the Endpoint Compliance settings:
1. In the Mobile Access tab, select Endpoint Security on Demand > Endpoint Compliance.

2. Select the Security Gateway and click Edit.
   The Endpoint Compliance page of the Security Gateway properties window opens.

3. Select Scan endpoint machine when user connects.
4. Click Threshold policy and from the drop-down menu select Laptop Computer.
5. Click OK.

Using Secure Workspace

Secure Workspace is a security solution that allows remote users to connect to enterprise network resources safely and securely. The Secure Workspace virtual workspace provides a secure environment on endpoint computers that is segregated from the "real" workspace. Users can only send data from this secure environment through the Mobile Access portal. Secure Workspace users can only access permitted applications, files, and other resources from the virtual workspace.

Secure Workspace creates an encrypted folder on the computer called My Secured Documents and can be accessed from the virtual desktop. This folder contains temporary user files. When the session terminates, Secure Workspace deletes this folder and all other session data.

For more about configuring Secure Workspace, see the R76 Mobile Access Administration Guide.

To enable Secure Workspace on a Mobile Access Security Gateway:
1. In the Mobile Access tab, select Endpoint Security on Demand > Secure Workspace.
2. Select the Security Gateway and click Edit.
   The Check Point Secure Workspace page of the Security Gateway properties window opens.
3. Select This gateway supports access to applications from within Check Point Secure Workspace.
4. Click OK and then install the policy.
Chapter 4

Creating VPN Policies

Overview

The IPsec VPN Software Blade lets the Firewall encrypt and decrypt traffic to and from external networks and clients. Use SmartDashboard to easily configure VPN connections between Security Gateways and remote devices. You can configure Star and Mesh topologies for large-scale VPN networks that include third-party gateways. The VPN tunnel guarantees:

- Authenticity - Uses standard authentication methods
- Privacy - All VPN data is encrypted
- Integrity - Uses industry-standard integrity assurance methods

IKE and IPsec

The Check Point VPN solution uses these secure VPN protocols to manage encryption keys, and send encrypted packets. IKE (Internet Key Exchange) is a standard key management protocol that is used to create the VPN tunnels. IPsec is protocol that supports secure IP communications that are authenticated and encrypted on private or public networks.

For more about using IPsec VPN, see the R76 VPN Administration Guide.

Site to Site VPN

The basis of Site to Site VPN is the encrypted VPN tunnel. Two Security Gateways negotiate a link and create a VPN tunnel and each tunnel can contain more than one VPN connection. One Security Gateway can maintain more than one VPN tunnel at the same time.

Sample Site to Site VPN Deployment
Creating VPN Policies

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Gateway</td>
</tr>
<tr>
<td>2</td>
<td>VPN tunnel</td>
</tr>
<tr>
<td>3</td>
<td>Internal network in VPN domain</td>
</tr>
<tr>
<td>4</td>
<td>Host 1</td>
</tr>
<tr>
<td>5</td>
<td>Host 6</td>
</tr>
</tbody>
</table>

In this sample VPN deployment, Host 1 and Host 6 securely send data to each other. The Firewalls do IKE negotiation and create a VPN tunnel. They use the IPsec protocol to encrypt and decrypt data that is sent between Host 1 and Host 6.

**VPN Workflow**

Host 1 sends packet to Host 6 → Firewalls A & B create VPN tunnel → Firewall A encrypts data → Host 6 receives unencrypted data ← Firewall B decrypts data ← Encrypted data is sent through VPN tunnel

**VPN Communities**

A VPN Domain is the internal networks that use Security Gateways to send and receive VPN traffic. Define the resources that are included in the VPN Domain for each Security Gateway. Then join the Security Gateways into a VPN community. Network resources of the different Security Gateways can securely communicate with each other through VPN tunnels.

VPN communities are based on Star and Mesh topologies. In a Mesh community, there are VPN connections between each Security Gateway. In a Star community, satellites have a VPN connection with the center Security Gateway, but not to each other.

**Mesh Topology**

**Star Topology**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Gateway. For Star topology, the central Security Gateway.</td>
</tr>
<tr>
<td>2</td>
<td>For Star topology, satellite Security Gateways.</td>
</tr>
</tbody>
</table>
## Sample Combination VPN Community

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>London Security Gateway</td>
</tr>
<tr>
<td>2</td>
<td>New York Security Gateway</td>
</tr>
<tr>
<td>3</td>
<td>London - New York Mesh community</td>
</tr>
<tr>
<td>4</td>
<td>London company partner (external network)</td>
</tr>
<tr>
<td>5</td>
<td>London Star community</td>
</tr>
<tr>
<td>6</td>
<td>New York company partner (external network)</td>
</tr>
<tr>
<td>7</td>
<td>New York Star community</td>
</tr>
</tbody>
</table>

This deployment is composed of a Mesh community for London and New York Security Gateways that share internal networks. The Security Gateways for external networks of company partners do not have access to the London and New York internal networks. The Star VPN communities let the company partners access the internal networks.

### Routing VPN Traffic

Configure the Security Gateway to route VPN traffic based on VPN domains or based on the routing settings of the operating system.

**Domain Based VPN**

The VPN traffic is routed according to the VPN domains that are defined in SmartDashboard. Use domain based routing to let satellite Security Gateways send VPN traffic to each other. The center Security Gateway creates VPN tunnels to each satellite and the traffic is routed to the correct VPN domain.

**Route Based VPN**

VPN traffic is routed according to the routing settings (static or dynamic) of the Security Gateway operating system. The Security Gateway uses a VTI (VPN Tunnel Interface) to send the VPN traffic as if it were a physical interface. The VTIs of Security Gateways in a VPN community connect and can support dynamic routing protocols.

### Granular Routing Control

The Link Selection feature gives you granular control of the VPN traffic in the network. Use this feature to enable the Security Gateway to:

- Find the best possible route for VPN traffic
- Select the interfaces that are used for VPN traffic to internal and external networks
- Configure the IP addresses that are used for VPN traffic
• Use route probing to select available VPN tunnels
• Use Load Sharing for Link Selection to equally distribute VPN traffic to VPN tunnels

**Remote Access VPN**

If employees remotely access sensitive information from different locations and devices, system administrators must make sure that this access does not become a security vulnerability. Check Point's Remote Access VPN solutions let you create a VPN tunnel between a remote user and the internal network. The Mobile Access Software Blade ("Remote Access to the Network" on page 21) extends the functionality of Remote Access solutions to include many clients and deployments.

**Using Site to Site VPN**

**Sample Star Deployment**

This section explains how to configure a VPN star community. This deployment lets the satellite Security Gateways connect to the internal network of the central Security Gateway. The internal network object is named: **Internal-network**.

**To create a new VPN Star Community:**

1. In the IPsec VPN tab, select **Communities**.
2. Click **New > Star Community**.
   The **General** page of the Star Community Properties window opens.
3. Enter the name for the community.
4. From the navigation tree, select **Encryption**.
5. Configure the VPN encryption methods and algorithms for the VPN community.
6. Click **OK**.

**To configure star VPN for the Security Gateways:**

1. Double-click the Security Gateway.
   The Gateway Properties window opens.
2. In **Network Security**, select **IPsec VPN**.
3. From the navigation tree, click **Topology**.
4. In the **VPN Domain** section:
   - For the central Security Gateway, click **Manually defined** and select the **Internal-network** object.
   - For a satellite Security Gateway, select **All IP addresses**.
5. From the navigation tree, click **IPsec VPN**.
6. Configure the Security Gateway as a member of a VPN star community.
   a) In the **This Security Gateway participates in the following VPN Communities** section, click **Add**.
      The **Add this Gateway to Community** window opens.
   b) Select the VPN Community and click **OK**.
   c) Configure the Security Gateway as a hub or a spoke.
      ▪ For the center, select **Center Gateways**.
      ▪ For the satellites, select **Satellite Gateways**.
   d) Click **Add**.
   e) Click **OK**.
7. Do these steps for all the Security Gateways for the VPN community.

**Allowing VPN Connections**

When you create a VPN connection between Security Gateways, add Firewall rules to allow the VPN traffic. Use the VPN Community objects in the VPN column of the Firewall Rule Base to define access control for VPN connections in the network.

**Allowing All VPN Traffic**

Use the **Allow All Encrypted traffic** feature to configure the Firewall to allow all VPN traffic to the internal networks for the VPN communities. It is not necessary to add rules to the Firewall Rule Base that allow the VPN traffic for the specified VPN communities.

SmartDashboard adds this automatic rule to the top of the rule base:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>NOT Member Gateways</td>
<td>&lt;VPN community&gt;</td>
<td>Encrypted Services</td>
<td>Accept</td>
<td>Log</td>
<td>&lt;VPN gateways&gt;</td>
</tr>
</tbody>
</table>

This automatic rule allows all encrypted packets that are sent between hosts or clients in the specified VPN community. Traffic that is sent to the Security Gateways in the VPN community is dropped. The rule is installed on all Security Gateways in the VPN communities.

**Note** - This automatic rule can apply to more than one VPN community.

**Sample VPN Firewall Rules**

This table shows sample VPN rules for a Firewall Rule Base. (The **Action**, **Track** and **Time** columns are not shown. **Action** is set to **Allow**, **Track** is set to **Log**, and **Time** is set to **Any**.)

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>-</td>
<td>Any</td>
<td>NOT Member Gateways</td>
<td>BranchOffices</td>
<td>Encrypted Services</td>
<td>BranchOffices</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>LondonOffices</td>
<td></td>
<td>LondonOffices</td>
</tr>
<tr>
<td>2</td>
<td>Site to site VPN</td>
<td>Any</td>
<td>Any</td>
<td>All_GwToGw</td>
<td>FTP-port HTTP HTTPS SMTP</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>
### Creating VPN Policies

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Remote access</td>
<td>Any</td>
<td>Any</td>
<td>RemoteAccess</td>
<td>HTTP HTTPS IMAP</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

The first rule is the automatic rule for the **Accept All Encrypted Traffic** feature. The Firewalls for the Security Gateways in the BranchOffices and LondonOffices VPN communities allow all VPN traffic from hosts in clients in these communities. Traffic to the Security Gateways is dropped. This rule is installed on all Security Gateways in these communities.

2. **Site to site VPN** - Connections between hosts in the VPN domains of all Site to Site VPN communities are allowed. These are the only protocols that are allowed: FTP, HTTP, HTTPS and SMTP.

3. **Remote access** - Connections between hosts in the VPN domains of RemoteAccess VPN community are allowed. These are the only protocols that are allowed: HTTP, HTTPS, and IMAP.

### Using Remote Access VPN

This section explains how to use a VPN tunnel to connect a client-based remote computer to an internal network. For more about using Mobile Access to connect remote devices to internal resources, see Remote Access to the Network (on page 21).

### VPN Connectivity Modes

The IPsec VPN Software Blade lets the Firewall overcome connectivity challenges for remote clients. Use VPN connectivity modes to make sure that remote users can connect to the VPN tunnels. These are some examples of connectivity challenges:

- The IP addresses of a remote access client might be unknown
- The remote access client can be connected to a hotel LAN with internal IP addresses
- It is necessary for the remote client to use protocols that are not supported

#### Office Mode

Remote users can be assigned the same or non-routable IP addresses from the local ISP. Office Mode solves these routing problems and encapsulates the IP packets with an available IP address from the internal network. Remote users can send traffic as if they are in the office and do not have VPN routing problems.

#### Visitor Mode

Remote users can be restricted to use HTTP and HTTPS traffic only. Visitor Mode lets these users tunnel all protocols with a regular TCP connection on port 443.
Sample Remote Access VPN Workflow

Use SmartDashboard to enable and configure the Security Gateway for remote access VPN connections. Then add the remote user information to the Security Management server: create and configure an LDAP Account Unit or enter the information in the SmartDashboard user database. You can also configure the Firewall to authenticate the remote users. Define the Firewall access control and encryption rules. Create the LDAP group or user group object that is used for the Firewall rules. Then create and configure the encryption settings for the VPN community object. Add the access rules to the Firewall Rule Base to allow VPN traffic to the internal networks.
Chapter 5

Adding Users to the Security Policy

In This Chapter

Using Identity Awareness 39
Using User Directory 44
Adding Users to the Rule Base 48

Using Identity Awareness

The Identity Awareness Software Blade lets you configure the Firewall to enforce access control for individual users and groups. You can use Identity Sources to get information about users and groups to create flexibility and additional security for the Rule Base. Identity Awareness lets you create rules that are for the specified users for these Rule Bases:

- Firewall
- URL Filtering and Application Control
- DLP
- Anti-Bot

For more about using Identity Awareness, see the R76 Identity Awareness Administration Guide.

Identity Sources

After the Security Gateway acquires the identity of a user, user-based rules can be enforced on the network traffic. Identity Awareness can use these sources to identify users:

- **AD Query** - Seamlessly queries the AD (Active Directory) servers to get user information.
- **Browser-Based Authentication** - Uses a Captive Portal to authenticate users.
- **Identity Agent** - Client that is installed on endpoint computers connects to a Security Gateway and authenticates users.
- **Terminal Servers Identity Agent** - An agent on a Terminal or Citrix server connects to a Security Gateway to get user information.
- **Remote Access Devices** - Use Identity Awareness with the Mobile Access and VPN Software Blades (Office Mode only) to authenticate users that connect from a remote device.

AD Query

The Security Gateway registers to receive security event logs from the AD domain controllers when the security policy is installed. When a user authenticates with AD credentials, these event logs are generated and are sent to the Security Gateway. The Firewall identifies the user based on the AD security event log. The user sends traffic that matches an Identity Awareness rule in the security policy. The Firewall can enforce the user-based rule on the traffic.
Browser-Based Authentication

Browser-Based Authentication uses the Internet browser to identify users. You can use these Browser-Based Authentication solutions:

- Captive Portal
- Transparent Kerberos Authentication

Captive Portal uses a web interface to authenticate users before they can access network resources. When users try to access a protected resource, they must log in to a web page to continue.

When Transparent Kerberos Authentication is enabled, the Transparent Authentication page tries to authenticate users before the Captive Portal opens. The Transparent Authentication page communicates with the AD to use the Kerberos protocol to authenticate the users. If the users are successfully authenticated, then they can access the network resources. If they are not authenticated, then they are redirected to the Captive Portal.

Enabling Identity Awareness

There is an Identity Awareness configuration wizard in SmartDashboard that helps you enable and configure the Identity Awareness Software Blade. You can use the configuration wizard on these identity sources:

- AD Query
- Browser-Based Authentication
- Terminal Servers

Using the Identity Awareness Wizard

The Identity Awareness Configuration wizard configures how the Security Gateway gets information about users and computers.

This section gives an example of how to configure the AD query and browser-based methods for Identity Awareness.

To use the configuration wizard:

1. From the Network Objects tree, double-click the Security Gateway. The Gateway Properties window opens.
2. From the navigation tree, click General Properties.
4. Select **AD Query** and **Browser-Based Authentication** and then click **Next**.
   The **Integration With Active Directory** window opens.
5. Select the AD domain and enter the **Username** and **Password**.
   Make sure that the AD account has domain administrator privileges.
6. Click **Connect**.
   The **Successfully connected** message is shown.
7. Click **Next**.
   The **Browser-Based Authentication Settings** window opens.
8. Enter the URL for the Captive Portal and then click **Next**.
   The **Identity Awareness is Now Active** window opens.
9. Click **Finish** and then install the policy.

### Identity Awareness and Remote Access

Identity Awareness for Mobile Access and IPSec VPN clients works in Office Mode for Security Gateways. The Remote Access option is included as an identity source when you enable Identity Awareness.

**To enable or disable Remote Access for Identity Awareness:**
1. From the **Network Objects** tree, double-click the Security Gateway.
   The **Gateway Properties** window opens.
2. From the navigation tree, click **Identity Awareness**.
3. Select or clear **Remote Access**.
4. Click **OK** and then install the policy.

### Creating a New AD Object

The Identity Awareness configuration wizard helps you create a new AD (Active Directory) LDAP Account Unit object in SmartDashboard. Enter the AD settings in the **Integration with Active Directory** window.

**To create new AD Account Unit with the Identity Awareness wizard:**
1. From the **Integration with Active Directory** window, select **Create new domain**.

   ![Integration With Active Directory](image)

   2. Enter the settings for the AD domain controller.
   3. Click **Connect**.
      SmartDashboard connects to the AD server.
   4. Click **Next** and then follow the instructions and finish the wizard.
      SmartDashboard creates the new AD Account Unit.
**Creating Access Roles**

After you enable Identity Awareness, you can create access role objects.

Access role objects define users, machines and network locations as one object. The access role can be for one or more users, networks and machines. You can select specified users, user groups or user branches.

**To create an access role:**

1. Select Users and Administrators in the Objects Tree.
   
   The Access Role window opens.

3. Enter a Name and Comment (optional) for the access role.
4. In the Networks tab, select one of these:
   - Any network
   - Specific networks - Click the plus sign and select a network.
     
     Your selection is shown in the Networks node in the Role Preview pane.

5. In the Users tab, select one of these:
   - Any user
   - All identified users - Includes users identified by a supported authentication method (internal users, AD users or LDAP users).
   - Specific users - Click the plus sign.
     
     A window opens. You can search for Active Directory entries or select them from the list.

6. In the Machines tab, select one of these:
   - Any machine
   - All identified machines - Includes machines identified by a supported authentication method (AD).
   - Specific machines - Click the plus sign.
     
     You can search for AD entries or select them from the list.

7. Optional: For computers that use Full Identity Agents, from the Machines tab select Enforce IP spoofing protection.
8. Click OK.

   The access role is added to the Users and Administrators tree.
Using Identity Awareness in the Firewall Rule Base

The Identity Awareness Software Blade lets you customize the Firewall for users regardless of what computer they are using. Use Access Role objects in a rule and Identity Awareness identifies users that match the rule. You can also enable an **Accept** action to redirect traffic from an unidentified user to a Captive Portal.

Sample Firewall Workflow with Identity Awareness

The Firewall inspects traffic that starts from a source that matches the Access Role object. The Identity Awareness source tries to identify the user.

- If the user is identified, the traffic is allowed.
- If the user is not identified, the traffic is only allowed when the user authenticates to the Captive Portal. If Captive Portal is not enabled, or the user does not authenticate, then the traffic is dropped.

Redirecting to a Captive Portal

You can configure rules that use an Access Role object and an **Accept** action, to redirect HTTP traffic to a Captive Portal. The rule allows traffic when the users for the Access Role are identified. If the Captive Portal action is enabled, these are the procedures for the Firewall to identify a user:

- The Identity Awareness source identifies the user
- The user authenticates at the Captive Portal

Rules can redirect HTTP traffic according to these parameters:

- **Source** - Includes an Access Role object
- **Action** - Uses **Accept**

To enable Captive Portal for a rule:

1. Right-click the **Action** cell and select **Edit Properties**. The **Action Properties** window opens.
2. Select the **Redirect http connections to an authentication (captive) portal**.
3. Click **OK**. The **Action** column shows **accept (display captive portal)**.
4. Install the policy.

Sample Identity Awareness Rules

This table shows sample Identity Awareness rules for a Firewall Rule Base. (The **VPN**, **Track** and **Time** columns are not shown. **Track** is set to **Log**, and **VPN** and **Time** are set to **Any**.)

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CEO allow</td>
<td>John_Smith_CEO</td>
<td>Any</td>
<td>Any</td>
<td>Accept Display Captive Portal</td>
</tr>
<tr>
<td>2</td>
<td>HR server allow</td>
<td>HR_Partners</td>
<td>HR_Server</td>
<td>Any</td>
<td>Accept Display Captive Portal</td>
</tr>
<tr>
<td>3</td>
<td>Drop non-identified HR traffic</td>
<td>Any</td>
<td>HR_Server</td>
<td>Any</td>
<td>Drop</td>
</tr>
<tr>
<td>4</td>
<td>Internet access</td>
<td>Guests</td>
<td>Internet_proxy</td>
<td>HTTP and HTTPS proxy</td>
<td>Accept Display Captive Portal</td>
</tr>
</tbody>
</table>
1. **CEO allow** - Allows the CEO, John Smith, to access all the network resources. The CEO is identified by Identity Awareness AD Query or he authenticates to the Captive Portal.

2. **HR server allow** - Allows users that are defined in the HR_Partners Access Role object to access the HR_Server subnet. The HR users are identified by Identity Awareness AD Query or they authenticate to the Captive Portal.

3. **Drop non-identified HR traffic** - Drops all traffic to the HR_Server subnet. All authenticated users were allowed by the earlier rules.

4. **Internet access** - Allows HTTP and HTTPS traffic from the Guests and All_Domain_Users Access Role objects to the Internet. Domain users are identified by Identity Awareness or they authenticate to the Captive Portal. Guests authenticate to the Captive Portal.

### Using User Directory

User Directory lets you integrate LDAP and other external user management servers with Check Point products and security solutions. These are some of the Software Blades that work with User Directory:

- Mobile Access
- Identity Awareness
- Data Loss Prevention

### User Directory Features

- Use LDAP servers to manage user information for the network
- Security Gateways can retrieve CRLs (Certificate Revocation Lists)
- Security Management server can use LDAP information to authenticate users
- High Availability can duplicate and backup user information across multiple LDAP servers
- Create multiple Account Units to work with distributed databases
- Use profiles to support multiple LDAP vendors
- Encrypt User Directory connections

### Deploying User Directory

User Directory integrates the Security Management server and an LDAP server and lets the Security Gateways use the LDAP information.
Adding Users to the Security Policy

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Gateway - Retrieves LDAP user information and CRLs</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway - Queries LDAP user information, retrieves CRLs, and does bind operations for authentication</td>
</tr>
<tr>
<td>3</td>
<td>Security Management server - Uses User Directory to manage user information</td>
</tr>
<tr>
<td>4</td>
<td>LDAP server - Server that holds one or more Account Units</td>
</tr>
</tbody>
</table>

**Creating an Account Unit**

An Account Unit represents branches of user information on one or more LDAP servers. The Account Unit is the interface between the LDAP servers and the Security Management server and Security Gateways.

When you enable the Identity Awareness ("Creating a New AD Object" on page 41) and Mobile Access Software Blades, SmartDashboard opens a configuration wizard. The **Active Directory Integration** window of this wizard can create a new AD Account Unit. After you complete the wizard, SmartDashboard creates the AD object and Account Unit.

**Editing an Account Unit**

Use the **LDAP Account Unit Properties** window to edit an Account Unit or to create one manually.

**To open the LDAP Account Unit Properties window:**

1. In SmartDashboard, select **Manage > Servers and OPSEC Applications**.
   - The **Servers and OPSEC Applications** window opens.
     a) To create a new Account Unit, click **New > LDAP Account Unit**.
     b) To edit an Account Unit, double-click the Account Unit object.
   - The **LDAP Account Unit Properties** window opens.
2. Configure the settings in the applicable tabs.
3. Click OK and then click Close.

**General Tab**

The **General** tab lets you configure how the Security Management server uses the Account Unit. You can select one or more of these options:

- **CRL retrieval** - The Security Management server manages how the CA sends information about revoked licenses to the Security Gateways.
- **User Management** - The Security Management server uses the user information from this LDAP server. Make sure that User Directory is enabled on the Security Management Server.
- **Active Directory Query** - This AD (Active Directory) server is used as an Identity Awareness source. This option is only available if the Profile is set to Microsoft_AD.

LDAP SSO (Single Sign On) is only supported for Account Unit Objects that use User Management.

**To configure the General tab:**
1. Enter the Name for the Account Unit.
2. From Profile, select the LDAP vendor.
3. Enter the prefix or domain for the Account Unit. This value is used when the same user name is used in multiple Account Units.
   - **Prefix** - For servers that do NOT use AD.
   - **Domain** - For AD servers. This value is also necessary for AD Query and SSO.
4. Select one or more of the Account Unit usage options.
5. For LDAP user information that uses non-English languages, select Enable Unicode support.
6. To configure and enable Kerberos SSO for Identity Awareness:
   a) Click Active Directory SSO configuration.
   b) Configure the settings.
   c) Click OK.
7. Configure the other tabs or click OK.

**Servers Tab**

The Servers tab lets you create and manage the LDAP servers that are used by this Account Unit. You can add LDAP server objects or create new ones.

Use the Update Account to All Servers window to configure the login parameters for all the servers for this Account Unit. If the servers use different login information, edit the parameters for each server.

**To configure the login parameters for all the servers:**
1. Click Update Account Credentials.
   - The Update Account to All Servers window opens.
2. Enter the login parameters.
3. Click OK.

**To remove a server from the Account Unit:**
Select the server and click Remove.

**To manage the servers for the Account Unit:**
1. Do one of these actions for the server:
   - To add a server, click Add.
   - To edit a server, select the server and click Edit.
   - The LDAP Server Properties window opens.
2. If necessary, create a new SmartDashboard server object:
   a) Click New.
      - The Host Node window opens.
b) Enter the settings for the LDAP server.

c) Click OK.

3. From Host, select the server object.
4. Configure the settings for the LDAP server.
5. Optional: Click the Encryption tab and configure the SSL encryption settings.
6. Click OK.
7. Configure the other tabs or click OK.

**Objects Management Tab**

The Objects Management tab lets you select which LDAP server object SmartDashboard queries for the applicable connections and users. You can also enable password protection for this object.

**To configure the Objects Management tab:**
1. From Manage objects on, select the LDAP server object.
2. Click Fetch branches.
   - The Security Management server queries and shows the LDAP branches.
3. Optional: Click Add, Edit and Delete to manage the LDAP branches.
4. Optional: Select Prompt for password when opening this Account Unit.
5. From Return entries, configure the number of entries that are stored in the LDAP database.
6. Configure the other tabs or click OK.

**Authentication Tab**

The Authentication tab lets you configure the authentication scheme for the Account Unit. You can use a common group path to optimize group membership queries. One path for all the LDAP group objects is created and only one query is necessary for the group objects.

**To configure the Authentication tab:**
1. Optional: Select Use common group path for queries.
2. Select one or more authentication schemes that are used to authenticate users in this Account Unit.
3. Select the default settings for new LDAP users:
   - User template - Template that you created
   - Default authentication scheme
4. Optional: Select and configure the login failure settings.
5. For IKE users in this Account Unit, enter the pre-shared secret key.
6. Configure the other tabs or click OK.

**Enabling User Directory**

Configure SmartDashboard to enable the Security Management server to manage users in the Account Unit. You cannot use the SmartDashboard User Database when the User Directory LDAP server is enabled.

For more about using the SmartDashboard User Database, see the R76 Security Management Administration Guide.

**To enable User Directory on the Security Management server:**
   - The User Directory page opens.
3. Configure other login and password settings.
4. Click OK.
5. Make sure that the User Directory Software Blade is enabled.
   a) From the Network Objects tree, double-click the Security Management server object.
   b) Click Management and make sure that Network Policy Management and User Directory are selected.
6. Click OK and install the policy.

**Managing LDAP Information**

User Directory lets you use SmartDashboard to manage information about users and OUs (Organizational Units) that are stored on the LDAP server.

**To manage LDAP information from SmartDashboard:**
1. From the objects tree, select **Users and Administrators**.
2. Double-click the Account Unit.
   The LDAP domain is shown.
3. Double-click the LDAP branch.
   The Security Management server queries the LDAP server and SmartDashboard shows the LDAP objects.
4. Expand the **Objects List** pane.

5. Double-click the LDAP object.
   The **Objects List** pane shows the user information.
6. Right-click a user and select **Edit**.
   The **LDAP User Properties** window opens.
7. Edit the user information and settings and then click **OK**.

**Adding Users to the Rule Base**

Identity Awareness and User Directory let you create rules for specified users, groups or OUs. Identity Awareness uses Access Roles that can put together users, networks gateways and other objects into a single SmartDashboard object that you can add to a rule. User Directory integrates an LDAP server and you can easily update SmartDashboard with user information.

**Adding an Access Role to a Rule**

Security Gateways that use the Identity Awareness Software Blade can add an Access Role as the **Source** or **Destination** of a rule. You can add SmartDashboard objects and LDAP information to the Access Role ("Creating Access Roles" on page 42) object and then use that object in the Firewall, URL Filtering, and Application Control Rule Base.

**Note** - Rules that use Access Role objects are enforced only on Security Gateways that have Identity Awareness enabled.
To add an Access Role to a rule:

1. From the Policy page, click the plus sign in a Source or Destination cell. The SmartDashboard window opens.

2. From the drop-down menu, select Access Roles.

3. Click the Access Role and it is added to the cell.

4. Install the policy.
Chapter 6

Defining an Internet Access Policy

In This Chapter

Managing URL Filtering and Application Control 50
HTTPS Inspection 55

Managing URL Filtering and Application Control

Today there are many challenges for businesses to keep up with security requirements of social media and Web 2.0 applications. It is necessary for system administrators to use the security policy to overcome these challenges. For example:

- **Malware threats** - Popular applications like Twitter, Facebook, and YouTube can cause users to download viruses unintentionally. When users download files and use torrents, they can also let malware into your network.
- **Bandwidth hogging** - Applications that use a lot of bandwidth can reduce the performance for important business applications.
- **Loss of productivity** - Employees can spend time on social networking and other applications that can decrease business productivity.
- **Content control** - Prevent Internet access to websites with inappropriate content, such as sex, violence, and alcohol.

For more about using Application Control and URL Filtering, see the R76 Application Control and URL Filtering Administration Guide.

The Check Point Solution for Internet Browsing

The Check Point Firewall can use the URL Filtering and Application Control Software Blades to monitor and control how organizations of all sizes use the Internet. You can easily create policies which identify or block thousands of applications and Internet sites. These Software Blades help complete the security policy for your organization.

Use URL Filtering and Application Control to:

- **Create a Granular Policy** - Make rules to allow or block applications and Internet sites for individual applications, categories, and risk levels. You can also create an HTTPS policy that enables the Security Gateway to inspect HTTPS traffic to prevent security risks related to the SSL protocol.
- **Manage Bandwidth Consumption** - Configure the rules to limit the available network bandwidth for specified users or groups. You can make separate limits for uploading and downloading.
- **Keep Your Policies Updated** - The Application Database is updated regularly and makes sure that your Internet security policy has the newest applications and website categories. The Security Gateway connects to the Check Point Online Web Service to identify new social networking widgets and website categories for URLs.
- **Communicate with Users** - UserCheck objects add flexibility to URL Filtering and Application Control and let the Security Gateway communicate with users. UserCheck helps users understand that certain websites are against the company's security policy. It also tells users about the changing Internet policy for websites and applications.
- **Create Custom Objects** - In addition to the hundreds of default objects, create new objects to manage Internet use for your network. You can create objects for applications, websites, categories and groups. Use these custom objects in rules to meet your organization's requirements.
**UserCheck**

UserCheck works with the URL Filtering and Application Control Software Blades and lets the Security Gateway send messages to users about possible non-compliant or dangerous Internet browsing. Create rules and UserCheck objects in the URL Filtering and Application Control Rule Base to communicate with the users. These actions use UserCheck objects:

- Inform
- Ask
- Block

**UserCheck on a Security Gateway**

You can enable UserCheck on Security Gateways that use URL Filtering and Application Control Software Blades. When UserCheck is enabled, the user's Internet browser shows the UserCheck messages in a new window.

**UserCheck on a computer**

The UserCheck client is installed on endpoint computers. This client:

- Sends messages for applications that are not based on Internet browsers. For example: Skype, iTunes, and Internet browser add-ons and plug-ins.
- Shows a message on the computer when it cannot be shown in the Internet browser.

**Enabling URL Filtering and Application Control**

You can enable Application Control and URL Filtering Software Blades from the General Properties page in SmartDashboard.

**To enable URL Filtering and Application Control:**

1. In SmartDashboard, double-click the Security Gateway. The Gateway Properties window opens.
2. From the navigation tree, click General Properties.
3. From the Network Security tab, select URL Filtering, Application Control or both.
4. Click OK and install the policy.

**Using the URL Filtering and Application Control Rule Base**

A strong security policy uses firewall rules to inspect packets, and URL Filtering and Application Control rules to control Internet browsing. SmartDashboard has a different Rule Base that manages URL Filtering and Application Control for a Security Gateway.

![Policy](image)

These are the fields that manage the rules for the URL Filtering and Application Control security policy.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Rule number in the URL Filtering and Application Control Rule Base.</td>
</tr>
<tr>
<td>Hits</td>
<td>Number of connections that match this rule.</td>
</tr>
<tr>
<td>Name</td>
<td>Name that the system administrator gives this rule.</td>
</tr>
<tr>
<td>Source</td>
<td>Network object that defines where the traffic starts.</td>
</tr>
<tr>
<td>Destination</td>
<td>Network object that defines the destination of the traffic.</td>
</tr>
<tr>
<td>Applications/Sites</td>
<td>Applications or web sites that are allowed or blocked.</td>
</tr>
<tr>
<td>Action</td>
<td>Action that is done when traffic matches the rule. Options include: <strong>Allow</strong>, <strong>Block</strong>, <strong>Limit</strong> (control the bandwidth) and <strong>Inform</strong> (UserCheck message).</td>
</tr>
<tr>
<td>Track</td>
<td>Tracking and logging action that is done when traffic matches the rule.</td>
</tr>
<tr>
<td>Install On</td>
<td>Network objects that will get the rule(s) of the policy.</td>
</tr>
<tr>
<td>Time</td>
<td>Time period that this rule is enforced.</td>
</tr>
<tr>
<td>Comment</td>
<td>An optional field that lets you summarize the rule.</td>
</tr>
</tbody>
</table>

**Order of Rule Enforcement**

The Security Gateway applies all the rules in Firewall Rule Base and then applies the URL Filtering and Application Control rules. The rules in the URL Filtering and Application Control Rule Base are sequentially applied to packets. The first rule that matches a packet is applied. There is no Cleanup rule in the URL Filtering and Application Control Rule Base: packets that do not match the rules are allowed.

**Special URL Filtering and Application Control Fields**

Internet browsing is not easily defined into allowed and prohibited categories. Many websites and applications can be used for legitimate business reasons. The rules that control Internet access must be flexible and granular. The URL Filtering and Application Control Rule Base uses these fields to create a strong and flexible security policy:

- Applications/Sites
- Action

**Applications/Sites**

Use the **Applications/Sites** field to define the web applications and sites that are included in the rule. This field can use one or more of these options:

- Web applications
- Web sites
- Internet widgets
- Default categories of Internet traffic
- Custom group or category that you create

**To add an application or site to a rule:**

1. Click **Application and URL Filtering > Policy**.
2. Right-click the **Applications/Sites** cell for the rule and select one of these options:
   - Add Applications/Sites
   - Add Category
The Application viewer window opens.

3. From the Available list, select the applications and sites for the rule.
4. Click OK.

To create a new application or site:
1. Click Application and URL Filtering > Applications/Sites.

2. Click New > Application/Site.
3. Select Application/Sites URLs.
4. Enter a URL and click Add.
   Do this step again for all the URLs.
5. Click Next.

To create a custom category:
1. Click Application and URL Filtering > Applications/Sites.
2. Click New > Application/Site Group.
   The Applications/Sites Group window opens.
3. Enter a Name for the group.
4. Click Add.
   The Application viewer window opens.
5. From the Available list, select the applications and sites for the group.
6. Click OK and then click OK.

Action

Use the Action field to define what occurs to traffic that matches the URL Filtering and Application Control rule. These are the Action options:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>Allows the traffic.</td>
</tr>
<tr>
<td>Block</td>
<td>Blocks the traffic. Shows a UserCheck Block message.</td>
</tr>
<tr>
<td></td>
<td>If no UserCheck object is defined for this action, no message is displayed.</td>
</tr>
<tr>
<td>Limit</td>
<td>Defines the maximum bandwidth that is allowed for this rule. Select or create a Limit object that defines the bandwidth limits.</td>
</tr>
<tr>
<td>Captive Portal</td>
<td>Redirects HTTP traffic to an authentication (captive) portal. Once the user is authenticated, new connections from this source are inspected but are not redirected.</td>
</tr>
</tbody>
</table>
### Defining an Internet Access Policy

#### Rule Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Rule</td>
<td>Creates a new rule Above or Below the selected rule.</td>
</tr>
<tr>
<td>Delete Rule</td>
<td>Deletes the selected rule or rules.</td>
</tr>
<tr>
<td>Disable Rule</td>
<td>The rule stays in the Rule Base but is not active.</td>
</tr>
<tr>
<td>Select All Rules</td>
<td></td>
</tr>
<tr>
<td>View rule logs in SmartView Tracker</td>
<td>Opens SmartView Tracker and shows logs related to the rule.</td>
</tr>
<tr>
<td>View rule logs in SmartEvent</td>
<td>Opens SmartEvent and shows logs related to the rule.</td>
</tr>
</tbody>
</table>

#### UserCheck Actions

These are the Action options work with the UserCheck feature:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ask</td>
<td>Shows a UserCheck Ask message. The message asks users to confirm that it is necessary that they to the application or site.</td>
</tr>
<tr>
<td>Block</td>
<td>Blocks the traffic. Shows a UserCheck Block message. If no UserCheck object is defined for this action, no message is displayed.</td>
</tr>
<tr>
<td>UserCheck Frequency</td>
<td>Defines how often users see the UserCheck message for Ask, Inform, or Block actions.</td>
</tr>
<tr>
<td>UserCheck Scope</td>
<td>Defines if the UserCheck message is shown for a category, application or all traffic that matches the rule.</td>
</tr>
<tr>
<td>Edit UserCheck Message</td>
<td>Opens the UserCheck message in a new window.</td>
</tr>
</tbody>
</table>

### Sample URL Filtering and Application Control Rule Base

This table shows a sample URL Filtering and Application Control Rule Base for a typical policy that monitors and controls Internet browsing. (The Hits and Install On columns are not shown.)

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Applications/ Sites</th>
<th>Action</th>
<th>Track</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Liability sites</td>
<td>Any</td>
<td>Internet</td>
<td>Potential_liability</td>
<td>Blocked Message</td>
<td>Log</td>
<td>Any</td>
</tr>
<tr>
<td>2</td>
<td>High risk applications</td>
<td>Any</td>
<td>Internet</td>
<td>High Risk iTunes</td>
<td>High Risk Block</td>
<td>Log</td>
<td>Any</td>
</tr>
<tr>
<td>3</td>
<td>Allow IT department</td>
<td>IT_Department</td>
<td>Any</td>
<td>Radmin</td>
<td>Allow</td>
<td>Log</td>
<td>Work-Hours</td>
</tr>
<tr>
<td></td>
<td>Remote Admin</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Allow Facebook for HR</td>
<td>HR</td>
<td>Internet</td>
<td>Facebook</td>
<td>Allow Download_1Gbps Down: 1 Gbps</td>
<td>Log</td>
<td>Any</td>
</tr>
<tr>
<td>No.</td>
<td>Name</td>
<td>Source</td>
<td>Destination</td>
<td>Applications/Sites</td>
<td>Action</td>
<td>Track</td>
<td>Time</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------</td>
<td>--------</td>
<td>-------------</td>
<td>--------------------------------------------------------</td>
<td>-----------------</td>
<td>--------</td>
<td>------</td>
</tr>
<tr>
<td>5</td>
<td>Block these categories</td>
<td>Any</td>
<td>Internet</td>
<td>Streaming Media, Social Networking, P2P File Sharing, Remote Administration</td>
<td>Blocked Message</td>
<td>Log</td>
<td>Any</td>
</tr>
<tr>
<td>6</td>
<td>Log all applications</td>
<td>Any</td>
<td>Internet</td>
<td>Any Recognized</td>
<td>Allow</td>
<td>Log</td>
<td>Any</td>
</tr>
</tbody>
</table>

1. **Liability sites** - Blocks traffic to sites and applications in the Potential_liability category. The UserCheck Blocked Message is shown to users and explains why their traffic is blocked.

2. **High risk applications** - Blocks traffic to sites and applications in the High Risk category and blocks the iTunes application. The UserCheck High Risk Block Message is shown to users and tells why their traffic is blocked.

3. **Allow IT department Remote Admin** - Allows the computers in the IT_Department network to use the Radmin application. Traffic that uses Radmin is allowed only during these hours, 8:00 - 18:30.

4. **Allow Facebook for HR** - Allows computers in the HR network to use Facebook. The total traffic downloaded from Facebook is limited to 1 Gbps, there is no upload limit.

5. **Block these categories** - Blocks traffic to these categories: Streaming Media, Social Networking, P2P File Sharing, and Remote Administration. The UserCheck Blocked Message is shown to users and explains why their traffic is blocked.

   The Remote Administration category blocks traffic that uses the Radmin application. If this rule is placed before rule 3, then this rule can also block Radmin for the IT department.

6. **Log all applications** - Logs all traffic that matches any of the URL Filtering and Application Control categories.

**HTTPS Inspection**

HTTPS Internet traffic uses the SSL (Secure Sockets Layer) protocol and is encrypted to give data privacy and integrity. However, HTTPS traffic has a possible security risk and can hide illegal user activity and malicious traffic. The Firewall cannot inspect HTTPS traffic because it is encrypted. You can enable the HTTPS Inspection feature to let the Firewall create new SSL connections with the external site or server. The Firewall is then able to decrypt and inspect HTTPS traffic that uses the new SSL connections.

There are two types of HTTPS Inspection:

- **Outbound HTTPS Inspection** - To protect against malicious traffic that is sent from an internal client to an external site or server.

- **Inbound HTTPS Inspection** - To protect internal servers from malicious requests that start from the Internet or an external network.

The Security Gateway uses certificates and becomes an intermediary between the client computer and the secure web site. All data is kept private in HTTPS Inspection logs. Only administrators with HTTPS Inspection permissions can see all the fields in a log.

For more about configuring HTTPS Inspection, see the *R76 Application Control and URL Filtering Administration Guide*. 

---

**Defining an Internet Access Policy**

Firewall Administration Guide R76 | 55
Inspecting HTTPS Packets

Outbound Connections

Outbound connections are HTTPS connections that start from an internal client and connect to the Internet. The Firewall compares the HTTPS request to the HTTPS Inspection Rule Base. If the request does not match a rule, the packet is not inspected and the connection is allowed.

If the request matches an inspection rule, the Firewall makes sure that the certificate from the server (in the Internet) is valid. The Security Gateway creates a new certificate and uses it for a new HTTPS connection to the server. There are two HTTPS connections, one to the internal client and one to the server. It can then decrypt and inspect the packets according to the Firewall and other Rule Bases. The packets are encrypted again and sent to the destination.

Inbound Connections

Inbound connections are HTTPS connections that start from an external client and connect to an internal server in the DMZ or the network. The Firewall compares the HTTPS request to the HTTPS Inspection Rule Base. If the request does not match a rule, the packet is not inspected and the connection is allowed.

If the request matches an inspection rule, the Firewall uses the certificate for the internal server to create a HTTPS connection with the external client. The Security Gateway creates a new HTTPS connection with the internal server. Since the Firewall has a secure connection with the external client, it can decrypt the HTTPS traffic. The decrypted traffic is inspected according to the Firewall and other Rule Bases.
Using the HTTPS Inspection Rule Base

The HTTPS Inspection Rule Base defines how the Firewall inspects HTTPS traffic. The HTTPS Inspection rules can use the Application Database objects to identify traffic for different websites and applications. For example, to protect the privacy of your users, you can use a rule to ignore HTTPS traffic to banks and financial institutions.

The HTTPS Inspection Rule Base is applied to all the Software Blades that have HTTPS Inspection enabled. Software Blades that can support HTTPS Inspection are:

- Application Control
- URL Filtering
- IPS
- DLP
- Anti-Virus
- Anti-Bot

HTTPS Inspection Rule Base in SmartDashboard

These are the fields that manage the rules for the HTTPS Inspection security policy.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Rule number in the HTTPS Inspection Rule Base.</td>
</tr>
<tr>
<td>Name</td>
<td>Name that the system administrator gives this rule.</td>
</tr>
<tr>
<td>Source</td>
<td>Network object that defines where the traffic starts.</td>
</tr>
<tr>
<td>Destination</td>
<td>Network object that defines the destination of the traffic.</td>
</tr>
<tr>
<td>Services</td>
<td>Type of network service that is inspected or bypassed.</td>
</tr>
<tr>
<td>Site Category</td>
<td>Categories for applications or web sites that are inspected or bypassed.</td>
</tr>
<tr>
<td>Action</td>
<td>Action that is done when HTTPS traffic matches the rule. The traffic is inspected or ignored (Bypass).</td>
</tr>
<tr>
<td>Track</td>
<td>Tracking and logging action that is done when traffic matches the rule.</td>
</tr>
<tr>
<td>Install On</td>
<td>Network objects that will get the HTTPS Inspection rule. You can only select Security Gateways that have HTTPS Inspection enabled.</td>
</tr>
</tbody>
</table>
### Defining an Internet Access Policy

#### Firewall Administration Guide R76

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>The certificate that is used for this rule.</td>
</tr>
<tr>
<td></td>
<td>• Inbound HTTPS inspection - Select the certificate that the internal server uses.</td>
</tr>
<tr>
<td></td>
<td>• Outbound HTTPS inspection - Select the Outbound Certificate object that you are using for the computers in the network.</td>
</tr>
<tr>
<td>Comment</td>
<td>An optional field that lets you summarize the rule.</td>
</tr>
</tbody>
</table>

#### Configuring Security Gateways

This section gives an example of how to configure a Security Gateway to inspect outbound and inbound HTTPS traffic.

**Overview**

1. From the **Global Properties** window for the Security Gateway, enable HTTPS Inspection.
2. Configure the Security Gateway to use the certificate.
   - Outbound Inspection - Generate a new certificate for the Security Gateway.
   - Inbound Inspection - Import the certificate for the internal server.
3. Configure the HTTPS Inspection Rule Base.
4. Install the policy.

#### Enabling HTTPS Inspection

**To enable HTTPS Inspection:**

1. In SmartDashboard, double-click the Security Gateway.
   - The **Gateway Properties** window opens.
2. From the navigation tree, click **HTTPS Inspection**.
3. From **Step 3**, select **Enable HTTP Inspection**.

#### Generating a New Certificate

The Firewall uses a certificate to inspect outbound HTTPS traffic. You can use SmartDashboard to generate a new certificate with a password for the private key. Make sure that you export and distribute the new certificate to the endpoint computers in the network. Computers that do not have the new certificate will show SSL error messages.

**To generate a new certificate for outbound HTTPS Inspection:**

1. Double-click the Security Gateway.
   - The **Gateway Properties** window opens.
2. From the navigation tree, click **HTTPS Inspection**.
3. From **Step 1**, click **Create certificate**.
4. Enter the necessary information:
   - **Issued by (DN)** - Enter the domain name of your organization.
   - **Private key password** - Enter the password that is used to encrypt the private key of the CA certificate.
   - **Retype private key password** - Retype the password.
   - **Valid from** - Select the date range for which the CA certificate is valid.
5. Click **OK**.
6. Export and deploy the certificate to the endpoint computers.
Adding a Certificate

The Firewall uses the internal server certificate to inspect inbound HTTPS traffic to the internal server. Make sure that you have a copy of the internal server certificate and the private key password before you configure inbound HTTPS inspection. The file for the certificate must have a P12 extension.

To add a server certificate for inbound HTTPS inspection:
1. Click the Application and URL Filtering tab > Advanced.
2. Click HTTPS Inspection > Server Certificates.
   The Server Certificates page opens.
3. Click Add.
   The Import Outbound Certificate window opens.
4. Enter the Certificate name.
5. Click Browse and select the certificate file.
6. Enter the Private key password.
7. Click OK.

Configuring HTTPS Inspection Rules

Create different HTTPS Inspection rules for outbound and inbound traffic. The outbound rules use the certificate that was generated for the Security Gateway ("Generating a New Certificate" on page 58). The inbound rules use a different certificate for each internal server ("Adding a Certificate" on page 59). You can also create bypass rules for traffic that is sensitive and is not inspected. Make sure that the bypass rules are at the top of the HTTPS Inspection Rule Base.

Sample Inspection Rule Base

This table shows a sample HTTPS Inspection Rule Base for a typical policy. (The Track and Install On columns are not shown. Track is set to None and Install On is set to Any.)

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Site Category</th>
<th>Action</th>
<th>Blade</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Financial sites</td>
<td>Any</td>
<td>Internet</td>
<td>HTTPS HTTP_HTTPS_</td>
<td>Financial</td>
<td>Bypass</td>
<td>Any</td>
<td>Outbound CA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>proxy</td>
<td>Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Outbound</td>
<td>Any</td>
<td>Internet</td>
<td>HTTPS HTTP_HTTPS_</td>
<td>Any</td>
<td>Inspect</td>
<td>Any</td>
<td>Outbound CA</td>
</tr>
<tr>
<td></td>
<td>traffic</td>
<td></td>
<td></td>
<td>proxy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Inbound</td>
<td>Any</td>
<td>WebCalendar Server</td>
<td>HTTPS</td>
<td>Any</td>
<td>Inspect</td>
<td>Any</td>
<td>WebCalendar Server CA</td>
</tr>
</tbody>
</table>
1. **Financial sites** - Does not inspect HTTPS traffic to websites that are defined in the Financial Services category. This rule uses the Outbound CA certificate.

2. **Outbound traffic** - Inspects HTTPS traffic to the Internet. This rule uses the Outbound CA certificate.

3. **Inbound traffic** - Inspects HTTPS traffic to the network object WebCalendarServer. This rule uses the WebCalendarServer certificate.
IPS

A Check Point Firewall can block traffic based on source, destination and port information. You can increase network security with the IPS Software Blade and analyze traffic for possible risks. The IPS detection engine has multiple defense layers, detects and prevents against known threats, and often protects against future ones.

For example IPS protects against drive-by-downloads, where a user can go to a legitimate web site and unknowingly download malware. The malware can exploit a browser vulnerability that lets it create a special HTTP response that sends the malware to the client. The Firewall allows the HTTP traffic from the web site and the computer is at risk for this malware. IPS protects the computer, it can identify and then block the drive-by-download connection.

For more about using the IPS Software Blade, see the R76 IPS Administration Guide.

IPS Protection Profiles

An IPS protection is a set of rules that lets you define how IPS analyzes network traffic. Create IPS profiles to easily configure one or more protections for groups of Security Gateways. You can customize the profile for the specified protections to identify specified attacks. These profiles can then be applied to the groups of Security Gateways to protect them against those attacks.

To create a new IPS protection profile:
1. In the IPS tab, select Profiles.
2. Click New and select Create New Profile.
The General page of the Profile Properties window opens.

3. Enter the Profile Name.
4. In IPS Mode, select the default action for an IPS protection.
   - Prevent: Protections block traffic that matches the definitions.
   - Detect: Protections log traffic that matches the definitions.
5. In Protections Activation, select if protections are enabled automatically or manually.
6. From the navigation tree, click IPS Policy > Updates Policy.
7. Select the default IPS Mode for new protections that are downloaded: Prevent or Detect.
8. Click OK to create the profile.

**Enabling IPS**

The Enforcing Gateways page in the IPS tab shows all the Security Gateways that the IPS Software Blade is enabled. You can enable IPS on a Security Gateway that has the Firewall Software Blade enabled.

**To enable IPS on a Security Gateway:**
1. From the IPS tab, click Enforcing Gateways.
The **Enforcing Gateways** page opens.

2. Click **Add**.
   The **Assign Profile** window opens.
3. Select a Security Gateway and click **OK**.
   IPS is enabled on the Security Gateway and it is shown in the **Enforcing Gateways** page.
4. Install the policy.

**Using IPS Profiles**

The **Enforcing Gateways** page shows all the Security Gateways that have the IPS Software Blade enabled. From this page, you can open the **Gateway Properties** window and assign an IPS profile to a Security Gateway.

**To assign a profile to a gateway:**

1. In the **IPS** tab, select **Enforcing Gateways**.
2. Select a gateway and click **Edit**.
   The **IPS** page of the **Gateway Properties** window opens.
3. From **Assign profile**, select an IPS profile.
4. Click **OK**.
To show the Security Gateways for a profile:
1. In the IPS tab, select Profiles.
2. Select the IPS profile.
3. Click Actions > Show Protected Gateways.
   The Protected Gateways window opens and shows the Security Gateways that are assigned to the IPS profile.

Adding Network Exceptions

You can configure exceptions for a protection with the Prevent action, so that it does not identify the specified traffic. These are some situations where it is helpful to use exceptions:

- Traffic that is legitimate for some machines or services can match the protection criteria for malware.
- A server that does not comply with RFC standards.

Adding an IPS Exception

To add a new exception:
1. In the IPS tab, select Network Exceptions.
2. Click New.
   The Add/Edit Exception Rule window opens.
3. From Profile, select a profile or Any.
4. From Protection, select the excluded protection(s).
   - Single protection - Click Select and then select the protection.
   - All supported protections - Only protections that support the Network Exceptions feature are excluded.
5. Define the Source and Destination, and Service for the excluded protection.
   - To use a SmartDashboard object, click Manage and then select the object.
   - To enter a value, click IP Address or Port and then enter the value.
6. Define on which Security Gateways this exception is installed. Select one of these options:
   - All R70 gateways
   - Apply this exception and select the Security Gateway object.
7. Click OK and then install the policy.

Browsing IPS Protections

The Protections window lets you quickly see IPS protections and shows a summary of each protection.

To browse IPS protections:
Click the IPS tab and from the navigation tree click Protections.

These columns give information about the IPS protections.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>Name of the protection.</td>
</tr>
<tr>
<td>Severity</td>
<td>Probable severity of a successful attack on your environment.</td>
</tr>
</tbody>
</table>
### Column Description

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidence Level</td>
<td>How confident IPS is that recognized attacks are actually undesirable traffic.</td>
</tr>
<tr>
<td>Performance Impact</td>
<td>How much this protection affects the performance of a Security Gateway.</td>
</tr>
<tr>
<td>Industry Reference</td>
<td>International CVE or CVE candidate name for attack.</td>
</tr>
<tr>
<td>Release Date</td>
<td>Date the protection was released by Check Point.</td>
</tr>
<tr>
<td>Follow Up</td>
<td>Shows if this protection is marked for Follow Up.</td>
</tr>
<tr>
<td>Products</td>
<td>Shows if this protection is enforced by IPS Software Blades or IPS-1 Sensors.</td>
</tr>
<tr>
<td>Supported</td>
<td>Which Security Gateway versions support this protection.</td>
</tr>
<tr>
<td>Has an Exception</td>
<td>Shows if this protection has a network exception.</td>
</tr>
<tr>
<td>&lt;profile_name&gt;</td>
<td>There is a separate column for each IPS Profile. The cell shows the Activation setting for the protection.</td>
</tr>
</tbody>
</table>

### Updating IPS Protections

Check Point is constantly developing and improving its protections against the latest threats. You can manually update the IPS protections and also set a schedule when updates are automatically downloaded and installed.

**Note** - The Security Gateways with IPS enabled only get the updates after you install the policy.

To show the IPS update settings:

Click the **IPS** tab and from the navigation tree click **Download Updates**.

### IPS Update Options

You can use these IPS update options to easily manage new IPS protections:

- **New protections are marked for Follow Up** - New protections can be automatically marked with a flag and are listed on the **Follow Up** page in the **IPS** tab. Click **Configure** to change these settings.

- **Use SmartDashboard Revision Control** - Automatically create a database revision before the IPS protections are updated. You can revert the SmartDashboard database back to the earlier IPS protections. For more information about Database Revision Control, see the **R76 Security Management Administration Guide**.

### Configuring Geo Protections

Geo Protection lets you control network traffic for specified countries. An IP-to-country database connects packet IP addresses to the countries. Configure one set of policies for each Profile to block or allow traffic for one or more countries. Configure a different policy that applies to the other countries. Private IP addresses are allowed unless the other side of the connection is explicitly blocked. Check Point control connections (such as between Security Gateways and the Security Management Server) are always allowed, regardless of the Geo Protection policy.

Configure the Geo Protections for each of the IPS Profiles separately. Policies with a Block action for **Specific** and **Other Countries** are only enabled when the **Profile Action** is set to **Prevent**.
To configure Geo Protection for specified countries:

1. Click the IPS tab and from the navigation tree click Geo Protection. The Geo Protection page opens.

2. Select the IPS Profile and one of these Geo Protection Actions for this Profile:
   - Prevent - The Block actions for these countries are enabled.
   - Detect - All traffic is allowed. Traffic that matches a policy with a Block action is logged.
   - Inactive - Geo Protection is disabled.

3. Optional: Click Exceptions and configure exceptions ("Adding Network Exceptions" on page 64) for the Geo Protection for this Profile.

   a) Click Country and select the country for this policy.
   b) Select the traffic Direction for this country.
   c) From Action, select Block or Allow.
   d) From Track, select a logging option.
      If a connection matches more than one Geo Protection policy, the first policy is logged.
   e) Click OK.

5. Configure the Geo Protection policy for the other countries.
   a) From the drop-down menu, select Block or Allow.
b) From **Track**, select a logging option.

6. Do these steps for all the IPS Profiles.

7. Install the policy.

   We recommend that after some days, you review the Geo Protection logs.

---

**Anti-Bot and Anti-Virus**

**Protecting Networks from Bots**

A *bot* is malicious software that can infect your computer. There are many infection methods, for example:

- Opening attachments that exploit a vulnerability
- Accessing a web site that results in a malicious download

When a bot infects a computer, it:

- Takes control of the computer and neutralizes its Anti-Virus defenses. It is not easy to find bots on your computer, they hide and change how they look to Anti-Virus software.
- Connects to a C&C (Command and Control center) for instructions from cyber criminals. The cyber criminals, or bot herders, can remotely control it and instruct it to do illegal activities without your knowledge. Your computer can do one or more of these activities:
  - Steal data (personal, financial, intellectual property, organizational)
  - Send spam
  - Attack resources (Denial of Service Attacks)
  - Consume network bandwidth and reduce productivity

One bot can often create multiple threats. Bots are frequently used as part of **Advanced Persistent Threats (APTs)** where cyber criminals try to damage individuals or organizations. A botnet is a collection of compromised and infected computers.

The Anti-Bot Software Blade detects and prevents these bot and botnet threats. For more about using the Anti-Bot Software Blade, see the *R76 Anti-Bot and Anti-Virus Administration Guide*.

**Identifying Bot Infected Computers**

The Anti-Bot Software Blade uses these procedures to identify bot infected computers:

- **Identify the C&C addresses used by criminals to control bots**
  These web sites are constantly changing and new sites are added on an hourly basis. Bots can attempt to connect to thousands of potentially dangerous sites. It is a challenge to know which sites are legitimate and which are not.

- **Identify the communication patterns used by each botnet family**
  These communication fingerprints are different for each family and can be used to identify a botnet family. Research is done for each botnet family to identify the unique language that it uses. There are thousands of existing different botnet families and new ones are constantly emerging.

- **Identify bot behavior**
  Identify specified actions for a bot such as, when the computer sends spam or participates in DOS attacks.

Check Point uses the ThreatSpect engine and ThreatCloud repository to find bots based on these procedures.

**Protecting Networks from Viruses**

The Anti-Virus Software Blade inspects connections to the Internet and scans file transfers and downloads to the internal network to find and prevent malware attacks. It also gives pre-infection protection from external malware and malicious servers.
**ThreatSpect Engine and ThreatCloud Repository**

The ThreatSpect engine is a unique multi-tiered engine that analyzes network traffic and correlates information across multiple layers to find bots and other malware. It combines information on remote operator hideouts, unique botnet traffic patterns and behavior to identify thousands of different botnet families and outbreak types.

The ThreatCloud repository contains more than 250 million addresses that were analyzed for bot discovery and more than 2,000 different botnet communication patterns. The ThreatSpect engine uses this information to classify bots and viruses.

The Security Gateway gets automatic binary signature and reputation updates from the ThreatCloud repository. It can query the cloud for new, unclassified IP/URL/DNS resources that it finds.

The layers of the ThreatSpect engine:

- **Reputation** - Analyzes the reputation of URLs, IP addresses and external domains that computers in the organization access. The engine searches for known or suspicious activity, such as a C&C.
- **Signatures** - Detects threats by identifying unique patterns in files or in the network.
- **Suspicious Mail Outbreaks** - Detects infected machines in the organization based on analysis of outgoing mail traffic.
- **Behavioral Patterns** - Detects unique patterns that indicate the presence of a bot. For example, how a C&C communicates with a bot-infected machine.

**Learning about Malware**

The Threat Wiki is an easy to use tool that lets you search and filter the ThreatCloud repository to find more information about identified malware. The Threat Wiki helps you to learn more about malware, you can:

- Filter by category, tag, or malware family
- Search for a malware

**To show the Threat Wiki:**

In the **Anti-Bot and Anti-Virus** tab, click **Threat Wiki**. The **Threat Wiki** page opens.

---

**ThreatSpect Engine and ThreatCloud Repository**

The ThreatSpect engine is a unique multi-tiered engine that analyzes network traffic and correlates information across multiple layers to find bots and other malware. It combines information on remote operator hideouts, unique botnet traffic patterns and behavior to identify thousands of different botnet families and outbreak types.

The ThreatCloud repository contains more than 250 million addresses that were analyzed for bot discovery and more than 2,000 different botnet communication patterns. The ThreatSpect engine uses this information to classify bots and viruses.

The Security Gateway gets automatic binary signature and reputation updates from the ThreatCloud repository. It can query the cloud for new, unclassified IP/URL/DNS resources that it finds.

The layers of the ThreatSpect engine:

- **Reputation** - Analyzes the reputation of URLs, IP addresses and external domains that computers in the organization access. The engine searches for known or suspicious activity, such as a C&C.
- **Signatures** - Detects threats by identifying unique patterns in files or in the network.
- **Suspicious Mail Outbreaks** - Detects infected machines in the organization based on analysis of outgoing mail traffic.
- **Behavioral Patterns** - Detects unique patterns that indicate the presence of a bot. For example, how a C&C communicates with a bot-infected machine.

**Learning about Malware**

The Threat Wiki is an easy to use tool that lets you search and filter the ThreatCloud repository to find more information about identified malware. The Threat Wiki helps you to learn more about malware, you can:

- Filter by category, tag, or malware family
- Search for a malware

**To show the Threat Wiki:**

In the **Anti-Bot and Anti-Virus** tab, click **Threat Wiki**. The **Threat Wiki** page opens.
Examining Anti-Bot and Anti-Virus Protections

The Protections browser shows information about the Anti-Bot and Anti-Virus protections.

To show the Protections browser:

In the Anti-Bot and Anti-Virus tab, click Protections. The lower pane shows a detailed description of the protection type.

<table>
<thead>
<tr>
<th>Protection</th>
<th>Blade</th>
<th>Engine</th>
<th>Known Today</th>
<th>Performance Impact</th>
<th>&lt;Profile Name&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Activity</td>
<td>Anti-Bot</td>
<td>Suspicious Malware</td>
<td>1,490,363</td>
<td>Low</td>
<td>Prevent</td>
</tr>
<tr>
<td>Malicious Activity</td>
<td>Anti-Bot</td>
<td>Signatures</td>
<td>2,715</td>
<td>Low</td>
<td>Prevent</td>
</tr>
<tr>
<td>Reputation-domain</td>
<td>Anti-Bot</td>
<td>Reputation</td>
<td>252,625,383</td>
<td>Low</td>
<td>Prevent</td>
</tr>
<tr>
<td>Reputation-SIP</td>
<td>Anti-Bot</td>
<td>Reputation</td>
<td>96,525,918</td>
<td>Low</td>
<td>Prevent</td>
</tr>
<tr>
<td>Reputation-URL</td>
<td>Anti-Bot</td>
<td>Reputation</td>
<td>202,673,936</td>
<td>Low</td>
<td>Prevent</td>
</tr>
<tr>
<td>Unusual Activity</td>
<td>Anti-Bot</td>
<td>BehavioralPattern</td>
<td>23</td>
<td>Low</td>
<td>Prevent</td>
</tr>
<tr>
<td>URLs with Malware</td>
<td>Anti-Virus</td>
<td>Reputation</td>
<td>993,547</td>
<td>Low</td>
<td>Prevent</td>
</tr>
<tr>
<td>Viruses</td>
<td>Anti-Virus</td>
<td>Signatures</td>
<td>9,154,550</td>
<td>Low</td>
<td>Prevent</td>
</tr>
</tbody>
</table>

File Types

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>Name of the protection type.</td>
</tr>
<tr>
<td>Blade</td>
<td>If the protection is used by the Anti-Bot or Anti-Virus Software Blade.</td>
</tr>
<tr>
<td>Engine</td>
<td>Layer of the ThreatSpect engine that is protecting the network.</td>
</tr>
<tr>
<td>Known Today</td>
<td>Number of known protections.</td>
</tr>
<tr>
<td>&lt;Profile Name&gt;</td>
<td>For each profile, shows the action for each protection:</td>
</tr>
<tr>
<td></td>
<td>- Prevent - Blocks traffic that matches the protection</td>
</tr>
<tr>
<td></td>
<td>- Detect - Allows all traffic and logs traffic that matches the protection</td>
</tr>
<tr>
<td></td>
<td>- Inactive - Protection is disabled</td>
</tr>
</tbody>
</table>

For File Type protections, the File Type layer of the ThreatSpect engine classifies and identifies each type of file. This allows preventing, detecting, and setting a policy according to file type.
Enabling the Anti-Bot and Anti-Virus Software Blades

Enable one or more of these Software Blades on a Security Gateway: Anti-Bot and Anti-Virus.

To enable the Software Blades:

1. In SmartDashboard, right-click the gateway object and select Edit. The Gateway Properties window opens.
2. In Network Security tab, select Anti-Bot, Anti-Virus, or both of them. The Anti-Bot and Anti-Virus First Time Activation window opens.
3. Select one of the activation mode options:
   - According to policy - Enable the Anti-Bot and Anti-Virus Software Blades and use the profile settings in the Anti-Bot and Anti-Virus policy.
   - Detect only - Packets are allowed, but the traffic is logged according to the settings in the Rule Base.
4. Click OK and then install the policy.

Anti-Bot and Anti-Virus Rule Base

There is a different Rule Base for Anti-Bot and Anti-Virus. The Anti-Bot and Anti-Virus rules use the Malware database and network objects. Security Gateways that have Identity Awareness ("Using Identity Awareness" on page 39) enabled can also use Access Role objects as the Protected Scope in a rule. The Access Role objects let you easily make rules for individuals or different groups of users.

The first Anti-Bot or Anti-Virus rule that matches the traffic is applied. There are no implied rules in this Rule Base, all traffic is allowed unless it is explicitly blocked. A rule that is set to the Prevent action, blocks activity and communication for that malware.

When necessary, you can add an exception directly to a rule. The object in the Protected Scope, can have a different Action from the specified Anti-Bot and Anti-Virus rule. Here are some examples of exception rules:

- A profile that only detects protections. You can set one or more of the protections for a user to Prevent.
- The RnD network is included in a profile with the Prevent action. You can set that network to Detect.

Managing the Anti-Bot and Anti-Virus Rule Base

These are the fields that manage the rules for the Anti-Bot and Anti-Virus threat prevention policy.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Rule number in the Rule Base. An exception rule contains the letter E and a digit that represents the exception number. For example, E-2.2 is the second exception for the second rule.</td>
</tr>
<tr>
<td>Name</td>
<td>Name that the system administrator gives this rule.</td>
</tr>
<tr>
<td>Protected Scope</td>
<td>Objects that are protected against bots and viruses. Traffic to and from these objects is inspected even if the objects did not open the connection.</td>
</tr>
</tbody>
</table>
## Field Description

**Protection**
For rules, the value for this field is always **N/A**. The protections are set according the profile in the **Action** field.
For exceptions, set this field to one or more specified protections.

**Action**
For rules, the value for this field is an Anti-Bot and Anti-Virus profile.
For exceptions, set this field to **Prevent** or **Detect**.

**Track**
Tracking and logging action that is done when traffic matches the rule.

**Install On**
Network objects that get this rule. The default setting is **All** and installs the policy on all Security Gateways that have Anti-Bot and Anti-Virus enabled.

### Sample Rule Base

This table shows a sample Anti-Bot and Anti-Virus Rule Base. (The **Install On** column is not shown and is set to **All**.)

<table>
<thead>
<tr>
<th>No.</th>
<th>Name</th>
<th>Protected Scope</th>
<th>Protection</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>High Security</td>
<td>Finance_server</td>
<td>- n/a</td>
<td>High_Security_Profile</td>
<td>Log Packet Capture</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Corporate_internal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Corporate_finance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Malware Rule</td>
<td>Any</td>
<td>- n/a</td>
<td>Recommended_Profile</td>
<td>Log</td>
</tr>
<tr>
<td>E-2.1</td>
<td>RnD Server</td>
<td>Server_1</td>
<td>Backdoor.Win32.Shark.A</td>
<td>Detect</td>
<td>Log</td>
</tr>
<tr>
<td>E-2.2</td>
<td>Users_3</td>
<td>Users_3</td>
<td>Adware.Win32.CashFiesta.A</td>
<td>Detect</td>
<td>Log</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RogueSoftware.Win32.Ackantta.A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Trojan.Win32.Agent.BA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. **High Security** - Traffic for the Finance server and two corporate networks are inspected for bots and viruses according to the settings in the High_Security profile. The traffic is logged and the packets are captured for analysis in SmartView Tracker.

2. **Malware Rule** - All traffic in the network is inspected for bots and viruses according to the settings in the Recommend_Profile.

E-2.1 **RnD Server** - A global exception rule for the Server-1 object, that only detects the Backdoor.Win32.Shark.A protection.

E-2.2 **Users_3** - An exception rule for the Users_3 Access Role, that only detects some protections.

### Anti-Spam

Employees waste more and more time to sort through bulk emails commonly known as spam. The amount of resources (disk space, network bandwidth, CPU) devoted to handling spam also increases from year to year. In addition, unwanted emails continue to grow and can be an unexpected security threat to networks. Cyber-criminals can use emails to let viruses and malware into your network. The Anti-Spam and Mail Software Blade gives system administrators an easy and central tool to eliminate most of the spam that reaches their networks.
These are some of the Anti-Spam features. For more about using Anti-Spam, see the R76 Anti-Bot and Anti-Virus Administration Guide.

Enabling Anti-Spam

Use the Overview page in the Anti-Spam & Mail tab to enable Anti-Spam on a Security Gateway.

To enable Anti-Spam:
1. In the Anti-Spam & Mail tab, select Overview.
2. Click Anti-Spam.
   The Anti-Spam Enforcing Gateways window opens.
3. Select one or more Security Gateways.
4. Click OK.
## Sample Configuration

<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content based Anti-Spam</td>
<td>High protection</td>
<td>Identifies spam based on email content</td>
</tr>
<tr>
<td>IP Reputation Anti-Spam</td>
<td>High protection</td>
<td>Identifies spam based on IP address database of known spammers</td>
</tr>
<tr>
<td>Block List Anti-Spam</td>
<td>Block</td>
<td>Identifies spam based on domains or IP addresses that you define</td>
</tr>
<tr>
<td>Mail Anti-Virus</td>
<td>Block</td>
<td>Scans and filters emails for viruses and other malware</td>
</tr>
<tr>
<td>Zero hour malware protection</td>
<td>Off</td>
<td>Does not scan the Internet to identify and filter new virus email attacks</td>
</tr>
</tbody>
</table>

The **Zero hour malware protection** feature is set to **Off** because enabling the feature has a negative effect on network performance.
Chapter 8

Securing Data

In This Chapter

Overview 74
Enabling DLP 77
DLP Rule Base 78
Analyzing and Tracking DLP 81

Overview

Data is more accessible and transferable today than ever before, and the vast majority of data is sensitive at different levels. Some is confidential simply because it is part of an internal organization and is not meant to be available to the public. Some data is sensitive because of corporate requirements and legal regulations.

The Check Point Data Loss Prevention Software Blade (DLP) lets you use the Firewall to prevent users from sending sensitive data to external networks. DLP helps you implement an automated corporate policy that catches sensitive and protected data before it leaves your organization.

For more about using DLP, see the R76 Data Loss Prevention Administration Guide.

Data Loss Prevention Features

These are the features that the Data Loss Prevention Software Blade uses:

- **UserCheck™** - Lets users handle data loss incidents with automated user notification and the unique Ask User mode. Each person in your organization learns the best practices to prevent future accidental leaks. These are the majority of DLP incidents and they can be handled quickly with the DLP Self Incident Handling Portal or the UserCheck client ("UserCheck" on page 51).

- **MultiSpect™** - Unmatched precision to identify and prevent incidents. DLP uses multi-parameter correlation with different customizable data types and with CPcode.

- **Out of the Box Security** - A rich set of defined data types recognizes sensitive forms, templates and data. DLP has a good out-of-the-box policy to make sure that the data stays in the internal network.

- **Data Owner Auditing** - Data Owners are the users in the organization that control the information and files for their own area or department. They get timely automated notifications and reports that show how their data is being moved. Without Data Owner control, system administrators can frequently be placed in an awkward position between managers and employees.

- **CPcode™** - DLP supports fully customized data identification through the use of CPcode. You can define how email data matches DLP policies and rules.

## Sample DLP Deployment

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External computers and servers in the Internet</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway configured with DLP</td>
</tr>
<tr>
<td>3</td>
<td>Web server in the DMZ</td>
</tr>
<tr>
<td>4</td>
<td>Mail relay in the DMZ</td>
</tr>
<tr>
<td>5</td>
<td>Internal computers</td>
</tr>
<tr>
<td>6</td>
<td>AD or LDAP server</td>
</tr>
<tr>
<td>7</td>
<td>Internal Exchange server with Exchange Security Agent</td>
</tr>
<tr>
<td>8</td>
<td>SmartEvent and SmartView Tracker server</td>
</tr>
<tr>
<td>9</td>
<td>SmartConsoles and Security Management server</td>
</tr>
</tbody>
</table>


2. The Security Gateway uses the built-in data types and rules to supply out-of-the-box Data Loss Prevention. DLP can also use the AD or LDAP server to identify users in the internal organization.

3. The Security Gateway analyzes all traffic from the web and mail server before it goes to the Internet. It catches all traffic containing data and being sent through supported protocols. It scans the traffic, including email attachments, for data that should be protected from being sent to external networks. This data is recognized by protocol, source, destination, and complex data type representations. The Security Gateway can also inspect internal traffic between Microsoft Exchange clients in the organization. The Exchange Security Agent forwards internal emails to DLP.

4. SmartView Tracker and SmartEvent log, track, analyze events, and report incidents that are captured by DLP.
Using a Mail Relay and Mail Server

You can configure the Security Gateway to send email notifications to users and Data Owners. If you are using email notifications, it is necessary for the Security Gateway to access a mail server and a mail relay. We recommend that you use different computers for a mail server and a mail relay. For more about other deployments, see the R76 DLP Administration Guide.

Sample Mail Relay Deployment

In this deployment the Security Gateway with the DLP Software Blade scans emails once, as they are sent from an internal mail server (such as Microsoft Exchange) to a mail relay in the DMZ. The Security Gateway scans the email before it reaches the mail relay. The mail relay can send the allowed emails to internal and external recipients.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External computers and servers in the Internet</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway configured with DLP</td>
</tr>
<tr>
<td>3</td>
<td>Mail relay in the DMZ</td>
</tr>
<tr>
<td>4</td>
<td>Internal mail server</td>
</tr>
<tr>
<td>5</td>
<td>Internal computers</td>
</tr>
</tbody>
</table>

Mail Relay Workflow

1. User at internal computer sends email.
2. Email reaches the internal mail server and is forwarded to the mail relay.
3. Security Gateway intercepts and scans the email.
   - Email matches a **Prevent** rule - email is not forwarded
   - Email matches an **Ask User** rule - User must confirm that the email does not violate the DLP policy to forward it
   - Email matches **Inform User, Detect**, or no rule - email is forwarded
4. The mail relay receives the email from the Security Gateway and sends it to the internal or external recipient.
Enabling DLP

You can configure a DLP rule that sends users to the DLP portal when they send questionable data. This rule lets users decide if they will send data that can potentially violate the security policy.

The DLP portal is a web page that informs users that the specified data is possibly against company policy. If the users **Send** the data, then the action is logged.

⚠️ **Important** - If you are using Data Owners, it is necessary to configure a mail server in the **DLP Portal and Mail Server** window.

**To enable DLP on an existing Security Gateway or cluster:**

1. From the **Network Objects** tree, double-click the Security Gateway. The **General Properties** window opens.
2. In the **Network Security** tab, select **Data Loss Prevention**. The **Data Loss Prevention Wizard** opens.
3. Click **Next**.
   The **Email Domain and Active Directory** page opens.
4. Enter the email domain for your company to let DLP distinguish between internal and external email addresses.
5. **Optional**: To enable the Security Gateway to access user information in an AD, enter the AD user name and password. The Security Gateway accesses information in the definition of **My Organization**.
6. Click **Next**.
   The **My Organization Name** page opens.
7. Enter different names and phrases that are used to identify your organization. DLP uses these names to accurately detect incidents of data loss.
8. Click **Next**.
   The **DLP Portal and Mail Server** page opens.
9. **Optional**: Enable the DLP portal.
   **NOTE**: It is not necessary to enable the DLP portal if UserCheck is enabled.
   a) Select **Activate DLP Portal for Self Incident Handling**.
   b) In **Main URL**, enter the URL for the DLP portal.
10. **Optional**: Enable a mail server to send DLP emails to users about possible DLP incidents.
    a) Select **Mail Server**.
    b) From **Send emails using this mail server**, select a mail server or click **New**.
    c) To create a new mail server, in the **Mail Server** window enter the settings for the mail server and click **OK**.
11. Click **Next**.
    The **Protocols** page opens.
12. Select one or more of these protocols to which the DLP policy applies.
    - **Email**
    - **Web**
    - **File Transfer**
13. Click **Next**.
    The **Data Loss Prevention Blade Setup is Completed** window opens.
14. Click **Finish**.
Adding Data Owners
When DLP incidents are logged, the DLP gateway can send automatic notifications to the Data Owners.

To add Data Owners to a Data Type:
1. In the Data Loss Prevention tab, select Data Types.
2. Double-click a data type.
   The Data Type properties window opens.
3. From the navigation tree, select Data Owners.
4. Click Add.
   The Add Data Owners window opens.
5. Select the user or group who is responsible for this data and click Add.
   If the data owner is not in the list, click New. In the Email Addresses window, enter the name and email address of the data owner (or name a list of email addresses).
6. Add as many data owners as needed.
7. Click OK.

Notifying Data Owners
DLP can send automatic messages to Data Owners for incidents that involve the applicable data types.

To configure Data Owner notification:
1. In the Data Loss Prevention tab, select Policy.
2. Right-click the Track cell of the rule and select Email.
   The Email window opens.
3. Select When data is matched.
   Data Owners are added to the Email Notification list.
4. Optional: Click Add to send notification emails to more users.
5. Use the default notification email message, or click Customize and enter the message.
   The default message is: The Check Point Data Loss Prevention system has found traffic which matches a rule
6. Click OK.

Using DLP with Microsoft Exchange
Internal emails between Microsoft Exchange clients use a proprietary protocol which is not supported by the Security Gateways. To scan internal emails between Microsoft Exchange clients, you must install an Exchange Security Agent on the Exchange Server. The agent sends emails to the Security Gateway for inspection using the SMTP protocol encrypted with TLS. To supply Data Loss Prevention for Microsoft exchange, it is necessary that the Exchange server can communicate with the Security Gateway.

An Exchange Security Agent must be installed on each Exchange Server that sends traffic to the Security Gateway with DLP. Each agent is centrally managed through SmartDashboard and can only send emails to one Security Gateway. If your organization uses Exchange servers for all of its emails, you can also use this setup for scanning all emails.

To use the Exchange Security Agent it is necessary to configure settings in SmartDashboard and on the Exchange server. For more about configuring an Exchange Security Agent, see the R76 DLP Administration Guide.

DLP Rule Base
The rules in the DLP Rule Base are not applied sequentially, all the rules are applied to each data transmission. If the data matches multiple rules, the most restrictive rule is applied. The order from most restrictive to least is:
1. Rule with an exception
2. Action - Prevent
3. Action - Ask User
4. Action - Inform User
5. Action - Detect

### Managing the DLP Rule Base

Use SmartDashboard to easily create and configure DLP rules.

These are the fields that manage the rules for the DLP Rule Base.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flag</td>
<td>Mark a rule to <strong>Follow Up</strong> or <strong>Improve Accuracy</strong>.</td>
</tr>
<tr>
<td>Name</td>
<td>Name of the rule.</td>
</tr>
<tr>
<td>Data</td>
<td>Data type for this rule.</td>
</tr>
<tr>
<td>Source</td>
<td>Users and Administrators object that starts the connection. You can also use an object for a network or email domains. If Identity Awareness is enabled, you can also use Access Roles.</td>
</tr>
<tr>
<td>Destination</td>
<td>Users and Administrators object that completes the connection. You can also use an object for a network or email domains. If Identity Awareness is enabled, you can also use Access Roles.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Type of network protocol for this rule.</td>
</tr>
<tr>
<td>Exceptions</td>
<td>Number of exceptions that allow traffic for this rule.</td>
</tr>
<tr>
<td>Action</td>
<td>DLP action that is done when traffic matches the rule.</td>
</tr>
<tr>
<td>Track</td>
<td>Tracking and logging action that is done when traffic matches the rule.</td>
</tr>
<tr>
<td>Severity</td>
<td>Set the severity level for this rule. Use <strong>Severity</strong> to help filter Data Loss Prevention incidents with SmartEvent.</td>
</tr>
<tr>
<td>Install On</td>
<td>Network objects that will get the rule of the security policy. The <strong>Policy Targets</strong> option installs the rule on all firewall gateways.</td>
</tr>
<tr>
<td>Time</td>
<td>Time period that DLP enforces this rule.</td>
</tr>
<tr>
<td>Category</td>
<td>DLP category for this rule.</td>
</tr>
</tbody>
</table>
**DLP Rule Exceptions**

You can create exceptions for DLP rules. When a data transmission matches a DLP rule with an exception, the data is sent and the rule **Action** is not applied. If the data matches two DLP rules, and only one of the rules has an exception, the rule without exceptions is applied.

**To create an exception for a DLP rule:**

1. In the **Data Loss Prevention** tab, select **Policy**.
   
   The **Policy** window opens and shows the DLP Rule Base.

2. Right-click the **Exceptions** cell for a rule and select **Edit**.
   
   The **Exceptions for Rule** window opens.

3. Click **New Exception**.

4. Configure these settings for the exception:
   
   - **Data** - Data Type
   - **Source**
   - **Destination**
   - **Protocol** - Traffic that is allowed

5. Click **OK** and then install the policy.

**DLP Rule Actions**

For each DLP rule that you create for a data type, you also define what action is to be taken if the rule matches a transmission.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect</td>
<td>The Firewall sends the data. The event is logged in SmartView Tracker and is available for your review and analysis in SmartReporter and SmartEvent. The data and the email itself, or the properties of the transmission if not email, are saved in storage for future reference.</td>
</tr>
<tr>
<td>Inform User</td>
<td>The Firewall sends the data, but the incident is logged and the user is notified.</td>
</tr>
<tr>
<td>Ask User</td>
<td>The Firewall blocks the data and DLP holds it until the user verifies that it should be sent. A notification, usually with a remediation link to the Self Incident Handling portal, is sent to the user. The user decides whether the transmission should be completed or not. The decision itself is logged in SmartView Tracker under the User Actions category. Administrators with full permissions or with the View/Release/Discard DLP messages permission can also decide whether the transmission should be completed or not from SmartView Tracker. This can be useful in the event that a user is not available to make sure if it should be sent.</td>
</tr>
<tr>
<td>Prevent</td>
<td>The Firewall blocks the data. <strong>Note:</strong> Check Point does not recommend using the <strong>Prevent</strong> action as a first choice. The action may prove disruptive. To improve the accuracy of rule matches, set rules to <strong>Prevent</strong> only when you have tested them with the less strict actions over a reasonable amount of time.</td>
</tr>
<tr>
<td>Watermark</td>
<td>Tracks Microsoft Office documents (Word, Excel, or PowerPoint files from Office 2007 and higher) and adds visible watermarks or invisible encrypted text.</td>
</tr>
<tr>
<td></td>
<td>- By default, all rules are created without a watermark action.</td>
</tr>
<tr>
<td></td>
<td>- Watermarks can be created and edited without having to apply them.</td>
</tr>
<tr>
<td></td>
<td>- Once a watermark object is created, it can be reused in multiple rules.</td>
</tr>
</tbody>
</table>
Sample Rule Base
This table shows a sample DLP Rule Base. These are the settings for the columns that are not shown:

- **Source** - My Organization
- **Destination** - Outside My Organization
- **Install On** - DLP Blades
- **Protocol** - Any
- **Time** - Any

<table>
<thead>
<tr>
<th>Flag</th>
<th>Name</th>
<th>Data</th>
<th>Exceptions</th>
<th>Action</th>
<th>Track</th>
<th>Severity</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Follow Up</td>
<td>Salesforce Reports</td>
<td>Salesforce Reports</td>
<td>None</td>
<td>Ask User</td>
<td>Log</td>
<td>High</td>
<td>Business</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Restricted</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Flag</td>
<td>PCI - Credit Card Numbers</td>
<td>PCI - Cardholder Data</td>
<td>None</td>
<td>Prevent</td>
<td>Log</td>
<td>Critical</td>
<td>Compliance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PCI - Credit Card Numbers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Flag</td>
<td>SEC Filings - Draft or Recent</td>
<td>SEC Filings - Draft or Recent</td>
<td>None</td>
<td>Detect</td>
<td>Log</td>
<td>High</td>
<td>Financial</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Email</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Flag</td>
<td>Source Code</td>
<td>Source Code</td>
<td>1</td>
<td>Detect</td>
<td>Alert</td>
<td>High</td>
<td>Intellectual Property</td>
</tr>
</tbody>
</table>

**Salesforce Reports** - When users send data that matches the Salesforce Reports Data Type category, they are asked to confirm the data transmission. A watermark with the word Restricted is added to Microsoft Word, Excel and PowerPoint files. This incident is logged with High severity.

**PCI - Credit Card Numbers** - Users are blocked from sending data that matches the PCI - Cardholder Data, and PCI - Credit Card Numbers Data Type categories. These incidents are logged with Critical severity.

**SEC Filings - Draft or Recent** - Data transmissions that matches the SEC Filings - Draft or Recent Data Type category are logged with High severity. An email is sent to the Data Owners for each incident.

**Source Code** - Data transmissions that matches the Source Code Data Type category are logged with High severity. A pop-up window opens in SmartView Monitor for each incident.

Analyzing and Tracking DLP
To keep a strong Data Loss Prevention policy, it is necessary to do an analysis of DLP incidents. These SmartConsoles can help your DLP analysis:

- SmartView Tracker
- SmartEvent

You can use the Follow Up flag in SmartDashboard for the DLP rules. If you find one or more incidents that you want to change or fine-tune, set the Data Type or rule to Follow Up.

**Note** - To use a Windows 7 computer to view DLP incidents in SmartView Tracker or SmartEvent, Microsoft Office 2010 must be installed. These SmartConsoles do not show DLP incidents, if these EML files are associated with another application.

Using SmartView Tracker
You can open the log of an incident and see the actual data that caused the incident. It is not necessary to review most of the incidents manually, but the data transmission (for example, the email or attachment) is saved.
**Important** - The DLP logs can contain personal emails and web posts that were captured. **You must let the users know** that this can happen. Failure to do so may cause your organization to be in conflict with local privacy laws.

To use SmartView Tracker to analyze DLP:
1. In SmartDashboard, select *SmartConsole > SmartView Tracker*.
2. In the **Network & Endpoint** tab, select *Predefined > Data Loss Prevention Blade*.
3. Double-click a category.

The Data Loss Prevention logs for the category are shown.

---

### DLP Actions

SmartView Tracker actions for DLP incidents include:

<table>
<thead>
<tr>
<th>DLP Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ask User</strong></td>
<td>DLP incident captured and put in Quarantine, user asked to decide what to do.</td>
</tr>
<tr>
<td><strong>Do not Send</strong></td>
<td>User decided to drop transmission that was captured by DLP. An administrator with full permissions or with the View/Release/Discard DLP messages permission can also drop these transmissions. Email notification is sent to the user.</td>
</tr>
<tr>
<td><strong>Send</strong></td>
<td>User decided to continue transmission after DLP notified that it may contain sensitive data. An administrator with full permissions or with the View/Release/Discard DLP messages permission can also decide to continue transmission. Email notification is sent to the user.</td>
</tr>
<tr>
<td><strong>Quarantine Expired</strong></td>
<td>DLP captured data transmission cannot be sent because the user did not make a decision in time. Expired incidents may still be viewed, until they are deleted (routine cleanup process).</td>
</tr>
<tr>
<td><strong>Prevent</strong></td>
<td>DLP transmission was blocked.</td>
</tr>
<tr>
<td><strong>Allow</strong></td>
<td>DLP transmission was allowed; usually by exception to rule.</td>
</tr>
</tbody>
</table>
### DLP General Columns

DLP incidents can show some or all of these columns and are available to all administrators.

<table>
<thead>
<tr>
<th>DLP Columns</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident UID</td>
<td>Unique ID of the incident.</td>
</tr>
<tr>
<td>DLP Action Reason</td>
<td>Reason for the action. Possible values: Rule Base, Internal Error, Prior User Decision</td>
</tr>
<tr>
<td>Related Incident</td>
<td>Internal incident ID related to the current log.</td>
</tr>
<tr>
<td>DLP Transport</td>
<td>Protocol of the traffic of the incident: HTTP, FTP, Email.</td>
</tr>
</tbody>
</table>

#### Using the Incident UID as a key between multiple logs:

Each DLP incident has a unique ID included in the log and sent to the user as part of an email notification. User actions (Send, Do not Send) are assigned the same Incident UID that was assigned to the initial DLP incident log.

If a user/administrator sends an email with a DLP violation and then decides to discard it, two logs are generated. The first log is a DLP incident log with **Ask User** action and is assigned an Incident UID. On the user action, the second log is generated with the same UID, with the **Do not Send** action.

Each matched data type generates its own log. The gateway makes sure that all the data type logs of one incident show the same unique Incident UID and rule action (Prevent, Ask, Inform, or Detect). This happens also if data types were matched on different rules. The same action shown for an incident is the most restrictive.

For example, in a case that a transmission matches two data types. Each data type is used in a different rule. The action of one rule is Prevent. The action in the second rule is Detect. The two logs that are generated will show Prevent as the action. The action implemented will be Prevent. The log of the Detect rule will show **Rule Base (Action set by different rule)** in the DLP Action Reason column.

### DLP Restricted Columns

These columns are restricted to administrators with permissions.

<table>
<thead>
<tr>
<th>Restricted Filters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP Rule Name</td>
<td>Name of the DLP rule on which the incident was matched.</td>
</tr>
<tr>
<td>DLP Rule UID</td>
<td>Internal rule ID of the DLP rule on which the incident was matched.</td>
</tr>
<tr>
<td>Data Type UID</td>
<td>Internal ID of the data type on which the incident was matched.</td>
</tr>
<tr>
<td>Data Type Name</td>
<td>Name of the matched data type.</td>
</tr>
<tr>
<td>User Action Comment</td>
<td>Comment given by user when releasing the incident from the Portal.</td>
</tr>
<tr>
<td>DLP Recipients</td>
<td>For SMTP traffic, list of recipients of captured email.</td>
</tr>
<tr>
<td>Scanned Data Fragment</td>
<td>Captured data itself: email and attachment of SMTP, file of FTP, or HTTP traffic.</td>
</tr>
<tr>
<td>Message to User</td>
<td>Message sent, as configured by administrator, for the rule on which the incident was matched.</td>
</tr>
</tbody>
</table>
### Restricted Filters

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DLP Categories</strong></td>
</tr>
<tr>
<td><strong>DLP Words List</strong></td>
</tr>
<tr>
<td><strong>Mail Subject</strong></td>
</tr>
</tbody>
</table>

## Using SmartEvent

SmartEvent provides advanced analysis tools with filtering, charts, reporting, statistics, and more, of all events that pass through enabled Security Gateways. SmartEvent combines all DLP logs of the same incident (all matching rules and data types and user action if applicable) to a single event. You can filter out the specific Data Loss Prevention information for efficient monitoring and relevant reporting on DLP incidents.

- Real-time and history graphs and reports of Data Loss Prevention incidents
- Graphical incident timelines for rapid information retrieval
- Easily configured custom views to quickly answer specific queries
- Incident management workflow
- Reports to data owners on a scheduled basis

**To open SmartEvent:**

1. In SmartDashboard, select **Window > SmartEvent**.
2. When SmartEvent is open, open **Events**.
3. Select **Predefined > DLP** or any of the analysis data categories under **DLP**.
Chapter 9

Maximizing Network Performance

In This Chapter

Check Point Software Acceleration Solutions 85
CoreXL 85
Using SecureXL 86
Multi-Queue 87

Check Point Software Acceleration Solutions

These are features that you can enable to increase the performance of the Firewall:

- CoreXL
- SecureXL (Performance Pack)

These are software based features that are included in the Check Point operating systems. It is not necessary to purchase additional hardware to use them. You cannot configure CoreXL and SecureXL with SmartDashboard, instead run the applicable commands from the CLI.

For more about configuring CoreXL and SecureXL, see the *R76 Performance Tuning Administration Guide*.

CoreXL

In a Security Gateway with CoreXL enabled, the Firewall kernel is replicated multiple times. Each replicated instance runs on one processing core. These instances handle traffic concurrently and each instance is a complete Firewall kernel that inspects traffic. When CoreXL is enabled, all Firewall instances in the Security Gateway process traffic through the same interfaces and apply the same gateway security policy.

The maximum number of Firewall instances is based on the total number of CPU cores.

<table>
<thead>
<tr>
<th>Number of Cores</th>
<th>Number of Firewall Instances</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>6</td>
</tr>
<tr>
<td>12</td>
<td>10</td>
</tr>
<tr>
<td>More than 12</td>
<td>Open server - 10</td>
</tr>
<tr>
<td></td>
<td>Check Point appliance - Number of cores, minus 2. Maximum number of instances is 14</td>
</tr>
</tbody>
</table>
Configuring CoreXL

Use the `cpconfig` command to open the wizard to enable CoreXL and configure the number of firewall instances.

To enable/disable CoreXL:
1. Log in to the Security Gateway.
2. Run `cpconfig`.
3. Select Configure Check Point CoreXL.
4. Enable or disable CoreXL.
5. Reboot the Security Gateway.

To configure the number of instances:
1. Run `cpconfig`.
2. Select Configure Check Point CoreXL.
3. If CoreXL is enabled, enter the number of firewall instances.
4. If CoreXL is disabled, enable CoreXL and then set the number of firewall instances.
5. Reboot the gateway.

Using SecureXL

SecureXL is an acceleration solution that maximizes performance of the Firewall and does not compromise security. When SecureXL is enabled on a Security Gateway, some CPU intensive operations are processed by virtualized software instead of the Firewall kernel. The Firewall can inspect and process connections more efficiently and accelerate throughput and connection rates. These are the SecureXL traffic flows:

- **Slow path** - Packets and connections that are inspected by the Firewall and are not processed by SecureXL.
- **Accelerated path** - Packets and connections that are offloaded to SecureXL and are not processed by the Firewall.
- **Medium path** - Packets that require deeper inspection cannot use the accelerated path. It is not necessary for the Firewall to inspect these packets, they can be offloaded and do not use the slow path. For example, packets that are inspected by IPS cannot use the accelerated path and can be offloaded to the IPS PSL (Passive Streaming Library). SecureXL processes these packets more quickly than packets on the slow path.

The goal of a SecureXL configuration is to minimize the connections that are processed on the slow path.

Throughput Acceleration

Connections are identified by the 5 tuple attributes: source address, destination address, source port, destination port, protocol. When the packets in a connection match all the 5 tuple attributes, the traffic flow can be processed on the accelerated path.

The first packets of a new TCP connection require more processing and they are processed on the slow path. The other packets of the connection can be processed on the accelerated path and the Firewall throughput is dramatically increased.

Connection-rate Acceleration

SecureXL also improves the rate of new connections (connections per second) and the connection setup/teardown rate (sessions per second). To accelerate the rate of new connections, connections that do not match a specified 5 tuple are still processed by SecureXL.

For example, if the source port is masked and only the other 4 tuple attributes require a match. When a connection is processed on the accelerated path, SecureXL creates a template of that connection that does not include the source port tuple. A new connection that matches the other 4 tuples is processed on the accelerated path because it matches the template. The Firewall does not inspect the new connection and the Firewall connection rates are increased.
**Configuring SecureXL**

SecureXL is enabled by default and you cannot use SmartDashboard to configure it.

**To configure SecureXL:**

1. Log in to the CLI on the Security Gateway.
2. Run `cpconfig`
3. Enter the option that enables or disables SecureXL.
   - For example, `dis`able Check Point SecureXL
4. Enter `y` and then enter `11`.

   **Note** -
   - Run `fwaccel` or `fwaccel6` to dynamically enable or disable SecureXL acceleration for IPv4 or IPv6 traffic
   - This setting does not survive reboot or the Security Gateway

**Multi-Queue**

By default, the traffic for each interface is processed on one CPU core. If there are more CPU cores than interfaces, not all of the CPU cores are used to process traffic.

You can enable the Multi-queue feature to assign more than one CPU core to one interface. Run the `cpmq` command to configure the Multi-queue settings.

The SND (Secure Network Distributer) is part of SecureXL and CoreXL. It processes and helps to accelerate network traffic:

- SecureXL - Distributes traffic to the accelerated or slow path
- CoreXL - Processes traffic on a specified Firewall instance

**Sample Multi-queue Configuration**

This sample configuration shows how CoreXL, SecureXL and Multi-queue can help to use more CPU cores for SNDs to accelerate network traffic. There is a Security Gateway with two six core CPUs (total 12 CPU cores) and three interfaces:

- External
- Internal
- DMZ

<table>
<thead>
<tr>
<th></th>
<th>CPU cores for SND</th>
<th>CPU cores for CoreXL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multi-queue disabled</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>Multi-queue enabled</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>
Chapter 10

Configuring the NAT Policy

In This Chapter

Translating IP Addresses 88
NAT Rule Base 91
Configuring Static and Hide NAT 93
Advanced NAT Settings 98

Translating IP Addresses

NAT (Network Address Translation) is a feature of the Firewall Software Blade and replaces IPv4 and IPv6 addresses to add more security. You can enable NAT for all SmartDashboard objects to help manage network traffic. NAT protects the identity of a network and does not show internal IP addresses to the Internet. You can also use NAT to supply more IPv4 addresses for the network.

The Firewall can change both the source and destination IP addresses in a packet. For example, when an internal computer sends a packet to an external computer, the Firewall translates the source IP address to a new one. The packet comes back from the external computer, the Firewall translates the new IP address back to the original IP address. The packet from the external computer goes to the correct internal computer.

SmartDashboard gives you the flexibility to make necessary configurations for your network:

- Easily enable the Firewall to translate all traffic that goes to the internal network.
- SmartDashboard can automatically create Static and Hide NAT rules that translate the applicable traffic.
- You can manually create NAT rules for different configurations and deployments.

How Security Gateways Translate Traffic

A Security Gateway can use these procedures to translate IP addresses in your network:

- **Static NAT** - Each internal IP address is translated to a different public IP address. The Firewall can allow external traffic to access internal resources.

- **Hide NAT** - The Firewall uses port numbers to translate all specified internal IP addresses to a single public IP address and hides the internal IP structure. Connections can only start from internal computers, external computers CANNOT access internal servers. The Firewall can translate up to 50,000 connections at the same time from external computers and servers.

- **Hide NAT with Port Translation** - Use one IP address and let external users access multiple application servers in a hidden network. The Firewall uses the requested service (or destination port) to send the traffic to the correct server. A typical configuration can use these ports: FTP server (port 21), SMTP server (port 25) and an HTTP server (port 80). It is necessary to create manual NAT rules ("Automatic and Manual NAT Rules" on page 91) to use Port Translation.

Using Hide NAT

For each SmartDashboard object, you can configure the IP address that is used to translate addresses for Hide NAT mode:

- Use the IP address of the external Security Gateway interface
- Enter an IP address for the object
Hide NAT uses dynamically assigned port numbers to identify the original IP addresses. There are two pools of port numbers: 600 to 1023, and 10,000 to 60,000. Port numbers are usually assigned from the second pool. The first pool is used for these services:

- `rlogin` (destination port 512)
- `rshell` (destination port 513)
- `rexec` (destination port 514)

If the connection uses one of these services, and the source port number is below 1024, then a port number is assigned from the first pool.

You cannot use Hide NAT for these configurations:

- Traffic that uses protocols where the port number cannot be changed
- An external server that uses IP addresses to identify different computers and clients

### Sample NAT Deployments

#### Static NAT

Firewalls that do Static NAT, translate each internal IP address to a different external IP address.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External computers and servers in the Internet</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway - Firewall is configured with Static NAT</td>
</tr>
<tr>
<td>3</td>
<td>Internal computers</td>
</tr>
</tbody>
</table>

#### Sample Static NAT Workflow

An external computer in the Internet sends a packet to 192.0.2.5. The Firewall translates the IP address to 10.10.0.26 and sends the packet to internal computer A. Internal computer A sends back a packet to the external computer. The Firewall intercepts the packet and translates the source IP address to 192.0.2.5.

Internal computer B (10.10.0.37) sends a packet to an external computer. The Firewall intercepts the packet translates the source IP address to 192.0.2.16.
Configuring the NAT Policy

### Hide NAT

Firewalls that do Hide NAT use different port numbers to translate internal IP address to one external IP address. External computers cannot start a connection to an internal computer.

#### Sample Hide NAT Workflow

Internal computer A (10.10.0.26) sends a packet to an external computer. The Firewall intercepts the packet and translates the source IP address to 192.0.2.1 port 11000. The external computer sends back a packet to 192.0.2.1 port 11000. The Firewall translates the packet to 10.10.0.26 and sends it to internal computer A.
NAT Rule Base

The NAT Rule Base has two sections that specify how the IP addresses are translated:

- Original Packet
- Translated Packet

Each section in the NAT Rule Base is divided into cells that define the Source, Destination, and Service for the traffic.

Automatic and Manual NAT Rules

There are two types of NAT rules for network objects:

- Rules that SmartDashboard automatically creates and adds to the NAT Rule Base
- Rules that you manually create and then add to the NAT Rule Base

When you create manual NAT rules, it can be necessary to create the translated NAT objects for the rule.

Using Automatic Rules

You can enable automatic NAT rules for these SmartDashboard objects:

- Security Gateways
- Nodes
- Networks
- Address Ranges

SmartDashboard creates two automatic rules for Static NAT to translate both the source and destination of the packets. One rule is created for Hide NAT to translate the source of the packets.

For network and address range objects, SmartDashboard creates a different rule to NOT translate intranet traffic. IP addresses for computers on the same object are not translated.

This table summarizes the NAT automatic rules:
## Configuring the NAT Policy

<table>
<thead>
<tr>
<th>Type of Traffic</th>
<th>Static NAT</th>
<th>Hide NAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal to external</td>
<td>Rule translates source IP address</td>
<td>Rule translates source IP address</td>
</tr>
<tr>
<td>External to internal</td>
<td>Rule translates destination IP address</td>
<td>N/A (External connections are not allowed)</td>
</tr>
<tr>
<td>Intranet (for network and address range objects)</td>
<td>Rule does not translate IP address</td>
<td>Rule does not translate IP address</td>
</tr>
</tbody>
</table>

### Order of NAT Rule Enforcement

The Firewall enforces the NAT Rule Base in a sequential manner. Automatic and manual rules are enforced differently. Automatic rules can use bidirectional NAT to let two rules be enforced for a connection.

- **Manual rules** - The first manual NAT rule that matches a connection is enforced. The Firewall does not enforce a different NAT rule that can be more applicable.

- **Automatic rules** - Two automatic NAT rules that match a connection, one rule for the *Source* and one for the *Destination* can be enforced. When a connection matches two automatic rules, those rules are enforced.

SmartDashboard organizes the automatic NAT rules in this order:

1. Static NAT rules for Firewall, or node (computer or server) objects
2. Hide NAT rules for Firewall, or node objects
3. Static NAT rules for network or address range objects
4. Hide NAT rules for network or address range objects

### Sample Automatic Rules

#### Static NAT for a Network Object

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Original Packet</th>
<th>Destination</th>
<th>Service</th>
<th>Translated Packet</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sales</td>
<td>Sales</td>
<td>HR</td>
<td>Any</td>
<td>Original</td>
<td>All</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>HR (Valid Addr)</td>
<td>Any</td>
<td>Any</td>
<td>HR (Valid Addr)</td>
<td>All</td>
</tr>
</tbody>
</table>

1. Intranet connections in the HR network are not translated. The Firewall does not translate a connection between two computers that are part of the HR object.

   The Firewall does not apply rules 2 and 3 to traffic that matches rule 1.

2. Connections from IP addresses from the HR network to any IP address (usually external computers) are translated to the Static NAT IP address.

3. Connections from any IP address (usually external computers) to the HR are translated to the Static NAT IP address.

#### Hide NAT for Address Range

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Original Packet</th>
<th>Destination</th>
<th>Service</th>
<th>Translated Packet</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sales</td>
<td>Sales</td>
<td>Any</td>
<td>Any</td>
<td>Sales (Hiding A)</td>
<td>All</td>
</tr>
<tr>
<td>2</td>
<td>Any</td>
<td>Sales</td>
<td>Any</td>
<td>Any</td>
<td>Sales (Hiding A)</td>
<td>All</td>
</tr>
</tbody>
</table>

1. Intranet connections in the Sales address range are not translated. The Firewall does not translate a connection between two computers that use IP addresses that are included in the Sales object.

   The Firewall does not apply rule 2 to traffic that matches rule 1.
2. Connections from IP addresses from the Sales address range to any IP address (usually external computers) are translated to the Hide NAT IP address.

Configuring Static and Hide NAT

Use the NAT page in the Gateway Properties window to enable and configure NAT for SmartDashboard objects.

Configuring Static NAT

When you enable Static NAT, each object is translated to a different IP address. SmartDashboard can automatically create the NAT rules, or you can create them manually.

Configuring Hide NAT

Hide NAT uses different port numbers to identify the internal IP addresses. When you enable Hide NAT mode, the Firewall translates the IP address to:

- The IP address of the external Security Gateway interface
- The IP address for the object

**Note** - You cannot use Hide NAT for these configurations:
- Traffic that uses protocols where the port number cannot be changed
- An external server that uses IP addresses to identify different computers and clients

Enabling Automatic NAT

SmartDashboard can automatically create and configure the NAT rules for a network. Enable automatic NAT for each object that you are translating the IP address. Then configure the Firewall Rule Base to allow traffic to the applicable objects.

To enable automatic NAT:

1. Double-click the SmartDashboard object.
   The General Properties window opens.
2. Click NAT.
3. Select Add Automatic Address Translation rules.
4. Configure the automatic NAT settings.
   a) Select the Translation method: Hide or Static.
   b) Configure the NATed IP address for the object.
      - Hide behind Gateway - Use the Security Gateway IP address.
      - Hide behind IP address - Enter the IP address.
   c) Click Install on Gateway and select All or the Security Gateway that translates the IP address.
5. Click OK.
6. Do these steps for all the applicable objects.
7. Click Firewall > Policy.
   The Policy page opens and shows the Firewall Rule Base.
8. Add rules that allow traffic to the applicable objects.
9. Install the policy.

Automatic Hide NAT to External Networks

For large and complex networks, it can be impractical to configure the Hide NAT settings for all the internal IP addresses. An easy alternative is to enable a Firewall to automatically Hide NAT for all traffic with external networks. The Firewall translates all traffic that goes through an external interface to the valid IP address of that interface.
In this sample configuration, computers in internal networks open connections to external servers on the Internet. The source IP addresses of internal clients are translated to the IP address of the external interface.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External computers and servers in the Internet</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway - Firewall is configured with automatic Hide NAT. There are two external interfaces 192.0.2.1 and 192.0.2.100.</td>
</tr>
<tr>
<td>3</td>
<td>Internal computers</td>
</tr>
</tbody>
</table>

The source IP address is translated to the applicable external interface IP address: 192.0.2.1 or 192.0.2.100.

Note - If a connection matches a regular NAT rule and a NAT-for-internal-networks rule, the regular NAT rule takes precedence.

**To enable automatic Hide NAT:**
2. From the navigation tree, click NAT. The NAT page opens.
3. Select Hide internal networks behind the Gateway's external IP.
4. Click OK and then install the policy.

**Enabling Manual NAT**

For some deployments, it is necessary to manually define the NAT rules. Create SmartDashboard objects that use the valid (NATed) IP addresses. Create NAT rules to translate the original IP addresses of the objects to valid IP addresses. Then configure the Firewall Rule Base to allow traffic to the applicable translated objects with these valid IP addresses.

Note - For manual NAT rules, it is necessary to configure proxy ARPs to associate the translated IP address ("Automatic and Proxy ARP" on page 98).

These are some situations that must use manual NAT rules:
- Rules that are restricted to specified destination IP addresses and to specified source IP addresses
- Translate both source and destination IP addresses in the same packet.
- Static NAT in only one direction
- Translate services (destination ports)
• Rules that only use specified services (ports)
• Translate IP addresses for dynamic objects

This procedure explains how to configure manual Static NAT for a web server. You can also configure manual Hide NAT for SmartDashboard objects ("Sample Deployment (Manual Rules for Port Translation)" on page 96).

**To enable manual Static NAT:**

1. Right-click the object in SmartDashboard and select **Clone**. The **General Properties** window of the new object opens.
2. Enter the **Name**. We recommend that you name the object `<name>_valid_address`.
3. Enter the NATed IP address.
4. Click **OK**.
5. Click **Firewall > NAT**. The **NAT** page opens and shows the NAT Rule Base.
6. Add a manual rule above the automatic NAT rules.
7. Configure the manual rule to translate the IP address. For example:
   • Original Packet Source - **WebServer**
   • Translated Packet Source - **WebServer_valid_address**
8. Click **Firewall > Policy**. The **Policy** page opens and shows the Firewall Rule Base.
9. Add rules that allow traffic to the applicable NATed objects.
   These objects are the cloned objects that are called `<name>_valid_address`.
10. Install the policy.

**Sample Deployment (Static and Hide NAT)**

The goal for this sample deployment is to configure:

• Static NAT for the SMTP and the HTTP servers on the internal network. These servers can be accessed from the Internet using public addresses.

• Hide NAT for the users on the internal network that gives them Internet access. This network cannot be accessed from the Internet.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External computers and servers in the Internet</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway (External interface 2001:db8::a:1)</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>3</td>
<td>Internal computers (Alaska_LAN 2001:db8::/64)</td>
</tr>
</tbody>
</table>

**To configure NAT for the network:**

1. Enable automatic Static NAT for the web server.
   a) Double-click the Alaska.Web object and select **NAT**.
   b) Select **Add Automatic Address Translation Rules**.
   c) In **Translation method**, select **Static**.
   d) Select **Hide behind IP Address** and enter 2001:db8::a:5.
   e) Click **OK**.

2. Enable automatic Static NAT for the mail server.
   a) Double-click the Alaska.Mail object and select **NAT**.
   b) Select **Add Automatic Address Translation Rules**.
   c) In **Translation method**, select **Static**.
   d) Select **Hide behind IP Address** and enter 2001:db8::a:6.
   e) Click **OK**.

3. Enable automatic Hide NAT for the internal computers.
   a) Double-click the Alaska_LAN object and select **NAT**.
   b) Select **Add Automatic Address Translation Rules**.
   c) In **Translation method**, select **Hide**.
   d) Select **Hide behind Gateway**.

4. Click **OK** and then install the policy.

**Sample Deployment (Manual Rules for Port Translation)**

The goal for this sample configuration is to let external computers access a web and mail server in a DMZ network from one IP address. Configure Hide NAT for the DMZ network object and create manual NAT rules for the servers.
### Configuring the NAT Policy

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>External computers and servers in the Internet</td>
</tr>
<tr>
<td>2</td>
<td>Security Gateway (Alaska_GW external interface 2001:db8::c:1)</td>
</tr>
<tr>
<td>3</td>
<td>DMZ network (Alaska_DMZ 2001:db8::/128)</td>
</tr>
<tr>
<td>4</td>
<td>Web server (Alaska_DMZ_Web 2001:db8::35:5 translated to 2001:db8::c:1)</td>
</tr>
<tr>
<td>5</td>
<td>Mail server (Alaska_DMZ_Mail 2001:db8::35:6 translated to 2001:db8::c:1)</td>
</tr>
</tbody>
</table>

**To configure NAT for the DMZ servers:**

1. Enable automatic Hide NAT for the DMZ network.
   a) Double-click the Alaska_DMZ object and select **NAT**.
   b) Select **Add Automatic Address Translation Rules**.
   c) In **Translation method**, select **Hide**.
   d) Select **Hide behind Gateway**.
   e) Click **OK**.

2. Create a manual NAT rule that translates HTTP traffic from the Security Gateway to the web server.
   a) In the **Firewall** tab, select **NAT**.
   b) Add a rule below the automatic rules.
   c) Right-click the cell and select **Add Object** to configure these settings:
      - **Original Destination** - Alaska_GW
      - **Original Service** - HTTP
      - **Translated Destination** - Alaska_DMZ_Web

3. Create a manual NAT rule that translates SMTP traffic from the Security Gateway to the mail server.
   a) Add a rule below the automatic rules.
   b) Right-click the cell and select **Add Object** to configure these settings:
      - **Original Destination** - Alaska_GW
      - **Original Service** - SMTP
      - **Translated Destination** - Alaska_DMZ_Web

4. Create a rule in the Firewall Rule Base that allows traffic to the servers.
   a) In the **Firewall** tab, select **Policy**.
   b) Add a rule to the Rule Base.
   c) Right-click the cell and select **Add Object** to configure these settings:
      - **Destination** - Alaska_DMZ
      - **Service** - HTTP, SMTP
      - **Action** - Allow

5. Install the policy.

---

**NAT Rule Base for Manual Rules for Port Translation Sample Deployment**

<table>
<thead>
<tr>
<th>No.</th>
<th>Original Packet</th>
<th>Translated Packet</th>
<th>Install On</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Source</td>
<td>Destination</td>
<td>Service</td>
<td>Source</td>
</tr>
<tr>
<td>1</td>
<td>Alaska_DMZ</td>
<td>Alaska_DMZ</td>
<td>Any</td>
<td>Alaska_DMZ</td>
</tr>
<tr>
<td>2</td>
<td>Alaska_DMZ</td>
<td>Alaska_DMZ</td>
<td>Any</td>
<td>Alaska_DMZ_W</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Alaska_GW</td>
<td>http</td>
<td>Original</td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>Alaska_GW</td>
<td>smtp</td>
<td>Original</td>
</tr>
</tbody>
</table>
Advanced NAT Settings

Deployment Configurations

This section discusses how to configure NAT in some network deployments.

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 Security Gateway replies on behalf of translated network objects to ARP requests from the Internet router for the address of the internal machine.

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

For more about configuring Proxy ARP for IPv4 Manual NAT, see sk30197 (http://supportcontent.checkpoint.com/solutions?id=sk30197).

For more about configuring Proxy NDP for IPv6 Manual NAT, see sk91905 (http://supportcontent.checkpoint.com/solutions?id=sk91905).

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.

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.
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 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, 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

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 \(192.168.30.0/24\) network as a destination. Users in Network B who want to communicate with users in Network A must use the \(192.168.20.0/24\) network as a destination.

The 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 \(192.168.1.0/24\).
Configuring the NAT Policy

**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>
<thead>
<tr>
<th>Step</th>
<th>Source IP address</th>
<th>Destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface A — before NAT</td>
<td>192.168.1.10</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>Interface A — after NAT</td>
<td>192.168.20.10</td>
<td>192.168.30.10</td>
</tr>
</tbody>
</table>

Security Gateway enforces the security policy for packets from network 192.168.20.0/24 to network 192.168.30.0/24.

<table>
<thead>
<tr>
<th>Step</th>
<th>Source IP address</th>
<th>Destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface B — before NAT</td>
<td>192.168.20.10</td>
<td>192.168.30.10</td>
</tr>
<tr>
<td>Interface B — after NAT</td>
<td>192.168.20.10</td>
<td>192.168.1.10</td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th>Step</th>
<th>Source IP address</th>
<th>Destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface A — before NAT</td>
<td>192.168.1.10</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>Interface A — after NAT</td>
<td>192.168.20.10</td>
<td>10.10.10.10</td>
</tr>
</tbody>
</table>

Security gateway enforces the security policy for packets from network 192.168.20.0/24 to the Internet.

<table>
<thead>
<tr>
<th>Step</th>
<th>Source IP address</th>
<th>Destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface C — before NAT</td>
<td>192.168.20.10</td>
<td>10.10.10.10</td>
</tr>
<tr>
<td>Interface C — after NAT Hide</td>
<td>192.168.4.1</td>
<td>10.10.10.10</td>
</tr>
</tbody>
</table>

**Routing Considerations**
To allow routing from Network A to Network B, routing must be configured on the Firewall.
These sections contain sample routing commands 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:

**Sample Network Configuration: Interface Configuration**

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

**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 Security Gateways inside the NATed network, on the border between the NATed network and the outside world and outside the NATed network.
In ordinary Hide NAT configurations, connections cannot be established from the external side the NAT A 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 A Security Gateway control connections.

Non-Corresponding Gateway Addresses
Sometimes the gateway contacts the Security Management server with an address that does not correspond to the remote gateway's deployment, for example:
- 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. All workarounds 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.
Configuring the Security Gateway Object

To configure the Security Gateway object:
2. In the General tab in the Interface Properties window, define the IP Address and the Net Mask.
3. In the Topology tab of the Interface Properties window, select Network defined by the interface IP and Net Mask.

**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.

**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. The following illustration shows one of the MEP Gateways in a SecuRemote/SecureClient to MEP (Multiple Entry Point) gateway deployment.
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 non-encrypted (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.

**Reusing IP Pool Addresses For Different Destinations**

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. 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.
Configuring the NAT Policy

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 the following illustration). 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.

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.
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,
   a) In the network objects tree, right-click Network Objects branch and select New > Address Range.
   b) In the General tab, enter the first and last IP of the address range.
   c) 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:
   a) Allocate IP Addresses from and then select the address range you created to configure IP Pool NAT for the whole gateway, or
   b) 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:
a) **Use IP Pool NAT for VPN client connections**

b) **Use IP Pool NAT for gateway to gateway connections**

c) **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**.

a) **Return unused addresses to IP Pool after**: Addresses in the pool are reserved for 60 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 timeout to prevent the IP Pool from being depleted.

b) **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 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 11

Monitoring and Logging

In This Chapter

Monitoring Important Events with SmartEvent 107
Monitoring Traffic and Connections with SmartLog 110

Monitoring Important Events with SmartEvent

The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. SmartEvent consolidates and shows all security events that are generated by these Software Blades:

- Firewall
- IPS
- Application Control
- Anti-Bot and Anti-Virus
- DLP

Administrators can quickly identify very important security events and do the necessary actions to prevent more attacks.
For more information about using SmartEvent, see the R76 SmartEvent Administration Guide.

**Enabling SmartEvent**

**To enable SmartEvent on the Security Management server:**

1. In SmartDashboard from the **Network Objects** navigation tree, double-click the Security Management server.
   The **General Properties** window opens.
2. In the **Management** tab, select these Software Blades:
   - **Logging & Status**
   - **SmartEvent Server**
   - **SmartEvent Correlation Unit**
3. Click **OK**.
4. From the menu bar, select **Policy > Install Database**.
5. From the menu bar, select **SmartConsole > SmartEvent**.
   The SmartEvent console opens.

**Creating Reports**

SmartEvent lets you create reports that summarize events for the supported Software Blades. These reports can help you identify attack trends and the effectiveness of the Firewall Rule Base and the security policy. The reports can be automatically sent as emails and PDF files at regular intervals.

**To create a SmartEvent report:**

1. In SmartEvent, click the **Reports** tab.
2. From the navigation tree, click **All** or a Software Blade.
3. Select the report.
The report is created and shown in the window.

**Sample Application and URL Filtering Event Analysis**

This is a sample procedure that shows how to use SmartEvent to do an analysis of Internet browsing events from the Application and URL Filtering Software Blade.

**To show an Internet browsing event:**

1. From SmartEvent **Overview** tab, in the **View** section, click the Application and URL Filtering icon.
   The Application and URL Filtering **Overview** page opens.
2. In **Timeline View**, click the **High Risk** events for a day.
The **High Risk** window opens.

![High Risk window](image)

This some of the information about the event:

- 5 users tried to access the VTunnel web proxy
- VTunnel is classified as a **High** security risk and is a Web proxy site that lets users go to websites anonymously
- The names of the 5 users that tried to go to the VTunnel website are shown

### Monitoring Traffic and Connections with SmartLog

The SmartLog Software Blade is a log management tool that reads logs from all Software Blades on Security Management servers and Security Gateways. SmartLog works with the SmartLog Index Server that gets log files from different log servers and indexes them. SmartLog supplies these monitoring features:

- Quickly search through billions of logs with simple search strings
- Select from many default search queries to find the applicable logs
• Monitor logs from administrator activity and connections in real-time

For more about using SmartLog, see the R76 SmartLog Administration Guide.

**Enabling SmartLog**

The SmartLog Index Server contains a central index of log entries from all SmartLog enabled Security Management and log servers.

To enable SmartLog:

1. Open SmartDashboard.
2. From the Network Objects tree, double-click the Security Management server. The General Properties window opens.
3. In the Management tab, select Logging & Status.
4. From the navigation tree, click Logs.
5. Select Enable SmartLog and then click OK.
6. From the menu bar, select Policy > Install Database.
   The SmartLog Index Server is installed on the Security Management server.
7. From the menu bar, select SmartConsole > SmartLog.
   The SmartLog console opens.
**Sample Log Analysis**

This is a sample procedure that shows how to use SmartLog to do an analysis of a log of a dropped connection.

**To show a log of a dropped connection:**

1. From SmartLog, in the **Query Top Results** pane select **Top Actions > Drop**.
   
The Results pane shows the logs for dropped connections.

2. Double-click a log.
   
The **Log Details** window opens.

![Log Details Window](image)

This is some of the information about the dropped connection in the log:

- A telnet connection from 10.6.20.54 to 10.17.45.125 was dropped
- The connection matched rule number 2 (Telnet not allowed) in the Firewall Rule Base
Index

A
Access Control and the Rule Base • 9
Action • 54
Activating Single Sign On • 25
AD Query • 40
Adding a Certificate • 60
Adding an Access Role to a Rule • 49
Adding an IPS Exception • 65
Adding Data Owners • 78
Adding Network Exceptions • 65
Adding Users to the Rule Base • 49
Adding Users to the Security Policy • 40
Advanced NAT Settings • 99
Allowing Mobile Connections • 25
Allowing VPN Connections • 37
Analyzing and Tracking DLP • 82
Analyzing the Rule Base (Hit Count) • 19
Anti-Bot and Anti-Virus • 68
Anti-Bot and Anti-Virus Rule Base • 71
Anti-Spam • 72
Applications/Sites • 53
Authentication Tab • 48
Automatic and Manual NAT Rules • 92
Automatic and Proxy ARP • 99
Automatic Hide NAT to External Networks • 94

B
Basic Rules • 14
Browser-Based Authentication • 40
Browsing IPS Protections • 65

C
Check Point Firewall Security Solution • 7
Check Point Mobile Access Solutions • 21
Check Point Software Acceleration Solutions • 86
Citrix Services • 26
Client-Based vs. Clientless • 21
Communication Between an Internal Network and the Internet • 101
Communication Between Internal Networks • 101
Communication Examples • 101
Compliance Policy Rules • 28
Components of the Check Point Solution • 7
Configuring Anti-Spoofing • 17
Configuring Citrix Services for Mobile Access • 27
Configuring Compliance Settings for a Security Gateway • 30
Configuring CoreXL • 86
Configuring Geo Protections • 66
Configuring HTTPS Inspection Rules • 60
Configuring IP Pool NAT • 106
Configuring Remote Access to Network Resources • 22
Configuring SecureXL • 87
Configuring Security Gateways • 59
Configuring Static and Hide NAT • 93
Configuring the Hit Count Display • 19
Configuring the NAT Policy • 89
Configuring the Security Gateway Object • 104
Configuring the Security Management Server Object • 103
Connecting to a Citrix Server • 26
Connecting Translated Objects on Different Interfaces • 100
CoreXL • 86
Creating a New AD Object • 42
Creating a Secure Firewall Rule Base • 14
Creating a Strong Firewall Security Policy • 12
Creating Access Roles • 42
Creating an Account Unit • 46
Creating an Endpoint Compliance Policy • 29
Creating Reports • 109
Creating VPN Policies • 33
Data Loss Prevention Features • 75
Defining Access to Applications • 25
Defining an Internet Access Policy • 51
Defining Security Zones • 15
Deploying User Directory • 45
Deployment Configurations • 99
Disabling NAT in a VPN Tunnel • 99
DLP Actions • 83
DLP General Columns • 83
DLP Restricted Columns • 84
DLP Rule Actions • 81
DLP Rule Base • 79
DLP Rule Exceptions • 80
DMZ • 16
Dual Stack (IPv4 and IPv6) Network Configuration • 8

E
Editing an Account Unit • 46
Enabling Anti-Spam • 73
Enabling Automatic NAT • 94
Enabling DLP • 78
Enabling HTTPS Inspection • 59
Enabling Identity Awareness • 41
Enabling IPS • 63
Enabling Manual NAT • 95
Enabling or Disabling Hit Count • 19
Enabling SmartEvent • 109
Enabling SmartLog • 112
Enabling the Anti-Bot and Anti-Virus Software Blades • 70
Enabling URL Filtering and Application Control • 52
Enabling User Directory • 48
Endpoint Compliance Check • 28
Examining Anti-Bot and Anti-Virus Protections • 70
Excluding Specific Internal Addresses • 18
Explicit and Implied Rules • 13

G
General Tab • 46
Generating a New Certificate • 59
Granular Routing Control • 35
User Directory Features • 45
UserCheck • 52
UserCheck Actions • 55
Using a Mail Relay and Mail Server • 77
Using Automatic Rules • 92
Using DLP with Microsoft Exchange • 79
Using Hide NAT • 89
Using Identity Awareness • 40
Using Identity Awareness in the Firewall Rule Base • 43
Using IPS Profiles • 64
Using Remote Access VPN • 38
Using Secure Workspace • 31
Using SecureXL • 87
Using Site to Site VPN • 36
Using SmartEvent • 85
Using SmartView Tracker • 82
Using the Firewall Rule Base • 12
Using the HTTPS Inspection Rule Base • 58
Using the Identity Awareness Wizard • 41
Using the Mobile Access Configuration Wizard • 23
Using the URL Filtering and Application Control Rule Base • 52
Using User Directory • 45

V

VPN Communities • 34
VPN Connectivity Modes • 38