Important Information

Check Point R80
For more about this release, see the R80 home page

Latest Version of this Document
Download the latest version of this document
To learn more, visit the Check Point Support Center

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 Pre-R80 Security Gateways with R80 Security Management Getting Started Guide.

Searching in Multiple PDFs
To search for text in all the R80 PDF documents, download and extract the complete R80 documentation package
To search for all text in the R77 PDF documents, download and extract the R77 documentation package
Use Shift-Control-F in Adobe Reader or Foxit reader.

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>28 March 2016</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
**Terms**

**Anti-Bot**
1. An application that prevents computers from being controlled by hackers. 2. Check Point Software Blade that inspects network traffic for malicious bot software.

**Anti-Virus**
A solution to protect a computer or network against self-propagating programs or processes that can cause damage.

**APP Wiki**
A searchable application library, for Check Point Application Control and URL Filtering, with details about known Web applications and social networking widgets. (Also: AppWiki)

**Block**
1. To stop traffic before it reaches its destination. 2. To stop a command from execution. 3. To deny access by rule (though allowed by permission).

**Bot**
Malicious software that neutralizes Anti-Virus defenses, connects to a Command and Control center for instructions from cyber criminals, and carries out the instructions.

**CoreXL**

**CSCF**
Call Session Control Function. A set of roles for SIP servers or proxies that handle SIP signal packets in the IP Multimedia Subsystem (IMS).

**DBedit**
A CLI tool that lets administrators make changes to objects in the Check Point databases. We recommend that administrators use the GuiDBedit tool instead of dbedit when not using scripts.

**Diameter**
An authentication, authorization and accounting protocol that has many features not included in the legacy RADIUS protocol.

**Diameter Application**
An extension to the Diameter base protocol (as defined in RFC6733). Each application contains one or more commands and/or attributes. Applications are typically associated with an RFC.

**DLP**
Data Loss Prevention. Detects and prevents the unauthorized transmission of confidential information.

**DPD**
Dead Peer Detection. A methodology for the detection of a failed IKE peer. It can reclaim lost resources when a peer fails or trigger an IKE peer failover.

**Drop**
To not allow packets through the gateway, blocking the connection.

**Event**
1. A record of a security incident that is based on one or more logs, and on a customizable set of rules that are defined in the Event Policy. 2. In Media Encryption, a device connects to an endpoint computer. 3. In SmartLSM, an object with schedule settings for the Security Gateway to fetch its security policy. 4. In Endpoint Security, an object with schedule settings for Active and Standby server synchronization.

**Firewall**
The software and hardware that protects a computer network by analyzing the incoming and outgoing network traffic (packets).

**GGSN**
Gateway GPRS Support Node. The main component of a GPRS network that is responsible for communication between the
GPRS network and external, packet-switched networks, such as the Internet.

**GPRS**

General Packet Radio Service. A packet-oriented, mobile data service that works over Global System for Mobile Communication (GSM) networks.

**GSM**

Global System for Mobile Communications. An international standard that defines protocols for second generation digital cellular networks used by mobile phones.

**GTP**

GPRS Tunneling Protocol. A set of IP-based communication protocols that handle GPRS traffic over GSM, UMTS and LTE networks.

**GuiDBedit**

A graphical interface tool for administrators to change objects in Check Point databases.

**HSPA**

High Speed Packet Access. An improved third generation mobile communication protocol that significantly enhances data transfer. It is a combination of two protocols:

- HSUPA - High Speed Uplink Packet Access
- HSDPA - High Speed Downlink Packet Access

**IKE**

Internet Key Exchange. An Encryption key management protocol for IPSec that creates a shared key to encrypt and decrypt IP packets and establishes a VPN tunnel and Security Association.

**IPS**

Intrusion Prevention System. Check Point Software Blade that inspects and analyzes packets and data for numerous types of risks.

**IPv4 embedded IPv6 address**

An IPv6 address where the rightmost 32 bits are a valid IPv4 address.

**LTE**

Long Term Evolution. A fourth generation communication standard for high-speed wireless communication for mobile phone and data terminals. It is based on GSM and UMTS/HSPA network technologies.

**PDP**


**Performance Pack**

Check Point product that accelerates IPv6 and IPv4 traffic. Installed on Security Gateways for significant performance improvements.

**PLMN**

Public Land Mobile Network. A network established and operated by a recognized operating agency to supply land/mobile telephony and data services.

**PSWT**

Public Switched Telephone Network. A collection of public circuit-switched telephone network, including telephone lines, fixed lines, microwave transmission links, cellular networks, and satellite communication.

**Remote Access Community**

A group of computers, appliances, and devices that access, with authentication and encryption, the internal protected network from physically remote sites.

**Remote Access VPN**

An encryption tunnel between a Security Gateway and remote access clients, such as Endpoint Security VPN, and communities.

**Rule**

A set of traffic parameters and other conditions that cause specified actions to be taken for a communication session.
**Rule Base**
The database that contains the rules in a security policy and defines the sequence in which they are enforced.

**SA**
Security Association. A VPN tunnel where all hosts on one or more subnets are associated with the tunnel. By default, Check Point VPN tunnels are created between subnets, rather than hosts.

**SCTP**

**Security Gateway**
A computer or appliance that inspects traffic and enforces Security Policies for connected network resources.

**Security Management Server**
The application that manages, stores, and distributes the security policy to Security Gateways.

**Security Policy**
A collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

**SGSN**
Serving GPRS Support Node. The component of a GPRS network that is responsible for delivery of data packets to and from mobile stations in its geographical service area.

**SIP**
Session Initiation Protocol. A signaling protocol used for controlling multimedia communication sessions, such as voice and video calls over an IP network.

**SmartEvent Server**
Physical server that hosts the events database.

**Software Blade**
A software blade is a security solution based on specific business needs.
Each blade is independent, modular and centrally managed. To extend security, additional blades can be quickly added.

**ThreatCloud Repository**
A cloud database with more than 250 million Command and Control (C&C) IP, URL, and DNS addresses and over 2,000 different botnet communication patterns, used by the ThreatSpect engine to classify bots and viruses.

**ThreatSpect Engine**
A unique multi-tiered engine that analyzes network traffic and correlates data across multiple layers (reputation, signatures, suspicious mail outbreaks, behavior patterns) to detect bots and viruses.

**UserCheck**
Gives users a warning when there is a potential risk of data loss or security violation. This helps users to prevent security incidents and to learn about the organizational security policy.

**UTMS**
About this Guide

In This Section:

R80 SmartConsole Toolbars .................................................................12

This guide explains how to manage backward compatible (R77.xx and lower) Security Gateways with the R80 SmartConsole.

This guide shows only the updated procedures. To learn more about earlier features, see the R77 documentation http://supportcontent.checkpoint.com/documentation_download?ID=26770.

R80 SmartConsole Toolbars

Global Toolbar (top left of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description and Keyboard Shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>The main R80 SmartConsole Menu</td>
</tr>
</tbody>
</table>

| The Objects menu.  
Also leads to the Object Explorer Ctrl+E |
|-------------------|

| Install policy on managed gateways  
Ctrl+Shift+Enter |
|--------------------|

Navigation Toolbar (left side of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description and Keyboard Shortcut</th>
</tr>
</thead>
</table>
| Gateway configuration view  
Ctrl+1 |

| Security Policies Access Control view  
Security Policies Threat Prevention view  
Ctrl+2 |
|-----------------------------|

| Logs & Monitor view  
Ctrl+3 |
|----------------------|

| Manage & Settings view - review and configure the Security Management Server settings  
Ctrl+4 |
|-----------------------------|
## Command Line Interface Button (left bottom corner of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description and Keyboard Shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open a command line interface for management scripting and API F9</td>
</tr>
</tbody>
</table>

## What's New Button (left bottom corner of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description and Keyboard Shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open a tour of the R80 SmartConsole</td>
</tr>
</tbody>
</table>

## Objects and Validations Tabs (right side of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objects</td>
</tr>
<tr>
<td>Validations</td>
</tr>
</tbody>
</table>

## System Information Area (bottom of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task List</td>
</tr>
<tr>
<td>Server Details</td>
</tr>
<tr>
<td>Connected Users</td>
</tr>
</tbody>
</table>
Check Point Firewall Security Solution

In This Section:

Overview of Firewall Features .............................................................. 14
How to Use this Guide ............................................................................. 16

Firewalls control the traffic between internal and external networks and are the core of a strong network security policy. Check Point implements firewall security solutions through Software Blades - a set of security features that can be selected and configured to fit various security needs.

Overview of Firewall Features

The Check Point Software Blade architecture provides the "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 Firewall Solution
These are the primary components of a Check Point firewall solution:

- **Security Gateway** - The engine that enforces the organization’s security policy, is an entry point to the LAN, and is managed by the Security Management Server.
- **Security Management Server** - The application that manages, stores, and distributes the security policy to Security Gateways.
- **R80 SmartConsole** - A Check Point GUI application used to manage security policies, monitor products and events, install updates, provision new devices and appliances, and manage a multi-domain environment.

**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>R80 SmartConsole</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>IPv4 network traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 network traffic</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Gateway for dual stack network</td>
</tr>
<tr>
<td>2</td>
<td>Internal network (IPv6 traffic)</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>3</td>
<td>Dual stack web server in the DMZ</td>
</tr>
<tr>
<td>4</td>
<td>Security Gateway for IPv4 network</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 and higher, you can configure the interfaces to use only IPv6 addresses.

## How to Use this Guide

To configure an effective firewall security solution, you must understand how to configure different Software Blades and how to add rules to your security policy. In some sections of this guide, you will find configuration examples that will help you understand the general principles of creation of a Check Point firewall solution. However, before you configure your production security environment, make sure to familiarize yourself with the Administration Guides for the applicable Check Point Software Blades.

### 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</td>
</tr>
<tr>
<td></td>
<td>Configuring the NAT Policy (on page 112)</td>
</tr>
<tr>
<td>Mobile Access</td>
<td>Remote Access to the Network (on page 28)</td>
</tr>
<tr>
<td>IPsec VPN</td>
<td>Creating VPN Policies (on page 38)</td>
</tr>
<tr>
<td>Identity Awareness</td>
<td>Adding Users to the Security Policy (on page 46)</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>Defining an Internet Access Policy (on page 57)</td>
</tr>
<tr>
<td>Application Control</td>
<td></td>
</tr>
<tr>
<td>Software Blade</td>
<td>Chapter</td>
</tr>
<tr>
<td>----------------</td>
<td>---------</td>
</tr>
<tr>
<td>IPS</td>
<td>Defending against Network Intrusions (&quot;IPS&quot; on page 73)</td>
</tr>
<tr>
<td>Anti-Bot</td>
<td>Threat Prevention Policies (&quot;Creating a Threat Prevention Policy&quot; on page 72)</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>Securing Data (on page 96)</td>
</tr>
<tr>
<td>Advanced Networking &amp; Clustering</td>
<td>Maximizing Network Performance (on page 109)</td>
</tr>
<tr>
<td>Logging &amp; Status SmartEvent</td>
<td>Monitoring and Logging (on page 133)</td>
</tr>
</tbody>
</table>
Managing Network Access Control

In This Section:

- Introducing the Access Control Policy ................................................................. 18
- Ensuring a Secure Network Access ...................................................................... 20
- Preventing IP Spoofing .......................................................................................... 21
- Analyzing the Rule Base (Hit Count) ..................................................................... 23
- Inspection Settings ................................................................................................. 25

A firewall controls access to computers, clients, servers, and applications through a set of rules that comprise an Access Control Rule Base. You need to configure a Rule Base that not only provides highly secure Access Control, but optimizes network performance. A strong Access Control Rule Base:

- Only allows authorized connections and prevents vulnerabilities in a network
- Gives authorized users access to the correct internal resources
- Efficiently inspects connections and uses network resources efficiently

Introducing the Access Control Policy

An Access Control Policy Rule Base consists of these types of rules:

- Firewall - Control access to the internal network through different access points (gateways)
- Application Control and URL Filtering - Prevent malicious applications from compromising any internal company data and the internal network resources

Types of Rules in the Rule Base

There are three types of rules in the Rule Base - explicit, implied and implicit.

Explicit rules

The rules that the administrator configures explicitly, to allow or to block traffic based on specified criteria.

⚠ Important - The Cleanup rule is a default explicit rule and is added with every new layer. You can change or delete the default Cleanup rule. We recommend that you have an explicit cleanup rule as the last rule in each layer.

Implied rules

The default rules that are available as part of the Global properties configuration and cannot be edited. You can only select the implied rules and configure their position in the Rule Base:

- First - Applied first, before all other rules in the Rule Base - explicit or implied
- Last - Applied last, after all other rules in the Rule Base - explicit or implied, but before the Implicit Cleanup Rule
- Before Last - Applied before the last explicit rule in the Rule Base
Implied rules are configured to allow connections for different services that the Security Gateway uses. For example, the **Accept Control Connections** rules allow packets that control these services:

- Installation of the security policy on a Security Gateway
- Sending logs from a Security Gateway to the Management Server
- Connecting to third party application servers, such as RADIUS and TACACS authentication servers

**Implicit cleanup rule**

The default "catch-all" rule that deals with traffic that does not match any explicit or implied rules in the Policy Layers. For R77.30 or earlier versions Security Gateways, the action of the implicit rule depends on the Policy Layer:

- **Drop** - for the **Network** Layer
- **Accept** - for the **Application Control** Layer

**Note** - If you change the default values, the policy installation will fail.

The implicit rules do not show in the Rule Base.

**Order of Rule Enforcement**

When a packet arrives at the gateway, the gateway checks it against the rules in the top Policy Layer, sequentially from top to bottom, and enforces the first rule that matches a packet.

If the **Action** of the matching rule is **Drop**, the gateway stops matching against later rules in the Policy Rule Base and drops the packet. If the **Action** is **Accept**, the gateway continues to check rules in the next Policy Layer down.

If none of the rules in the Policy Layer match the packet, the explicit **Default Cleanup Rule** is applied. If this rule is missing, the **Implicit Cleanup Rule** is applied.

**Important** - Always add an explicit **Default Cleanup Rule** at the end of each Policy Layer, and make sure that its **Action** is the same as the **Action** of the **Implicit Cleanup Rule**.

**Order in which the rules in each Access Control Policy Layer are applied:**

1. **First Implied Rule** - No explicit rules can be placed before it.
2. **Explicit Rules** - These are the rules that you create.
3. **Before Last Implied Rules** - Applied before the last explicit rule.
4. **Last Explicit Rule** - We recommend that you use a **Cleanup rule** as the last explicit rule.
   **Note** - If you use the **Cleanup rule** as the last explicit rule, the **Last Implied Rule** and the **Implicit Cleanup Rule** are not enforced.
5. **Last Implied Rule** - Remember that although this rule is applied after all other explicit and implied rules, the Implicit Cleanup Rule is still applied last.
6. **Implicit Cleanup Rule** - The default rule that is applied if none of the rules in the Policy Layer match.
Best practices for performance-efficient Access Control Policy

- Add all rules that are based only on source and destination IP addresses and ports in a Firewall/Network Policy Layer at the top of the Rule Base
- Create Firewall/Network rules to explicitly accept safe traffic, and add the Explicit Cleanup Rule at the bottom of the Policy Layer to drop everything else
- Create Application Control rules to explicitly drop unwanted or unsafe traffic, and add the Explicit Cleanup Rule at the bottom of the Policy Layer to accept everything else
- Turn XFF inspection off, unless the gateway is behind a proxy server. For more, see: sk92839 http://supportcontent.checkpoint.com/solutions?id=sk92839.

Configuring the Implied Rules

Some of the implied rules are enabled by default. You can change the default configuration as necessary.

To configure the implied rules:

1. In R80 SmartConsole, from the Menu, select Global Properties. The Global Properties window opens.
2. Select a rule to enable it, or clear a rule to disable it.
3. For the enabled rules, select the position of the rules in the Rule Base ("Order of Rule Enforcement" on page 19):
   - First - The rule is applied before any other rule in the Rule Base
   - Last - The rule is applied if all other rules in the Rule Base were applied and none of them matched
   - Before Last - The rule is applied before the last explicit rule, if none of the other rules in the Rule Base matched
4. Click OK and install the policy.

Ensuring a Secure Network Access

A robust security policy must have some basic rules in its 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 in the policy

Note - There is also the implicit drop rule that drops all traffic that did not match all other rules. This rule does not create log entries. If you want to log the traffic, create an explicit cleanup rule.
Preventing IP Spoofing

IP spoofing replaces the untrusted source IP address with a fake, trusted one, to hijack connections to your network. Attackers use IP spoofing to send malware and bots to your protected network, to execute DoS attacks, or to gain unauthorized access.

Anti-Spoofing detects if a packet with an IP address that is behind a certain interface, arrives from a different interface. For example, if a packet from an external network has an internal IP address, Anti-Spoofing blocks that packet.

Example:
The diagram shows a Gateway with interfaces A and B, and C, and some example networks behind the interfaces.

For the Gateway, anti-spoofing makes sure that
- All incoming packets to A come from 192.168.33.0
- All incoming packets to B come from 192.0.2.0 or 10.10.10.0
- All incoming packets to C come from the Internet

If an incoming packet to B has a source IP address in network 192.168.33.0, the packet is blocked, because the source address is spoofed.

When you configure Anti-Spoofing on a Check Point Security Gateway, specify the type of networks that each interface faces - **External** (Internet) or **Internal**.

Configuring Anti-Spoofing

Make sure to configure Anti-Spoofing protection on all the interfaces of the Security Gateway, including internal interfaces.

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

1. In R80 SmartConsole, go to **Gateways & Servers** and double-click the gateway object. The **General Properties** window of the gateway opens.
2. From the navigation tree, select **Network Management**.
3. Click **Get Interfaces**.
4. Click **Accept**.

The gateway network topology shows. If R80 SmartConsole fails to automatically retrieve the topology, make sure that the details in the **General Properties** section are correct and the Security Gateway, the Security Management Server, and the R80 SmartConsole can communicate with each other.
5. Select an interface and click Edit.
   The Interface properties window opens.
6. From the navigation tree, select General.
7. In the Topology section of the page, click Modify.
   The Topology Settings window opens.
8. Select the type of network the interface leads to:
   - External - All external/Internet addresses
   - Internal -
     - Not Defined - All IP addresses behind this interface are considered a part of the internal network that connects to this interface
     - Network defined by the interface IP and Net Mask - Only the network that directly connects to this internal interface
     - Specific - A specific network object (a network, a host, an address range, or a network group) behind this internal interface
     - Interface leads to DMZ - The DMZ that directly connects to this internal interface
9. In the Anti-Spoofing section, make sure that Perform Anti-Spoofing based on interface topology is selected.
10. Select an Anti-Spoofing action:
    - Prevent - Drops spoofed packets
    - Detect - Allows spoofed packets. To monitor traffic and to learn about the network topology without dropping packets, select this option together with the Spoof Tracking Log option.
11. Configure Anti-Spoofing exceptions (optional) - addresses, from which packets are not inspected by Anti-Spoofing ("Excluding Specific Internal Addresses" on page 22):
    a) Select Don't check packets from.
    b) Select an object from the drop-down list, or click New to create a new object.
12. Configure Spoof Tracking - select the tracking action that is done when spoofed packets are detected:
    - Log - Create a log entry (default)
    - Alert - Show an alert
    - None - Do not log or alert
13. Click OK twice to save Anti-Spoofing settings for the interface.
For each interface, repeat the configuration steps. When finished, 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 hits from total hits
- The indicator level (very high, high, medium, low, or zero)

These options are configured in the Access Control Policy 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.

- Improve 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 Access Control 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. In R80 SmartConsole, click **Menu >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 Management Server database for this period and is shown in the Hits column.
4. Click **OK**.
5. Install the Policy.
To enable or disable Hit Count on each Security Gateway:

1. From the Gateway Properties for 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.
4. 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
  - 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.

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

To show the Hit Count in the Rule Base:

Right-click the heading row of the Rule Base and select Hits.
To configure the Hit Count in a rule:
1. Right-click the rule number of the rule.
2. Select Hit Count and one of these options (you can repeat this action to configure more options):
   - Timeframe - Select All, 1 day, 7 days, 1 month, or 3 months
   - Display - Select Percentage, Value, or Level

To update the Hit Count in a rule:
1. Right-click the rule number of the rule.
2. Select Hit Count > Refresh.

Inspection Settings

You can configure inspection settings for the Firewall:
- Deep packet inspection settings
- Protocol parsing inspection settings
- VoIP packet inspection settings

Security Management Server comes with two preconfigured inspection profiles:
- Default Inspections
- Recommended Inspections

When a Security Gateway is configured, the Default Inspections profile is enabled for it. You can also assign the Recommended Inspections profile the Security Gateway, or to create a custom profile and assign it to the Security Gateway.

To activate the Inspection Settings, install the Access Control Policy.

Note - In pre-R80 SmartConsole, Inspection Settings are configured as IPS Protections.

Configuring Inspection Settings

To configure Inspection Settings:
1. In R80 SmartConsole, go to the Manage & Settings > Blades view.
2. In the General section, click Inspection Settings.
   The Inspection Settings window opens.

Here, you can:
- Edit protection properties
- Edit user-defined Inspection Settings profiles. You cannot change the Default Inspection profile and the Recommended Inspection profile.
- Assign Inspection Settings profiles to Security Gateways
- Configure exceptions to protections
To edit properties of a protection:
1. In the **General** view, select a protection.
2. Click **Edit**.
3. In the window that opens, select a profile, and click **Edit**.
   The protection properties window opens.
4. Select the **Main Action** -
   - **Default Action** - preconfigured action
   - **Override with Action** - from the drop-down menu, select an action with which to override the default - **Accept, Drop, Inactive** (the protection is not activated)
5. Configure the **Logging Settings**
   Select **Capture Packets**, if you want to be able to examine packets that were blocked in Drop rules.
6. Click **OK**.
7. Click **Close**.

To view protections for a certain profile:
1. In the **General** view, click **View >Show Profiles**.
2. In the window that opens, select **Specific Inspection settings profiles**.
3. Select profiles.
4. Click **OK**.
   Only protections for selection profiles are shown.

You can add, edit, clone, or delete custom Inspection Settings profiles.

To edit a custom Inspection Settings profile:
1. In the **Profiles** view, select a profile.
2. Click **Delete**, to remove it, or click **Edit** to change the profile name, associated color, or tag.
3. If you edited the profile attributes, click **OK** to save the changes.

To clone an Inspection Settings profile:
1. In the **Profiles** view, select the profile, and click **Clone**.
2. In the **New Profile** window that opens, edit the profile attributes:
3. Click **OK**.

To add a new Inspection Settings profile:
1. In the **Profiles** view, click **New**.
2. In the **New Profile** window that opens, edit the profile attributes:
3. Click **OK**.

To assign an Inspection Settings profile to a Security Gateway:
1. In the **Gateways** view, select a gateway, and click **Edit**.
2. In the window that opens, select an Inspection Settings profile.
3. Click **OK**.
To configure exceptions to protections:

1. In the Exceptions view, click New to add a new exception, or select an exception and click Edit to modify an existing one.
   The Exception Rule window opens.
2. Configure the exception settings:
   - Apply To - select the Profile to which to apply the exception
   - Protection - select the Protection
   - Source - select the source Network Object, or select IP Address and enter a source IP address
   - Destination - select the destination Service Object, or select Port/Range, TCP or UDP, and enter a destination port number or a range of port numbers
   - Install On - select a gateway on which to install the exception
3. Click OK.

To enforce the changes, publish the session and install the Access Control Policy.
Remote Access to the Network

In This Section:

Overview...........................................................................................................................................28
Check Point Mobile Access Solutions ............................................................................................28
Configuring Remote Access to Network Resources .......................................................................29
Connecting to a Citrix Server ..............................................................................................................33
Compliance Check...............................................................................................................................35

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, and authenticate with one of these options:

- User name and password
- Certificate
- SecurID

R80 SmartConsole 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 through a web 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).

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.
Remote Access to the Network

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

- Capsule Workspace - An app that creates a secure container on the mobile device to give users access to internal websites, file shares, and Exchange servers.
- Capsule Connect - 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 R80 SmartConsole 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:
   a) Select mobile device access clients
   b) Define the Mobile Access portal
c) Define the web applications, for example Outlook Web App
d) 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 Capsule Workspace app.

6. Users open the Capsule Workspace 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>Users download app</td>
</tr>
<tr>
<td>5</td>
<td>Users open app and enter settings</td>
</tr>
<tr>
<td></td>
<td>Users can access internal resources</td>
</tr>
</tbody>
</table>

---
### Item | Description
--- | ---
4 | Mobile Access Security Gateway
5 | Internal network resources, AD and Exchange servers

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 30).

This configuration lets these clients connect to internal resources:
- 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 R80 SmartConsole, go to **Gateways & Servers** and double-click the gateway object. The **General Properties** window opens.
2. In the **General Properties > Network Security** section, select **Mobile Access**. The **Mobile Access** page of the **Mobile Access Configuration Wizard** 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://<gw_IPv4>/sslvpn`.
6. Click **Next**. The **Applications** page opens.
7. Configure the applications to show:
   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:
      - Capsule Workspace 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.
    Click Add and then select the group Mobile_Access.

12. Click Next and then click Finish.
    The Mobile Access Configuration Wizard closes.

13. Click OK.
    The Gateway Properties window 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 MS Exchange. This rule is installed on Security Gateways in the MobileAccessGW group.

Defining Access to Applications

Use the Security Policies page in R80 SmartConsole 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 R80 SmartConsole objects:

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

1. In R80 SmartConsole, go to Manage & Settings > Blades.
2. In the Mobile Access, click Configure in SmartDashboard.
3. In the Mobile Access tab, select Additional Settings > Single Sign On.
   The Single Sign On page opens.
4. Select an application and click Details.
   The application properties window opens and shows the Single Sign On page.
5. For Web form applications, do these steps:
   a) In the Application Single Sign On Method section, select Advanced and click Details.
      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.
6. 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 34).

To configure Citrix services:

1. In R80 SmartConsole, go to Manage & Settings > Blades.
2. In the Mobile Access, click Configure in SmartDashboard.
4. Click New.
   The General Properties page of the Citrix Service window opens.
5. Enter the Name for the Citrix server object.
6. From the navigation tree, click Web Interface.
7. Create a new object for the Citrix web interface server, in Servers, click Manage > New > Host.
   The Host Node window opens.
8. Enter the settings for the Citrix web interface server and click OK.
9. In Services, select one or more of these services that the Citrix web interface server supports:
   - HTTP
   - HTTPS
10. From the navigation tree, click Link in Portal.
11. 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
12. From the navigation tree, select Additional Settings > Single Sign On.
13. Enable Single Sign On for Citrix services, select these options:
   - Turn on single Sign On for this application
   - Prompt users for their credentials
14. Click OK.
   The Citrix server object is added to Defined Citrix Services.
15. From the Mobile Access navigation tree, select Policy.
16. 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.
17. Install the policy.

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 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 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 a compliance policy:
- Windows security - Microsoft Windows hotfixes, patches and Service Packs.
- Anti-Spyware protection - Anti-Spyware software.
- Anti-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 a Compliance Policy

By default, Endpoint Security on Demand only allows endpoint computers that are compliant with the compliance policy log in to the Mobile Access portal.

To create a compliance policy:
1. In R80 SmartConsole, go to Manage & Settings > Blades.
2. In the Mobile Access section, click Configure in SmartDashboard.
3. In the Mobile Access tab, select Endpoint Security on Demand > Endpoint Compliance.
4. Click Edit policies.
   The Policies window opens.
5. Click New Policy.
   The Policies > New Policy window opens.
6. Enter the Name and Description for the policy.
7. Click Add.
   The Add Enforcement Rules window opens.
8. Select rules for the policy.
    You can also create new rules - click New Rule, and configure the rule settings.
9. Click OK.
   The Policies > New Policy window shows the rules for the policy.
10. Select Bypass spyware scan if necessary.
    When 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.
11. Click OK.
   The Policies window opens.
12. 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 compliance policy.

This procedure shows how to configure the Laptop Computer policy ("Compliance Policy Rules" on page 36) for a Security Gateway.

**To configure the compliance settings:**

1. In R80 SmartConsole, go to **Manage & Settings > Blades**.
2. In the Mobile Access section, click **Configure in SmartDashboard**.
3. In the **Mobile Access** tab, select **Endpoint Security on Demand > Endpoint Compliance**.
4. Select the Security Gateway and click **Edit**.
   - The **Endpoint Compliance** page of the Security Gateway properties window opens.
5. Select **Scan endpoint machine when user connects**.
6. Select **Threshold policy** and from the drop-down menu select **Laptop Computer**.
7. Click **OK**.
8. Install the policy on the Mobile Access Security Gateway.

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.

**To enable Secure Workspace on a Mobile Access Security Gateway:**

1. In R80 SmartConsole, go to **Manage & Settings > Blades**.
2. In the Mobile Access section, click **Configure in SmartDashboard**.
3. In the **Mobile Access** tab, click **Endpoint Security on Demand > Secure Workspace**.
4. Select the Security Gateway and click **Edit**.
   - The **Check Point Secure Workspace** page of the Security Gateway properties window opens.
5. Select **This gateway supports access to applications from within Check Point Secure Workspace**.
6. Click **OK** and then install the policy.
Creating VPN Policies

In This Section:
Overview .................................................................................................................................................. 38
Using Site to Site VPN .......................................................................................................................... 42
Using Remote Access VPN .................................................................................................................. 44

Overview
The IPsec VPN Software Blade lets the Security Gateways encrypt and decrypt traffic to and from external networks and clients. 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 communication sessions that are authenticated and encrypted on private or public networks.

**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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Security Gateway</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</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 Security Gateways 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 a collection of 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 - collection of VPN tunnels and their attributes. Network resources of different VPN Domains can securely communicate with each other through VPN tunnels that terminate at the Security Gateways in the VPN communities.

VPN communities are based on Star and Mesh topologies. In a Mesh community, there are VPN tunnels between each pair of Security Gateway. In a Star community, each satellite Security Gateway has a VPN tunnel to the central Security Gateway, but not to other Security Gateways in the community.

**Note** - Global VPN Communities are not supported in this release.
Creating VPN Policies

### Mesh Topology

2. For Star topology, satellite Security Gateways.

### Star Topology

1. London Security Gateway
2. New York Security Gateway
3. London - New York Mesh community
4. London company partner (external network)
5. London Star community
6. New York company partner (external network)
7. New York Star community
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.

**Note** - For each VPN gateway, you must configure an existing gateway as a default gateway.

**Domain Based VPN**

The VPN traffic is routed according to the VPN Domains that are defined in R80 SmartConsole. Use domain based routing to let satellite Security Gateways in a star-based topology send VPN traffic to each other. The central Security Gateway creates a VPN tunnel to each satellite gateway 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 28) 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 R80 SmartConsole, go to the Security Policies page.
2. In the Related Tools section, click VPN Communities.
3. Click New and select Star Community.

The New Star Community window opens.

4. Enter the name for the community.
5. From the navigation tree, select Encryption.
6. Configure the VPN encryption methods and algorithms for the VPN community.
7. Click OK.

To configure star VPN for the Security Gateways:

For each Security Gateway in the VPN community, follow these configuration steps.

1. In R80 SmartConsole, go to the Gateways & Servers page and double-click the Security Gateway object.

   The gateway properties window opens.

2. In the Network Security section of the General Properties page, select IPsec VPN.
3. From the navigation tree, go to Network Management > VPN Domain.
   
   - For the central Security Gateway, click Manually defined and select the Internal-network object
   
   - For a satellite Security Gateway, select All IP addresses

4. From the navigation tree, click IPsec VPN.
5. 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.

6. Click OK.

After you create a community and configure Security Gateways, add those Security Gateways to the community as a center or as a satellite gateway.

To add a Security Gateway to a new star community:

1. In R80 SmartConsole, go to the Security Policies page.
2. In the Related Tools section, click VPN Communities.
3. Select the new start community and click Edit.

   The Star Community window opens.
4. In the **Gateways** page, add Security Gateways to the community:
   - **Center Gateways** - Click **Add** and select center gateways. Select **Mesh center gateways**, if necessary.
   - **Satellite Gateways** - Click **Add** and select satellite gateways.

5. Click **OK**.

Allowing VPN Connections

To allow VPN connections between Security Gateways in specific VPN communities, add Access Control rules that accept such connections.

To allow all VPN traffic to hosts and clients on the internal networks of a specific VPN community, select **Allow All Encrypted traffic** in the **Encrypted Traffic** section of the properties configuration window for that VPN Community.

Sample VPN Access Control Rules

This table shows sample VPN rules for an Access Control 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>1</td>
<td></td>
<td>Any</td>
<td>NOT Member Gateways</td>
<td>BranchOffices</td>
<td>Encrypted Services</td>
<td>BranchOffices LondonOffices</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>LondonOffices</td>
<td></td>
<td></td>
<td></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>
<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>

1. Automatic rule that R80 SmartConsole adds to the top of the Rule Base when the **Accept All Encrypted Traffic** configuration option is selected for the **BranchOffices** VPN community and the **LondonOffices** VPN community. This rule is installed on all the Security Gateways in these communities. It allows all VPN traffic to hosts and clients on the internal networks of these communities. Traffic that is sent to the Security Gateways in these VPN communities is dropped.

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

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 Remote Access 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 28).

Note - For each VPN gateway, you must configure an existing gateway as a default gateway.

VPN Connectivity Modes

When securely connecting remote clients with the internal resources, organizations face connectivity challenges, such as these:

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

The Check Point IPSec VPN Software Blade provides these VPN connectivity modes to help organizations resolve those challenges:

- **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 avoid VPN routing problems.

- **Visitor Mode**
  Remote users can be restricted to using only HTTP and HTTPS protocols. Visitor Mode lets these users tunnel all protocols through regular TCP connections on port 443.

Sample Remote Access VPN Workflow

Here is an example of a remote access VPN workflow:

1. Use R80 SmartConsole to enable remote access VPN on the Security Gateway.
2. Add the remote user information to the Security Management Server:
   - Create and configure an LDAP Account Unit
   - Enter the information in the R80 SmartConsole user database
3. Configure the gateway for remote user authentication (optional).
4. Define the gateway Access Control and encryption rules.
5. Create the group objects to use in the gateway rules:
   - **LDAP Group** object - for an LDAP Account Unit
   - **User Group** object - for users configured in the R80 SmartConsole user database
6. Create and configure the encryption settings for the VPN community object.
7. Add Access Control rules to the Security Gateway Rule Base to allow VPN traffic to the internal networks.
Creating VPN Policies

Enable remote access VPN

Configure LDAP
Account Unit

Manage Users?

R80 Smart
Console

Configure users

Configure user authentication

Create LDAP user group object

Create VPN Community

Configure rules for VPN access in Firewall Rule Base

Install policy

Configure LDAP user group object

Configure user authentication

Create user group object
Adding Users to the Security Policy

In This Section:

- Using Identity Awareness ................................................................. 46
- Using User Directory ........................................................................... 50
- Adding Users to the Rule Base ......................................................... 56

Using Identity Awareness

The Identity Awareness Software Blade lets you configure the Security Gateways to enforce access control for individual users and groups. You can use Identity Sources to get information about users and groups to add flexibility and security for the Rule Base. Identity Awareness lets you create rules in the Access Control and Threat Prevention Rule Bases.

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 gateway identifies the user based on the AD security event log, and enforces the appropriate Identity Awareness rule to the traffic that this user sends.

**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 web page 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 R80 SmartConsole 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 Configuration Wizard

Use the Identity Awareness Configuration wizard to configure how the Security Gateway gets information about users and computers.

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

To use the Identity Awareness configuration wizard:

1. In R80 SmartConsole, go to the Gateways & Servers page and double-click the Security Gateway object.
   The gateway properties window opens.

2. From the navigation tree, click General Properties.

3. From the Network Security tab, select Identity Awareness.
   The Identity Awareness Configuration wizard opens.

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 the Password.
   Make sure that the AD account has domain administrator privileges.
   \textit{Note} - you can also select Create new domain and configure a new AD (Active Directory) Account Unit object.

6. Click Connect.
   The message about user credentials shows.

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.
10. Install the policy.
Adding Users to the Security 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. In R80 SmartConsole, go to the Gateways & Servers page and double-click the Security Gateway object.
   The gateway properties window opens.
2. From the navigation tree, click Identity Awareness.
3. Select or clear Remote Access.
4. Click OK.
5. Install the policy.

Working with Access Roles

After you enable Identity Awareness, you create Access Role objects. You can use Access Role objects as source and/or destination parameter in a rule. Access role objects can include one or more of these objects:

- Networks
- Users and user groups
- Computers and computer groups
- Remote Access Clients

To create an Access Role object:
1. In R80 SmartConsole, open the Object Explorer (Ctrl+E).
2. Click New > Users > Access Role.
   The New Access Role window opens.
3. Enter a Name and Comment (optional).
4. On the Networks page, select one of these:
   - Any network
   - Specific networks - Click the plus sign and select a network - click the plus sign next to the network name or search for a known network
5. On the Users page, select one of these:
   - Any user
   - All identified users - Includes users identified by a supported authentication method.
   - Specific users - Click the plus sign and select a user - click the plus sign next to the username or search for a known user or user group.
6. On the Machines page, select one of these:
   - Any machine
   - All identified machines - Includes computers identified by a supported authentication method
   - Specific machines - Click the plus sign and select a device - click the plus sign next to the device name or search for a known device or group of devices

For computers that use Full Identity Agents, you can select (optional) Enforce IP Spoofing protection.

7. On the Remote Access Clients page, select the Allowed Clients or add new ones. For R77.xx Gateways or lower, you must choose Any.

8. Click OK.

Using Identity Awareness in the Access Control Policy

The Identity Awareness Software Blade lets you configure your Access Control Policy to allow connections for users regardless of what computer they are using. Use Access Role objects in the Source column of a rule, and Identity Awareness Software Blade will identify users based on those objects. You can also configure the Accept action to redirect traffic from an unidentified user to a Captive Portal.

Sample gateway workflow with Identity Awareness

The gateway inspects traffic that starts from a source that matches the Access Role object and 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 Access Role objects and the Accept action with the Action Settings option, to redirect HTTP traffic to a Captive Portal. The rule allows traffic when the users that match the source Access Role object are identified. If the Enable Identity Captive Portal option is enabled, the gateway identifies users this way:

1. The Identity Awareness source identifies the user
2. 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 More.
   The Action Settings window opens.
2. Select Enable Identity 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>
<tr>
<td></td>
<td>All_Domain_Users</td>
<td></td>
<td></td>
<td></td>
<td></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.

<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>

Account Units

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.

You can have a number of Account Units representing one or more LDAP servers. Users are divided among the branches of one Account Unit, or between different Account Units.

**Note:** When you enable the Identity Awareness and Mobile Access Software Blades, R80 SmartConsole opens a First Time Configuration Wizard. The **Active Directory Integration** window of this wizard lets you create a new AD Account Unit. After you complete the wizard, R80 SmartConsole creates the AD object and Account Unit.
Working with LDAP Account Units

Use the **LDAP Account Unit Properties** window in R80 SmartConsole to edit an existing Account Unit or to create a new one manually.

**To edit an existing LDAP Account Unit:**
1. In R80 SmartConsole, open the **Object Explorer** (Ctrl+E).
2. Select **Servers > LDAP Account Units**.
3. Right-click the LDAP Account Unit and select **Edit**.
   The **LDAP Account Unit Properties** window opens.
4. Edit the settings in these tabs:
   - **General** ("General Tab" on page 52) - Configure how the Security Management Server uses the Account Unit
   - **Servers** ("Configuring an LDAP Server" on page 53) - Manage LDAP servers that are used by this Account Unit
   - **Objects Management** ("Objects Management Tab" on page 54) - Configure the LDAP server for the Security Management Server to query and the branches to use
   - **Authentication** ("Authentication Tab" on page 54) - Configure the authentication scheme for the Account Unit
5. Click **OK**.
6. Install the policy.

**To create a new LDAP Account Unit:**
1. In the **Objects** tab, click **New > More > Server > LDAP Account unit**.
   The **LDAP Account Unit Properties** window opens.
2. Configure the settings on these tabs:
   - **General** ("General Tab" on page 52) - Configure how the Security Management Server uses the Account Unit
   - **Servers** ("Configuring an LDAP Server" on page 53) - Manage LDAP servers that are used by this Account Unit
   - **Objects Management** ("Objects Management Tab" on page 54) - Configure the LDAP server for the Security Management Server to query and the branches to use
   - **Authentication** ("Authentication Tab" on page 54) - Configure the authentication scheme for the Account Unit
3. Click **OK**.
4. Install the policy.

**General Tab**

These are the configuration fields in the **General** tab:
- **Name** - Name for the Account Unit
- **Comment** - Optional comment
- **Color** - Optional color associated with the Account Unit
- **Profile** - LDAP vendor
• **Domain** - Domain of the Active Directory servers, when the same user name is used in multiple Account Units (this value is also necessary for AD Query and SSO)

• **Prefix** - Prefix for non-Active Directory servers, when the same user name is used in multiple Account Units

• **Account Unit usage** - Select applicable 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 (User Directory must be enabled on the Security Management Server)
    
    **Note** - LDAP SSO (Single Sign On) is only supported for Account Unit objects that use **User Management**.

• **Active Directory Query** - This Active Directory server is used as an Identity Awareness source.
  
  **Note** - This option is only available if the **Profile** is set to **Microsoft_AD**.

• **Enable Unicode support** - Encoding for LDAP user information in non-English languages

• **Active Directory SSO configuration** - Click to configure Kerberos SSO for Active Directory - Domain Name, Account Name, Password, and Ticket encryption method

---

### Configuring an LDAP Server

You can add, edit, or delete LDAP server objects.

**To configure an LDAP server for the Account Unit:**

1. To add a new server, click **Add**. To edit an existing one, select it from the table and click **Edit**. The **LDAP Server Properties** window opens.

2. From the **Host** drop-down menu, select the server object.

   If necessary, create a new R80 SmartConsole server object:
   
   a) Click **New**.

   b) In the **New Host** window opens, enter the settings for the LDAP server.

   c) Click **OK**.

3. Enter the login credentials and the **Default priority**.

4. Select access permissions for the Check Point Gateways:
   
   • **Read data from this server**
   
   • **Write data to this server**

5. In the **Encryption** tab, configure the optional SSL encryption settings.

6. Click **OK**.

**To remove an LDAP server from the Account Unit:**

1. Select a server from the table.

2. Click **Remove**.

   If all the configured servers use the same login credentials, you can modify those simultaneously.
To configure the login credentials for all the servers simultaneously:

1. Click **Update Account Credentials**.
   The **Update Account to All Servers** window opens.
2. Enter the login credentials.
3. Click **OK**.

**Objects Management Tab**

Configure the LDAP server for the Security Management Server to query and the branches to fetch.

**Note** - Make sure there is LDAP connectivity between the Security Management Server and the LDAP Server that holds the management directory.

To configure LDAP query parameters:

1. From the **Manage objects on** drop-down menu, select the LDAP server object.
2. Click **Fetch branches**.
   The Security Management Server queries and shows the LDAP branches.
3. Configure **Branches in use**:
   - To add a branch, click **Add** and in the LDAP Branch Definition window that opens, enter a new **Branch Path**
   - To edit a branch, click **Edit** and in the LDAP Branch Definition window that opens, modify the **Branch Path**
   - To delete a branch, select it and click **Delete**
4. Select **Prompt for password when opening this Account Unit**, if necessary (optional).
5. Configure the number of **Return entries** that are stored in the LDAP database (the default is 500).

**Authentication Tab**

These are the configuration fields in the Authentication tab:

- **Use common group path for queries** - Select to use one path for all the LDAP group objects (only one query is necessary for the group objects)
- **Allowed authentication schemes** - Select one or more authentication schemes allowed to authenticate users in this Account Unit - **Check Point Password**, **SecurID**, **RADIUS**, **OS Password**, or **TACACS**
- **Users' default values** - The default settings for new LDAP users:
  - **User template** - Template that you created
  - **Default authentication scheme** - one of the authentication schemes selected in the **Allowed authentication schemes** section
• Limit login failures (optional):
  • Lock user’s account after - Number of login failures, after which the account gets locked
  • Unlock user’s account after - Number of seconds, after which the locked account becomes unlocked
• IKE pre-shared secret encryption key - Pre-shared secret key for IKE users in this Account Unit

Enabling User Directory

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

To enable User Directory on the Security Management Server:

1. From the Menu, select Global Properties.
   The Global Properties window opens.
3. Configure other login and password settings.
4. Click OK.
5. Make sure that the User Directory Software Blade is enabled:
   a) In R80 SmartConsole, open the Object Explorer (Ctrl+E).
   b) Go to Network Objects >Gateways and Servers.
   c) Double-click the Management Server object.
      The object properties window opens.
   e) Click OK.
   f) Click Close.
6. Install the policy.

Managing LDAP Information

User Directory lets you use R80 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 object 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 SmartConsole 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 Software Blades let you add users, networks, gateways, and other objects into single R80 SmartConsole Access Role objects, and then use those objects as source and destination criteria in the Access Control Policy rules. The User Directory Software Blade works with the LDAP server to update user information. You can also easily update user information through R80 SmartConsole.

### Adding an Access Role to a Rule

You can add rules with Access Role objects as the **Source** or **Destination** to the Access Control policy for Security Gateways that have the Identity Awareness Software Blade enabled.

**Note** - Rules that use Access Role objects cannot be enforced on Security Gateways that do not have Identity Awareness enabled.

**To add an Access Role object to a rule:**

1. Select a policy from the **Access Control > Policy** tree.
2. Click the plus sign in the **Source** or the **Destination** cell of a rule.
3. In the window that opens, click the **Filter** button and select **Categories > Users > Access Roles**.
4. Click the plus sign for every Access Role object you want to add.
5. Install the policy.
Defining an Internet Access Policy

In This Section:
- Managing URL Filtering and Application Control ........................................57
- HTTPS Inspection ............................................................................................62
- Configuring the Geo Policy .............................................................................70

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 and violence.

The Check Point Solution for Internet Browsing

The Check Point URL Filtering and Application Control Software Blades can help organizations of all sizes monitor and control the use of Internet by their employees. You can easily create policies which identify or block thousands of applications and Internet sites.

Use the URL Filtering and Application Control Software Blades 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 Security Gateways to inspect HTTPS traffic and prevent security risks related to the SSL protocol.

- **Manage Bandwidth Consumption** - Configure rules to limit the available network bandwidth for specified users or groups. You can define separate limits for uploading and downloading.

- **Keep Your Policies Updated** - The Application Database is updated regularly, which helps you make sure that your Internet security policy has the newest applications and website categories. Security Gateways connect to the Check Point Online Web Service to identify new social networking widgets and website categories.

- **Communicate with Users** - UserCheck objects add flexibility to URL Filtering and Application Control and let the Security Gateways communicate with users. UserCheck helps users understand that certain websites are against the company’s security policy. It also tells users about the changes in Internet policy related to websites and applications.
• **Create Custom Objects** - In addition to the hundreds of default objects, you can create custom objects, to better manage the use of Internet by your users. Create objects for applications, websites, categories and groups, and use them in your security policy rules.

**UserCheck**

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

- Inform
- Ask
- Drop

**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, such as Skype and 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**

To enable R80 Application Control and URL Filtering for pre-R80 gateways, enable the Application Control and URL Filtering Software Blades on each gateway. Then, if necessary, create a second Layer for the Application Control and URL Filtering rules. Configure this second Layer for the Access Control Policy.

**To enable URL Filtering and Application Control Software Blades on a Security Gateway:**

1. In R80 SmartConsole, go to **Gateways & Servers** and double-click the gateway object. The **General Properties** window of the gateway opens.
2. From the navigation tree, click **General Properties**.
3. In the **Network Security** tab, select **URL Filtering**, or **Application Control**, or both.
4. Click **OK**.

**To create a second Layer for URL Filtering and Application Control:**

1. In R80 SmartConsole, go to **Security Policies**.
2. Right-click a Layer in the **Access Control** Policy section and select **Edit Policy**. The **Policy** window opens and shows the **General** view.
3. In the **Access Control** section, click the plus sign.
4. Click **New Layer**.
   The **Layer Editor** window opens and shows the **General** view.

5. Enable Application Control and URL Filtering on the Layer.
   a) In the **Blades** section, enter a name for the Layer.
      We recommend the name **Application**.
   b) Click **Application Control and URL Filtering**.
   c) Click **OK** and the **Layer Editor** window closes.
   d) Click **OK** and the **Policy** window closes.

6. Install the policy.

The Columns of the Access Control Rule Base

These are the fields of the rules in the Access Control policy. Not all of these are shown by default. To select a field that does not show, right-click on the Rule Base table header, and select it.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Rule number in the Rule Base Layer.</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>Services &amp; Applications</td>
<td>Services, protocols, applications, and 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>Accept</strong>, <strong>Drop</strong>, <strong>Ask</strong>, <strong>Inform</strong> (UserCheck message), and <strong>Reject</strong>.</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>

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 Access Control Policy Rule Base uses these fields to create a strong and flexible URL Filtering and Application Control security policy:

- **Services & Applications**
- **Action**
Services & Applications

In the Services & Applications column, define the Web applications, sites, services and protocols that are included in the rule. A rule can contain one or more:

- Web applications
- Web sites
- Services
- Default categories of Internet traffic
- Custom groups or categories that you create, that are not included in the Check Point Application Database.

Notes -

It is not supported to configure a service and application in the same rule.

Applications are matched on their Recommended services, where each service runs on a specific port. The recommended services for Facebook, for example, are the default Application Control Web browsing services: http, https, HTTP_proxy, and HTTPS_proxy.

To add an application or site to a rule:
1. In the Security Policies view of R80 SmartConsole, go to the Access Control Policy.
2. Select the Application Control Layer.
3. Right-click the Services & Applications cell for the rule and select Add New Items.
   The Application viewer window opens.
4. Search for the applications or categories.
5. Click the + next to the ones you want to add.

To create a new application or site:
1. In the Security Policies view of R80 SmartConsole, go to the Access Control Policy.
2. Select the Application Control Layer.
3. Right-click the Services & Applications cell for the rule and select Add New Items.
   The Application viewer window opens.
4. Click New > Custom Applications/Site > User Application.
5. Enter a name for the object.
6. Enter one or more URLs.
   If you used a regular expression in the URL, click URLs are defined as Regular Expressions.
   Note - If the application or site URL is defined as a regular expression you must use the correct syntax.
7. Click OK.

To create a custom category:
1. In the Security Policies view of R80 SmartConsole, go to the Access Control Policy.
2. Select the Application Control Layer.
3. Right-click the Services & Applications cell for the rule and select Add New Items.
   The Application viewer window opens.
4. Click New > Custom Applications/Site > User Category.
5. Enter a name for the object.
6. Enter a description for the object.
7. Click OK.

**Action**

In the **Action** field, 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>Accept</td>
<td>Allows the traffic.</td>
</tr>
<tr>
<td>Drop</td>
<td>Blocks the traffic. Optionally, shows a UserCheck <strong>Block</strong> message.</td>
</tr>
<tr>
<td>Limit</td>
<td>Limits the bandwidth that is permitted for a rule. Add a Limit object to configure a maximum throughput for uploads and downloads.</td>
</tr>
<tr>
<td>Enable Identity Captive Portal</td>
<td>Redirects HTTP traffic to an authentication (captive) portal. After the user is authenticated, new connections from this source are inspected without requiring authentication.</td>
</tr>
</tbody>
</table>

**UserCheck Actions**

These are the **Action** options that work with UserCheck:

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop</td>
<td>Blocks the traffic. Optionally, shows a UserCheck <strong>Block</strong> message.</td>
</tr>
<tr>
<td>Ask</td>
<td>Shows a UserCheck <strong>Ask</strong> message. The message asks users to confirm that it is necessary that they go to the application or site.</td>
</tr>
<tr>
<td>Inform</td>
<td>Sends a message to the user attempting to access the application</td>
</tr>
<tr>
<td>UserCheck Frequency</td>
<td>Defines how often users see the UserCheck message for Ask, Inform, or Block actions.</td>
</tr>
</tbody>
</table>

**Confirm UserCheck**

Select the action that triggers a UserCheck message:
- **Per rule** - UserCheck message shows only once when traffic matches a rule.
- **Per category** - UserCheck message shows for each matching category in a rule.
- **Per application/Site** - UserCheck message shows for each matching application in a rule.
- **Per Data type** - UserCheck message shows for each matching data type.
Sample URL Filtering and Application Control Rules

This table shows some examples of URL Filtering and Application Control rules 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 Message</td>
<td>Log</td>
<td>Any</td>
</tr>
<tr>
<td>3</td>
<td>Allow IT department Remote Admin</td>
<td>IT</td>
<td>Any</td>
<td>Radmin</td>
<td>Allow</td>
<td>Log</td>
<td>Work-Hours</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>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 explains 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 the Work-Hours (set to 8:00 through 18:30, for example).

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.

   **Note** - 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. Security Gateways cannot inspect HTTPS traffic because it is encrypted. You can enable the HTTPS Inspection feature to let the Security Gateways create new SSL connections with the external site or server. The Security Gateways are 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 arrive from the Internet or an external network.

A 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 such a log.

**Inspecting HTTPS Packets**

**Outbound Connections**

Outbound connections are HTTPS connections that arrive from an internal client and connect to the Internet. The Security Gateway compares the HTTPS request to the rules in the HTTPS Inspection Rule Base. If the request does not match any rule, the packet is not inspected and the connection is allowed.

If the request matches an HTTPS Inspection rule, the Security Gateway validates the certificate from the server (on the Internet). For a new HTTPS connection to the server, the Security Gateway creates and uses a new certificate. There are two HTTPS connections, one to the internal client and one to the external server. It can then decrypt and inspect the packets according to the security policy. The packets are encrypted again and sent to the destination.

**Inbound Connections**

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

If the request matches an HTTPS Inspection rule, the Security Gateway uses the certificate for the internal server to create an HTTPS connection with the external client. The Security Gateway creates a new HTTPS connection with the internal server. Since the Security Gateway has a secure
connection with the external client, it can decrypt the HTTPS traffic. The decrypted traffic is inspected according to the security policy.

![Diagram of connection and inspection process]

**Configuring Security Gateways to inspect outbound and inbound HTTPS**

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

**Workflow overview**

1. Enable HTTPS Inspection on the Security Gateway.
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 Access Control Policy.

**Enabling HTTPS Inspection**

You must enable HTTPS inspection on each Security Gateway. From **Security Gateway >HTTPS Inspection >Step 3**, select **Enable HTTPS Inspection**.

The first time you enable HTTPS inspection on one of the Security Gateways, you must create an outbound CA certificate for HTTPS inspection or import a CA certificate already deployed in your organization. This outbound certificate is used by all Security Gateways managed on the Management Server.

**Creating an Outbound CA Certificate**

The outbound CA certificate is saved with a P12 file extension and uses a password to encrypt the private key of the file. The Security Gateways use this password to sign certificates for the sites...
accessed. You must keep the password as it also used by other Management Servers that import the CA certificate to decrypt the file.

After you create an outbound CA certificate, you must export it so it can be distributed to clients. If you do not deploy the generated outbound CA certificate on clients, users will receive SSL error messages in their browsers when connecting to HTTPS sites. You can configure a troubleshooting option that logs such connections.

After you create the outbound CA certificate, a certificate object named Outbound Certificate is created. Use this object in rules that inspect outbound HTTPS traffic in the HTTPS inspection Rule Base.

**To create an outbound CA certificate:**

1. In R80 SmartConsole, go **Manage & Settings > Blades > HTTPS Inspection > Configure In SmartDashboard**.
2. In SmartDashboard, right-click the Security Gateway object and select **Edit**. The **Gateway Properties** window opens.
3. In the navigation tree, select **HTTPS Inspection**.
4. In the HTTPS Inspection page, click **Create**.
5. 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.
6. Click **OK**.
7. Export and deploy the CA certificate (**"Exporting and Deploying the Generated CA" on page 66**).

**Importing an Outbound CA Certificate**

You can import a CA certificate that is already deployed in your organization or import a CA certificate created on one Management Server to use on another Management Server.

**Note** - It is recommended that you use **private** CA Certificates.

For each Management Server that has Security Gateways enabled with HTTPS inspection, you must:

- Import the CA certificate.
- Enter the password the Management Server uses to decrypt the CA certificate file and sign the certificates for users. This password is only used when you import the certificate to a new Management Server.

**To import a CA certificate:**

1. If the CA certificate was created on another Management Server, export the certificate from the Management Server on which it was created (**"Exporting a Certificate from the Management Server" on page 66**).
2. In SmartConsole, right-click a Security Gateway object, select **Edit > HTTPS Inspection > Import**
   The Import Outbound Certificate window opens.
4. Enter the **private key password**.
5. Click **OK**.
6. If the CA certificate was created on another Management Server, deploy it to clients ("Exporting and Deploying the Generated CA" on page 66).

**Exporting a Certificate from the Management Server**

If you use more than one Management Server in your organization, you must **first** export the CA certificate using the `export_https_cert` CLI command from the Management Server on which it was created before you can import it to other Management Servers.

Command syntax:

```
export_https_cert [-local] | [-s server] [-f certificate file name under FWDIR/tmp][-help]
```

**To export the CA certificate:**

On the Management Server, run this command:

```
$FWDIR/bin/export_https_cert -local -f [certificate file name under FWDIR/tmp]
```

**Example**

```
$FWDIR/bin/export_https_cert -local -f mycompany.p12
```

**Exporting and Deploying the Generated CA**

To prevent users from getting warnings about the generated CA certificates that HTTPS inspection uses, install the generated CA certificate used by HTTPS inspection as a trusted CA. You can distribute the CA with different distribution mechanisms such as Windows GPO. This adds the generated CA to the trusted root certificates repository on client computers.

When users run standard updates, the generated CA will be in the CA list and they will not receive browser certificate warnings.

**To distribute a certificate with a GPO:**

1. From the **HTTPS Inspection** window of the Security Gateway, click **Export certificate**.
2. Save the CA certificate file.
3. Use the Group Policy Management Console ("Deploying Certificates by Using Group Policy" on page 66) to add the certificate to the Trusted Root Certification Authorities certificate store.
4. Push the Policy to the client computers in the organization.
   **Note** - Make sure that the CA certificate is pushed to the client computer organizational unit.
5. Test the distribution by browsing to an HTTPS site from one of the clients and verifying that the CA certificate shows the name you entered for the CA certificate that you created in the **Issued by** field.

**Deploying Certificates by Using Group Policy**

You can use this procedure to deploy a certificate to multiple client machines by using Active Directory Domain Services and a Group Policy object (GPO). A GPO can contain multiple configuration options, and is applied to all computers that are within the scope of the GPO.

Membership in the local Administrators group, or equivalent, is necessary to complete this procedure.
To deploy a certificate using Group Policy:

1. On the Microsoft Windows Server, open the Group Policy Management Console.
2. Find an existing GPO or create a new GPO to contain the certificate settings. Make sure the GPO is associated with the domain, site, or organization unit whose users you want affected by the policy.
3. Right-click the GPO and select Edit.
   The Group Policy Management Editor opens and shows the current contents of the policy object.
5. Click Action > Import.
6. Do the instructions in the Certificate Import Wizard to find and import the certificate you exported from SmartConsole.
7. In the navigation pane, click Trusted Root Certification Authorities and repeat steps 5-6 to install a copy of the certificate to that store.

Configuring Inbound HTTPS Inspection

To enable inbound HTTPS traffic inspection:

2. Import server certificates for servers behind the organization Security Gateways (“Server Certificates” on page 67).
4. Configure the relevant server certificate in the HTTPS inspection Rule Base.

Server Certificates

When a client from outside the organization initiates an HTTPS connection to an internal server, the Security Gateway intercepts the traffic. The Security Gateway inspects the inbound traffic and creates a new HTTPS connection from the gateway to the internal server. To allow seamless HTTPS inspection, the Security Gateway must use the original server certificate and private key.

To assign the certificate for Inbound HTTPS inspection:

1. Add the server certificates to the Security Gateway.
   This creates a server certificate object (“Adding a Server Certificate” on page 68).
2. Add the server certificate object to the Certificate column in the HTTPS Inspection Policy, to enforce it in rules.
   The Server Certificates window in SmartDashboard has these options:
   - **Add** - Import a new server certificate. Enter a name for the server certificate, optional comment and import the P12 certificate file.
   - **Delete** - Delete a previously added server certificate. This option does not delete the server certificate option. It only removes it from the Server Certificate list.
   - **Search** - Enter a key word to search for a server certificate in the list.
Adding a Server Certificate

When you import a server certificate, enter the same password that was entered to protect the private key of the certificate on the server. The Security Gateway uses this certificate and the private key for SSL connections to the internal servers.

After you import a server certificate (with a P12 file extension) to the Security Gateway, make sure you add the object to the HTTPS Inspection Policy.

Do this procedure for all servers that receive connection requests from clients outside of the organization.

To add a server certificate:
1. In SmartConsole, open HTTPS Inspection >Server Certificates.
2. Click Add.
   The Import Certificate window opens.
3. Enter a Certificate name and a Description (optional).
5. Enter the Private key password.
6. Click OK.

The Successful Import window opens the first time you import a server certificate. It shows you where to add the object in the HTTPS Inspection Rule Base. Click Don’t show this again if you do not want to see the window each time you import a server certificate and Close.

HTTPS Inspection Policy

The HTTPS Inspection rules define how the Security Gateways inspect 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 rules are applied to all the Software Blades that have HTTPS Inspection enabled. These are the Software Blades that support HTTPS Inspection:
- Application Control
- URL Filtering
- IPS
- DLP
- Anti-Virus
- Anti-Bot

HTTPS Inspection rules in R80 SmartConsole

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>
</tbody>
</table>
Defining an Internet Access Policy

**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. The inbound rules use a different certificate for each internal server. 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 HTTPS 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 HTTPHTTPS_proxy</td>
<td>Financial Services</td>
<td>Bypass</td>
<td>Any</td>
<td>Outbound CA</td>
</tr>
<tr>
<td>2</td>
<td>Outbound traffic</td>
<td>Any</td>
<td>Internet</td>
<td>HTTPS HTTPHTTPS_proxy</td>
<td>Any</td>
<td>Inspect</td>
<td>Any</td>
<td>Outbound CA</td>
</tr>
<tr>
<td>3</td>
<td>Inbound traffic</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** - This is a bypass rule that 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.

Field | Description
--- | ---
Destination | Network object that defines the destination of the traffic.
Services | Type of network service that is inspected or bypassed.
Site Category | Categories for applications or web sites that are inspected or bypassed.
Action | Action that is done when HTTPS traffic matches the rule. The traffic is inspected or ignored (Bypass).
Track | Tracking and logging action that is done when traffic matches the rule.
Install On | Network objects that will get the HTTPS Inspection rule. You can only select Security Gateways that have HTTPS Inspection enabled.
Certificate | The certificate that is used for this rule.
  - Inbound HTTPS inspection - Select the certificate that the internal server uses.
  - Outbound HTTPS inspection - Select the Outbound Certificate object that you are using for the computers in the network.
Comment | An optional field that lets you summarize the rule.
Configuring the Geo Policy

The Geo Policy lets you control network traffic for specified countries. An IP-to-country database maps IP addresses to countries. You can configure different Geo policies that block or allow traffic for different countries. Private IP addresses are allowed unless 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 policy.

Follow this workflow to configure a Geo Policy:

1. Create a Geo Policy.
2. Configure exceptions to the policy (optional).
3. Apply the new Geo Policy to target Security Gateways.
4. Publish the configuration changes and install the Access Control Policy.

To create a new Geo Policy:

1. In R80 SmartConsole, go to the Security Policies page.
2. In the Shared Policies section, click Geo Policy.
3. From the drop-down Edited Policy menu, select New.
4. In the Object Name window that opens, enter a name for the new Geo Policy.
5. Click OK.
6. Select an Activation Mode:
   - Active - Policy is enabled
   - Monitory Only - Traffic that matches the policy is allowed and logged
   - Inactive - Policy is disabled
7. In Policy for specific countries section, click the plus sign.
   The Geo Policy - Add new rule window opens.
8. Configure the Rule Settings:
   - Country - Select or search for a country on the list
   - Action - Select Accept to allow the traffic or Drop to reject it
   - Direction - From and To Country for bidirectional traffic, or To Country or From Country for traffic only in a specific direction
   - Track - Select to Log, send Alerts, send Mail, send SNMP Traps, or to send one of possible three custom User Alerts (you can also choose to not do any tracking)
   - Comment - optional comment
9. Set the default Action and Track option for the Policy for other countries.
10. Optional - Select Aggregate logs by country.
11. Publish the Session to save the configuration changes.

To configure exceptions to a Geo Policy:

1. In the Shared Policies section of the Security Policies page, click Exceptions.
2. Click New.
   The New Exception Rule window opens.
3. In the Apply to section, select the Profile to which you want to apply the exception.
4. In the **Source** and **Destination** sections, select the exception criteria:
   - **Network Object** - A specific internal host or a network (or **Any**)
   - **IP Address** - A specific IP address
5. Select a **Service** or specify a **TCP** or **UDP Port/Range**.
6. Select the target gateways for the exception to **Install On**.
7. Add an optional **Comment** and click **OK**.

**To apply a Geo Policy:**
1. In the **Shared Policies** section of the **Security Policies** page, click **Gateways**.
2. Select a gateway or a cluster of gateways and click **Edit**.
   - The gateway **Geo Policy** window opens.
3. From the Assign Policy drop-down list, select a Geo Policy.
4. Click **OK**.

You can also edit Geo Policies, or delete them (if they are not applied to any target gateways).

**To delete a Geo Policy:**
1. In the **Shared Policies** section of the **Security Policies** page, click **Gateways**.
2. From the **Edited Policy** drop-down list, select a policy.
   - The rules of the selected Geo Policy show.
3. Click to open the **Edited Policy** list again, and select **Delete**.
4. Click **Yes** to confirm.
   - **Note** - If the policy is applied to a gateway or a cluster of gateways, the warning will show and the policy will not be deleted.

**To edit a Geo Policy:**
1. In the **Shared Policies** section of the **Security Policies** page, click **Gateways**.
2. From the **Edited Policy** drop-down list, select a policy.
   - The rules of the selected Geo Policy show.
3. Make changes to the policy.
4. Publish the changes and install the Access Control Policy.
Creating a Threat Prevention Policy

In This Section:
- Threat Prevention Components ................................................................. 72
- ThreatSpect Engine and ThreatCloud Repository ....................................... 73
- Learning about Malware ............................................................................... 73
- IPS ............................................................................................................. 73
- Anti-Bot ..................................................................................................... 78
- Anti-Virus ................................................................................................. 79
- Anti-Bot and Anti-Virus Rule Base ............................................................. 80
- Threat Emulation ....................................................................................... 82
- Creating a Threat Prevention Policy ......................................................... 84
- Creating Rules ........................................................................................... 88
- Installing the Threat Prevention Policy ....................................................... 93
- Updating the IPS and Malware Databases ................................................. 93
- Anti-Spam ................................................................................................. 95

Threat Prevention Components

To challenge today's malware landscape, Check Point's comprehensive Threat Prevention solution offers a multi-layered, pre- and post-infection defense approach and a consolidated platform that enables enterprise security to detect and block modern malware. These Threat Prevention Software Blades are available:

- **IPS** - A complete IPS network security solution, for comprehensive protection against malicious and unwanted network traffic, focusing on application and server vulnerabilities.
- **Anti-Bot** - Post-infection detection of bots on hosts. Prevents bot damages by blocking bot C&C (Command and Control) communications. The Anti-Bot Software Blade is continuously updated from ThreatCloud, a collaborative network to fight cybercrime. Anti-Bot discovers infections by correlating multiple detection methods.
- **Anti-Virus** - Pre-infection detection and blocking of malware at the gateway. The Anti-Virus Software Blade is continuously updated from ThreatCloud. It detects and blocks malware by correlating multiple detection engines before users are affected.
- **Threat Emulation** - Protection against infections from undiscovered exploits, zero-day and targeted attacks. This innovative solution quickly inspects files and runs them in a virtual sandbox to discover malicious behavior. Discovered malware is prevented from entering the network. The ThreatCloud Emulation service reports to the ThreatCloud and automatically shares the newly identified threat information with other Check Point customers.

Each Software Blade gives unique network protections. When combined, they supply a strong Threat Prevention solution. Data from malicious attacks are shared between the Threat Prevention Software Blades and help to keep your network safe. For example, the signatures from threats that Threat Emulation identifies are added to the Anti-Virus database.
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 operators, 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. You can filter by category, tag, malware family, and search for malware.

**To show the Threat Wiki:**

1. In R80 SmartConsole, go to the **Security Policies** page, and select **Threat Prevention**.
2. In the **Related Tools** section, click **Threat Wiki**.
   
   The Threat Wiki web page opens.

IPS

Overview of IPS

The Check Point IPS Software Blade analyzes traffic for possible risks, to enhance the network security of your organization. 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, because it identifies and then blocks the drive-by-download connection.
Creating a Threat Prevention Policy

Enabling the IPS Software Blade

To enable the IPS Software Blade on a Security Gateway:

1. In R80 SmartConsole, go to Gateways & Servers and double-click the gateway object. The General Properties window opens.
2. In the General Properties > Network Security section, click IPS.
3. Click OK.
4. Follow the steps in the wizard that opens.
5. Install the Access Control policy.

Choosing the Level of Protection

Check Point IPS provides instant protection based on pre-defined Threat Prevention Profiles. You can also configure a custom Threat Prevention profile (see "Threat Prevention Profiles" on page 87) to give the exact level of protection for your organization.

When you install an Access Control policy on the Security Gateways, they immediately begin to enforce IPS protection on network traffic.

Default IPS Protection Profiles

R80 SmartConsole includes these default Threat Prevention profiles:

- **Optimized** - Provides excellent protection for common network products and protocols against recent or popular attacks
- **Strict** - Provides a wide coverage for all products and protocols, with impact on network performance
- **Basic** - Provides reliable protection on a range of non-HTTP protocols for servers, with minimal impact on network performance

Using the Optimized Profile

The Optimized profile is activated by default, because it gives excellent security with good gateway performance. These are the goals of the Optimized profile:

- Apply settings to all the Threat Prevention Software Blades
- Avoid impact on the gateway performance
- Protect against important threats
- Reduces false-positives

Newly downloaded IPS protections are set to Detect the intrusion attempts. They are activated according to the IPS Updates Policy.

Customizing IPS Protections for Your Network

For additional granularity, in the Additional Activation section of the Profile configuration window, you can select IPS protections to activate and to deactivate. The IPS protections are arranged into categories such as Product, Vendor, Threat Year, and others, for the ease of search. Activated protections are enforced by gateways, and the deactivated protections are not enforced, regardless of the general profile protection settings.
**Configuring IPS Profile Settings**

To configure the IPS settings for a Threat Prevention profile:

1. In R80 SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.
   The **Profiles** page opens.
3. Right-click the profile, and click **Edit**.
4. From the navigation tree, click **IPS > Additional Activation**.
5. Configure the customized protections for the profile.
6. From the navigation tree, click **IPS > Updates**.
7. Configure the settings for newly downloaded IPS protections.
8. If you are importing IPS profiles from a pre-R80 deployment:
   a) From the navigation tree, click **IPS > Pre-R80 Settings**.
   b) Activate the applicable **Client** and **Server** protections.
   c) Configure the IPS protection categories to exclude from this profile.
   
   **Note** - These categories are different from the protections in the **Additional Activation** page.
9. Click **OK**.
10. Install the Access Control policy.

**Additional Activation Fields**

- **Activate IPS protections according to the following additional properties** - When selected, the categories configured on this page modify the profile’s IPS protections.
  - **Protections to activate** - The IPS protection categories in this section are enabled on the Security Gateways that use this Threat Prevention profile.
  - **Protections to deactivate** - The IPS protection categories in this section are NOT enabled on the Security Gateways that use this Threat Prevention profile.

These categories will only filter out or add protections that comply with the activation mode thresholds (Confidence, Severity, Performance).

For example, if a protection is inactive because of its Performance rating, it will not be enabled even if its category is in **Protections to activate**.

**Changing the Assigned Profile**

To assign an IPS profile:

1. In R80 SmartConsole, select **Security Policies > Threat Prevention > Policy > IPS**.
2. In the rule, right-click the **Action** cell.
3. Select the Threat Prevention profile with the applicable IPS settings.
4. Install the Access Control policy.
Browsing IPS Protections

The **IPS Protections** summary lets you quickly browse all IPS protections and their settings. The **IPS Protections** window lets you use the specified categories and tags to easily filter for IPS protections. For example, the **Vendor** category contains the **Oracle** tag with the IPS protections for **Oracle** products. You can also:

- Find IPS protections using the **Filters**:
  - Default filters: **Activations, Severity, Confidence Level, Performance Impact, and Type**
  - Predefined filters: Click the **Add filter** button
- Change the **Action** for selected profiles (overrides the profile setting) ("Activating Protections for a Profile" on page 77)

**Filtering IPS Protections**

**To show the IPS protections:**

1. In R80 SmartConsole, go to the **Security Policies** page and select **Threat Prevention**.
2. In the **Related Tools** section, click **IPS Protections**.

**To filter the protections:**

1. From the **IPS Protections** window, click the **Filter** icon.
   - The **Filters** pane opens and shows IPS protections categories.
2. To add more categories:
   a) Click the **Add filter** button.
      - A window opens and shows the IPS protections categories.
   b) Click the category.
      - The category is added to the **Filters** pane.
3. Click one or more filters to apply to the IPS protections.
4. To show all the IPS protections in a category, click **View All**.

**IPS Protections Columns**

These are some of the default columns in the IPS protections summary table.

<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>Industry Reference</td>
<td>International CVE or CVE candidate name for attack.</td>
</tr>
<tr>
<td>Performance Impact</td>
<td>How this protection affects the performance of a Security Gateway.</td>
</tr>
<tr>
<td>Severity</td>
<td>Probable severity of a successful attack on your environment.</td>
</tr>
<tr>
<td>Confidence Level</td>
<td>How confident IPS is in recognizing the attack.</td>
</tr>
<tr>
<td>profile_name</td>
<td>The Activation setting for the protection for each IPS profile.</td>
</tr>
</tbody>
</table>
Activating Protections for a Profile

To manually activate a protection for a profile:
2. From the Threat Tools section, click IPS Protections.
   The IPS Protections page opens.
3. For the specified protection, find the column for the profile.
   Note - The default IPS profiles are not shown.
4. Right-click the cell for the protection and profile and select Edit.
   The Protection Details window opens.
5. From the Main Action section, click Override with.
6. Select the action to apply.
7. Click OK.
8. Install the Access Control policy.

Removing Activation Overrides

You can remove the manually activated IPS protections and restore them to the settings in the Threat Prevention profile.

To remove IPS protection overrides:
2. From the Threat Tools section, click IPS Protections.
   The IPS Protections page opens.
3. Click the cell for the profile column.
   Press CTRL to select more than one protection.
4. Right-click a highlighted cell and select Restore to profile settings.
   A warning message opens.
5. Click Yes.
6. Install the Access Control policy.

Adding Network Exceptions

You can configure exceptions for a protection with the Prevent action. IPS does not identify the traffic. We recommend that you use IPS exceptions to allow traffic that is legitimate for some computers or services can match the protection criteria for malware. You can also create an exception for a server that does not comply with RFC standards.

Adding an IPS Exception

To add a new exception:
1. In R80 SmartConsole, go to the Security Policies page and select Threat Prevention.
2. In the Related Tools section of the Threat Prevention Policy, click Profiles.
3. Right-click the profile and select Edit.
   The Profile window opens.
4. From the navigation tree, select **IPS > Pre R80 Settings**.
5. In the **Excluded Protections Categories** section, make sure that **Do not activate protections of the following categories** is selected.
6. Click the plus sign and select a protection category.
7. Repeat the previous step for each protection category.
8. Click **OK**.
9. Install the Access Control policy.

**Anti-Bot**

**Protecting Networks from Bots**

A bot is malicious software that can infect your computer. It is possible to infect a computer when you open attachments that exploit a vulnerability, or go to 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.

The Anti-Bot Software Blade detects and prevents these bot and botnet threats. A botnet is a collection of compromised and infected computers.

**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.

**Enabling the Anti-Bot Software Blade**

**To enable the Anti-Bot Software Blade on a Security Gateway:**

1. In R80 SmartConsole, go to *Gateways & Servers* and double-click the gateway object. The General Properties window of the gateway opens.
2. From the *Network Security* tab, click *Anti-Bot*. The Anti-Bot and Anti-Virus First Time Activation window opens.
3. Select an activation mode option:
   - **According to the Anti-Bot and Anti-Virus policy** - Enable the Anti-Bot Software Blade and use the Anti-Bot settings of the Threat Prevention profile in the Threat Prevention policy.
   - **Detect only** - Packets are allowed, but the traffic is logged according to the settings in the Threat Prevention Rule Base.
4. Click **OK**.
5. Install the Threat Prevention policy.

**Anti-Virus**

**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.

**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:**

1. In R80 SmartConsole, go to the Security Policies page, and select Threat Prevention.
2. In the Related Tools section, click Protections.
   A detailed summary of the protections is shown in the table.

The table of protections has these fields:

<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>The Software Blade, by which the protection is used - Anti-Bot or Anti-Virus.</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>
</tbody>
</table>
Creating a Threat Prevention Policy

Firewall Getting Started Guide Pre-R80 Security Gateways with R80 Security Management

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Update</td>
<td>The date when the most recent update.</td>
</tr>
</tbody>
</table>

When you select a protection in the table, the summary and the activation information are shown in the bottom part of the screen. The Summary tab is shown by default. To see the activation information, click the Activations tab.

The table in the Activations tab view shows information in the table with these fields:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>The profile name.</td>
</tr>
<tr>
<td>Action</td>
<td>The action that is configured in the profile for the selected protection:</td>
</tr>
<tr>
<td></td>
<td>- Ask - Asks user to select an action</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 - Disables the protection</td>
</tr>
</tbody>
</table>

Protections can have more than one action. The Action column shows the percentage of protections set to each action.

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 46) 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 Research and Development (R&D) 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>
</tbody>
</table>
Creating a Threat Prevention Policy

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>Protection</td>
<td>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.</td>
</tr>
<tr>
<td>Action</td>
<td>For rules, the value for this field is an Anti-Bot and Anti-Virus profile. For exceptions, set this field to Prevent or Detect.</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 get this rule. The default setting is All and installs the policy on all Security Gateways that have Anti-Bot and Anti-Virus enabled.</td>
</tr>
</tbody>
</table>

Sample Anti-Bot and Anti-Virus 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_than</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Corporate_corporate内部</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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>Optimized Profile</td>
<td>Log</td>
</tr>
<tr>
<td>E-2.1</td>
<td>R&amp;D Server</td>
<td>Server_1</td>
<td>Backdoor.Win32.Shark.A</td>
<td>Detect</td>
<td>Log</td>
</tr>
</tbody>
</table>

Rule number 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 the Logs & Monitor >Logs view.

Rule number 2, Malware Rule - All traffic in the network is inspected for bots and viruses according to the settings in the Optimized profile.

Exception 2.1 to rule 2, R&D Server - A global exception rule for the Server_1 object, that only detects the Backdoor.Win32.Shark.A protection.

Exception 2.2 to rule 2, Users_3 - An exception rule for the Users_3 Access Role, that sets some protections to Detect instead of Prevent.
Threat Emulation

The Need for Threat Emulation

Cyber-threats continue to multiply and now it is easier than ever for criminals to create new malware that can easily bypass existing protections. On a daily basis, these criminals can change the malware signature and make it virtually impossible for signature based products to protect networks against infection. Threat Emulation can protect your network against new malware, zero-day vulnerabilities and targeted attacks http://www.checkpoint.com/products/threat-emulation/index.html.

Threat Emulation gives networks the necessary protection against unknown threats in files that are downloaded from the Internet or attached to emails. When emulation is done on a file:

- The file is opened on more than one virtual computer with different operating system environments
- The virtual computers are closely monitored for unusual and malicious behavior, such as an attempt to change registry keys or run an unauthorized process
- Any malicious behavior is immediately logged and you can use Prevent mode to block the file from the internal network
- The cryptographic hash of a new malicious file is saved to a database and the internal network is protected from that malware
- Information about malicious files and malware is shared with Check Point ThreatCloud and helps to protect all ThreatCloud users

ThreatCloud Emulation

You can securely send files to the Check Point ThreatCloud for emulation. The ThreatCloud is always up-to-date with the latest Threat Emulation releases.

Sample ThreatCloud Emulation Workflow

1. The Security Gateway gets a file from the Internet or an external network.
2. The Security Gateway compares the cryptographic hash of the file with the database.
   - If the file is already in the database, no additional emulation is necessary
   - If the file is not in the database, it is necessary to run full emulation on the file
3. The file is sent over an SSL connection to the ThreatCloud.
4. The virtual computers in the ThreatCloud run emulation on the file.
5. The emulation results are sent securely to the Security Gateway for the applicable action.
Sample ThreatCloud Deployment

<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>Perimeter Security Gateway</td>
</tr>
<tr>
<td>3</td>
<td>Computers and servers in the internal network</td>
</tr>
<tr>
<td>4</td>
<td>Check Point ThreatCloud servers</td>
</tr>
</tbody>
</table>

Using Cloud Emulation

Files are sent to the Check Point ThreatCloud over a secure SSL connection for emulation. The emulation in the ThreatCloud is identical to emulation in the internal network, but it uses only a small amount of CPU, RAM, and disk space of the Security Gateway. The ThreatCloud is always up-to-date with all available operating system environments.

Note - For ThreatCloud emulation, it is necessary that the Security Gateway can connect to the Internet. We recommend that you make sure that the DNS and proxy settings are configured correctly in Global Properties.

To enable ThreatCloud emulation:

1. In R80 SmartConsole, go to Gateways & Servers and double-click the perimeter Security Gateway.
   The Gateway Properties window opens.
2. From the Network Security tab, select Threat Emulation.
   The Threat Emulation First Time Configuration Wizard opens and shows the Emulation Location page.
3. Select ThreatCloud Emulation Service.
4. Click Next.
   The Summary page opens.
5. Click Finish to enable Threat Emulation and close the First Time Configuration Wizard.
6. Click OK.
   The Gateway Properties window closes.


Creating a Threat Prevention Policy

The Threat Prevention profile applies to these Software Blades:

- IPS - There is a dedicated layer for the IPS Rule Base for pre-R80 gateways. After you make changes to IPS, install the Access Control policy.

- Anti-Bot, Anti-Virus, Threat Emulation - These Software Blades are configured in the Threat Prevention Rule Base and policy. After you make changes to one of them, install the Threat Prevention policy.

Note - If you make changes to IPS and one of the other Threat Prevention Software Blades, you must install both the Access Control and Threat Prevention policy.

Overview of Creating a Threat Prevention Policy

After you enable the IPS and Threat Prevention Software Blades on the Security Gateways, configure the Threat Prevention policy.

This is the high-level workflow create and deploy a Threat Prevention policy:

1. Update the IPS database and Malware database with the latest protections.
2. Configure an IPS and Threat Prevention Rule Base with the Threat Prevention profile as the Action of the rule.
3. Install the Access Control and Threat Prevention policy.

Optimized Protection Profile Settings

Check Point defined the Optimized profile to give excellent security with good performance for the gateway.

These are the goals of the Optimized profile, and the settings that achieve those goals:

<table>
<thead>
<tr>
<th>Goal</th>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply settings to the IPS and Threat Prevention Software Blades</td>
<td>Blades Activation</td>
<td>Activate the profile for IPS, Anti-Bot, Anti-Virus, and Threat Emulation.</td>
</tr>
<tr>
<td>Do not have a critical effect on performance</td>
<td>Performance impact</td>
<td>Activate protections that have a Medium or lower effect on performance.</td>
</tr>
</tbody>
</table>
Newly downloaded IPS protections are set to **Detect**. They are activated according to the **IPS Newly Updated Protections**.

**To get quickly up and running with a Threat Prevention policy:**

To get quickly up and running with IPS without making changes to the IPS profile, install this Threat Prevention Rule Base with the **Optimized** profile:

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-the-box Threat Prevention</td>
<td>Any</td>
<td>Optimized</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>policy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IPS and Threat Prevention Policy Use Cases**

This section shows some sample IPS and Threat Prevention policies for different scenarios.

**Getting up and Running with IPS and Threat Prevention**

*Scenario: I want to quickly protect my organization against intrusions*

**IPS Policy**

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-the-box IPS policy</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Optimized profile with these settings:</td>
<td>One or more Security Gateways with IPS enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Activated for Threat Prevention Software Blades: All</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• <strong>Performance impact</strong>: Medium or lower</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• <strong>Severity</strong>: Medium or above</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• <strong>Confidence</strong> (Low\Medium\High): Detect\Prevent\Prevent</td>
<td></td>
</tr>
</tbody>
</table>

*Note* - Install the Access Control and Threat Prevention policies.
## Threat Prevention Policy

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-the-box Threat Prevention policy</td>
<td>Any</td>
<td><strong>Optimized</strong> profile with these settings:</td>
<td>Log Packet Capture</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Activated for Threat Prevention Software Blades: All</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Performance impact</strong>: Medium or lower</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Severity</strong>: Medium or above</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- <strong>Confidence</strong> (Low\Medium\High):</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Detect\Prevent\Prevent</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This scenario used the Optimized Threat Prevention profile ("Optimized Protection Profile Settings" on page 84).

Note - The Protection/Site column is used only for protection exceptions ("Disabling a Protection on a Specified Server" on page 91).

### Monitoring bot activity without blocking traffic

*Scenario: I want to monitor bot activity in my organization without blocking traffic at all. How can I do this?*

Add this rule above the Out-of-the-box Threat Prevention policy to monitor bot activity ("Monitoring Bot Activity" on page 90):

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor bot activity</td>
<td>Any</td>
<td>A profile, with these changes relative to the Recommended_Profile:</td>
<td>Log Packet Capture</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Confidence</strong> (Low\Medium\High):</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prevent\Prevent\Prevent</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Blocking bots

*Scenario: I want to block bots in my organization. How can I do this?*

You can block bots ("Blocking Bots" on page 89) using the out-of-the-box Threat Prevention policy rule, with the Optimized profile:

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-the-box Threat Prevention policy</td>
<td>Any</td>
<td>Optimized profile</td>
<td>Log Packet Capture</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>
Blocking viruses and malware

Scenario: I want to block viruses and malware in my organization. How can I do this?

You can block viruses ("Blocking Viruses" on page 92) using the out-of-the-box Threat Prevention policy rule, with the Optimized profile:

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-the-box Threat Prevention policy</td>
<td>Any</td>
<td>Optimized profile</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Packet Capture</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Capture</td>
<td></td>
</tr>
</tbody>
</table>

Disabling some protections for one server

Scenario: The protection Backdoor.Win32.Agent.AH detects malware on a server (Server_1). How can I disable this protection for this server only?

Add an exception to the specified Anti-Bot rule. This policy monitors bots activity in the organization without blocking traffic, but disables the Backdoor.Win32.Agent.AH protection on Server_1 ("Disabling a Protection on a Specified Server" on page 91).

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Protection</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Bot</td>
<td>Any</td>
<td>- N/A</td>
<td>A profile based on the Optimized profile, with these changes: <strong>Confidence</strong> (Low\Medium\High): Prevent\Prevent\Prevent</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Packet Capture</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Capture</td>
<td></td>
</tr>
<tr>
<td>Exclude Server_1</td>
<td>Server_1</td>
<td>Backdoor.Win32.Agent.AH</td>
<td>Detect</td>
<td>Log</td>
<td>Server_1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Threat Prevention Profiles

A Threat Prevention profile determines which protections are activated, and which Software Blades are enabled for the specified rule or policy. The protections that the profile activates depend on the:

- Performance impact of the protection.
- Severity of the threat.
- Confidence that a protection can correctly identify an attack.
- Settings that are specific to the Software Blade.

A Threat Prevention profile applies to one or more of these Software Blades: IPS, Anti-Bot, Anti-Virus, and Threat Emulation.
Editing Profiles
You can change the settings of the IPS and Threat Prevention profile according to your requirements.

To edit a profile:
2. From the Threat Tools section, click Profiles.
   The Profiles page opens.
3. Right-click the profile and select Edit.

Creating Rules
The Threat Prevention policy determines how the system inspects connections for bots and viruses. The primary component of the policy is the Rule Base. The rules use the Malware database and network objects.

If you enable Identity Awareness on your gateways, you can also use Access Role objects as the scope in a rule. This lets you easily make rules for individuals or different groups of users.

There are no implied rules in the Rule Base. All traffic is allowed unless it is explicitly blocked.

Predefined Rule
When you enable the IPS or one of the Threat Prevention Software Blades, a predefined rule is added to the Rule Base. The rule defines that all traffic for all network objects, regardless of who opened the connection, (the protected scope value equals any) is inspected for all protections according to the recommended profile. By default, logs are generated and the rule is installed on all Security Gateways that use a Threat Prevention Software Blade.

Note - You cannot edit the settings of the predefined rule for the IPS Security Gateway.

The result of this rule (according to the Optimized profile) is that:
- All protections that can identify an attack with a high or medium confidence level and have a medium or lower performance impact are set to Prevent mode.
- All protections that can identify an attack with a low confidence level and have a medium or lower performance impact are set to Detect mode.

Use the Logs & Monitor page to show logs related to IPS and Threat Prevention traffic. Use the data there to better understand the use of these Software Blades in your environment and create an effective Rule Base. You can also directly update the Rule Base from this page.

You can add more rules that prevent or detect specified protections or have different tracking settings.
Creating Rules

Here are examples of how to create different types of Anti-Bot rules.

Creating an Anti-Bot Policy

Create and manage the policy for the Anti-Bot Software Blade as part of the Threat Prevention Policy ("Creating Rules" on page 88).

- The Threat Prevention page shows the rules and exceptions for the Anti-Bot policy. The rules specify the Threat profiles set for network objects or locations defined as a protected scope. Click the Add Rule button to get started.
- To learn about bots and protections, look through the Threat Wiki.

Blocking Bots

Scenario: I want to block bots in my organization. How can I do this?

In this example you will install this default Threat Policy rule that uses the recommended policy, or create a new rule.

<table>
<thead>
<tr>
<th>Protected Scope</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Optimized</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Packet Capture</td>
<td></td>
</tr>
</tbody>
</table>

To block bots in your organization:

1. In R80 SmartConsole, click Gateways & Servers.
2. Enable the Anti-Bot Software Blade on the Gateways that protect your organization. For each Gateway:
   a) Double-click the Gateway object.
   b) In the Gateway Properties page, select the Anti-Bot Software Blade.
      The First Time Activation window opens.
   c) Select According to the Anti-Bot and Anti-Virus policy
   d) Click OK.
   You can block bots using the out-of-the-box Threat Prevention policy rule, with the default Optimized Profile and the previous rule.
   Alternatively, add a new Threat Prevention rule:
   a) Click Add Rule.
      A new rule is added to the Threat Prevention policy. The Software Blade applies the first rule that matches the traffic.
b) Make a rule that includes these components:
   - **Name** - Give the rule a name such as **Block Bot Activity**.
   - **Protected Scope** - The list of network objects you want to protect. By default, the Any network object is used.
   - **Action** - The Profile that contains the protection settings you want. The default profile is **Optimized**.
   - **Track** - The type of log you want to get when detecting malware on this scope.
   - **Install On** - Keep it as **Policy Targets** or choose Gateways to install the rule on.

4. Install the Threat Prevention policy (see "Installing the Threat Prevention Policy" on page 93).

### Monitoring Bot Activity

**Scenario:** I want to monitor bot activity in my organization without blocking traffic at all. How can I do this?

In this example, you will create this Threat Prevention rule, and install the Threat Prevention policy:

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor bot activity</td>
<td>Any</td>
<td>A profile that has these changes relative to the Optimized profile: Confident (High, Medium, Low): Detect, Detect, Detect</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

To monitor all bot activity:

1. In R80 SmartConsole, select **Security Policies > Threat Prevention**.
2. Create a new profile:
   a) From the **Threat Tools** section, click **Profiles**.
      The **Profiles** page opens.
   b) Right-click a profile and select **Clone**.
   c) Give the profile a name such as **Monitoring Profile**.
   d) Edit the profile, and under **Activation Mode**, configure all confidence level settings to **Detect**.
   e) Select the **Performance Impact** - for example, **Medium or lower**.
      This profile detects protections that are identified as an attack with low, medium or high confidence and have a medium or lower performance impact.
3. Create a new rule:
   a) Click **Threat Prevention > Policy > Threat Prevention**.
   b) Add a rule to the Rule Base.
      The first rule that matches is applied.
c) Make a rule that includes these components:
   - **Name** - Give the rule a name such as **Monitor Bot Activity**.
   - **Protected Scope** - Keep **Any** so the rule applies to all traffic in the organization.
   - **Action** - Right-click in this cell and select **Monitoring_Profile**.
   - **Track** - Keep **Log**.
   - **Install On** - Keep it as **Policy Targets** or choose Gateways to install the rule on.

4. Install the Threat Prevention policy (see "Installing the Threat Prevention Policy" on page 93).

**Disabling a Protection on a Specified Server**

*Scenario: The protection Backdoor.Win32.Agent.AH detects malware on a server (Server_1). How can I disable this protection for this server only?*

In this example, create this Threat Prevention rule, and install the Threat Prevention policy:

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Protection/Site</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Bot Activity</td>
<td>Any</td>
<td>- N/A</td>
<td>Optimized Profile</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
<tr>
<td>Exclude</td>
<td>Server_1</td>
<td>Backdoor.Win32.Agent.AH</td>
<td>Detect</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

**To add an exception to a rule:**

1. In R80 SmartConsole, click **Access Control > Threat Prevention > Policy > Threat Prevention**.
2. Click the rule that contains the scope of Server_1.
3. Click the **Add Exception** toolbar button to add the exception under the rule. The first exception matched is applied.
4. Right-click the rule and select **New Exception**.
5. Configure these settings:
   - **Name** - Give the exception a name such as **Exclude**.
   - **Protected Scope** - Change it to **Server_1** so that it applies to all detections on the server.
   - **Protection/Site** - Click + in the cell. From the drop-down menu, click the category and select one or more of the items to exclude
     
     **Note** - To add EICAR files as exceptions, you must add them as Whitelist Files. Adding EICAR files through Exceptions in Policy rules will still get them blocked.
   - **Action** - Keep it as **Detect**.
   - **Track** - Keep it as **Log**.
   - **Install On** - Keep it as **Policy Targets** or choose specified gateways to install the rule on.
6. Install the Threat Prevention policy.
Creating Anti-Virus Rules

Here are examples of how to create different types of Anti-Virus rules.
You can also use Anti-Virus rules to disable a specified malware protection ("Disabling a Protection on a Specified Server" on page 91).

Creating an Anti-Virus Policy

Create and manage the policy for the Anti-Virus Software Blade as part of the Threat Prevention Policy.

- The Threat Prevention page shows the rules and exceptions for the Anti-Virus policy. The rules specify the Threat profiles set for network objects or locations defined as a protected scope.
  Add a new rule to the Threat Prevention policy.
- You can configure the Anti-Virus settings in the Threat Prevention profile for the specified rule.
- To learn about bots and protections, look through the Threat Wiki.

Blocking Viruses

Scenario: I want to block viruses and malware in my organization. How can I do this?

To block viruses in your organization:

1. In R80 SmartConsole, click Gateways & Servers and double-click the Security Gateway.
2. In the General Properties page, select the Anti-Virus Software Blade.
   The First Time Activation window opens.
3. Select According to the Anti-Bot and Anti-Virus policy and click OK.
4. Close the gateway Properties window and publish the changes.
6. Click Add Rule.
   A new rule is added to the Threat Prevention policy. The Software Blade applies the first rule that matches the traffic.
7. Make a rule that includes these components:
   - Name - Give the rule a name such as Block Virus Activity.
   - Protected Scope - The list of network objects you want to protect. In this example, the Any network object is used.
   - Action - The Profile that contains the protection settings you want. The default profile is Optimized.
   - Track - The type of log you want to get when detecting malware on this scope. In this example, keep Log and also select Packet Capture to capture the packets of malicious activity. In SmartView Tracker, you will then be able to view the actual packets.
   - Install On - Keep it as All or choose specified gateways to install the rule on.
8. Install the Threat Prevention policy.
Installing the Threat Prevention Policy

The Anti-Bot, Anti-Virus and Threat Emulation Software Blades have a dedicated Threat Prevention policy. You can install this policy separately from the policy installation of the Access Control Software Blades. Install only the Threat Prevention policy to minimize the performance impact on the Security Gateways.

Settings for the IPS Software Blade are installed with the Access Control policy.

You can update the IPS, Anti-Bot, Anti-Virus and Threat Emulation Rule Base to give immediate coverage for new malware threats.

To install the Threat Prevention and Access Control policies:

1. From the Global toolbar, click Install Policy.
   The Install Policy window opens showing the installation targets (Security Gateways).
3. Expand the Install Mode options, and click the applicable settings:
   - Install on each selected gateway independently - Install the policy on the selected Security Gateways without reference to the other targets. A failure to install on one Security Gateway does not affect policy installation on other gateways.
     If the gateway is a member of a cluster, install the policy on all the members. The Security Management Server makes sure that it can install the policy on all the members before it installs the policy on one of them. If the policy cannot be installed on one of the members, policy installation fails for all of them.
   - Install on all selected gateways, if it fails do not install on gateways of the same version - Install the policy on all installation targets. If the policy fails to install on one of the Security Gateways, the policy is not installed on other targets of the same version.
4. Click OK.

Updating the IPS and Malware Databases

The IPS protection database and the Malware database automatically download updates at regular intervals. This ensures that you have the latest IPS protections, and the most current data and newly added signatures and URL reputations in your Anti-Bot and Anti-Virus policy.

The Malware database only updates if you have a valid Anti-Bot, Threat Emulation and/or Anti-Virus contract.

By default, updates for Anti-Virus and Anti-Bot run on the Security Gateway every two hours. For IPS and Threat Emulation you must configure an update schedule. You can change the update schedule or choose to manually update the Security Gateway. The updates are stored in a few files on each Security Gateway.
Updating IPS Protections

Check Point constantly develops and improves its protections against the latest threats. You can manually update the database with latest IPS protections.

**Note** - The Security Gateways with IPS enabled only get the updates after you install the Policy. For troubleshooting or for performance tuning, you can revert to an earlier IPS protection package.

To manually update the IPS protections:
1. In R80 SmartConsole, click **Security Policies > Threat Prevention**.
2. In the **Threat Tools** section, click **Updates**.
3. In the **IPS** section, click **Update Now**.
4. Install the Access Control policy.

To revert to an earlier protection package:
1. In the **IPS** section of the Threat Prevention Updates page, click **Switch to version**.
2. In the window that opens, select an **IPS Package Version**, and click **OK**.
3. Install the Access Control policy.

Scheduling Updates

You can change the default automatic schedule for when updates are automatically downloaded and installed. If you have Security Gateways in different time zones, they are not synchronized when one updates and the other did not yet update.

To configure Threat Prevention scheduled updates:
1. In R80 SmartConsole, go to the **Security Policies** page and select **Threat Prevention**.
2. In the **Threat Tools** section of the Threat Prevention Policy, click **Updates**.
3. In the section for the applicable Software Blade, click **Schedule Update**. The **Scheduled Update** window opens.
4. Make sure **Enable <feature> scheduled update** is selected.
5. Click **Configure**.
6. In the window that opens, set the **Update at** time and the frequency:
   - **Daily** - Every day
   - **Days in week** - Select days of the week
   - **Days in month** - Select dates of the month
7. Click **OK**.
8. Click **Close**.
9. Install the policy for the applicable Software Blade:
   - IPS updates, install the Access Control policy
   - Anti-Bot, Anti-Virus, and Threat Emulation updates, install the Threat Prevention policy
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.

Enabling Anti-Spam

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

To enable Anti-Spam:

1. In R80 SmartConsole, go to Manage & Settings >Blades.
2. In the Anti-Spam & Mail section, click Configure in SmartDashboard. SmartDashboard opens and shows the Overview page in the Anti-Spam & Mail tab.
4. Select one or more Security Gateways.
5. 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.
Securing Data

In This Section:

Overview ........................................................................................................................................... 96
Enabling DLP ........................................................................................................................................ 99
DLP Rule Base ..................................................................................................................................... 101
Analyzing and Tracking DLP ................................................................................................................ 104

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.

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 58).

- **MultiSpect™** - Unmatched accuracy 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 Log Server</td>
</tr>
<tr>
<td>9</td>
<td>R80 SmartConsole 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 R80 DLP Administration Guide http://supportcontent.checkpoint.com/documentation_download?ID=46527.

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. In R80 SmartConsole, go to Gateways & Servers and double-click the gateway object.
   The General Properties window of the gateway opens.
2. From the navigation tree, select the General Properties view.
   The Data Loss Prevention Wizard opens.
4. Click Next.
   The Email Domain and Active Directory page opens.
5. Enter the email domain for your company to let DLP distinguish between internal and external email addresses.
6. 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.
7. Click Next.
   The My Organization Name page opens.
8. Enter different names and phrases that are used to identify your organization.
   DLP uses these names to accurately detect incidents of data loss.
9. Click Next.
   The DLP Portal and Mail Server page opens.
10. **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.

11. **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**.

12. Click **Next**.
    
    The **Protocols** page opens.

13. Select one or more of these protocols to which the DLP policy applies.
    
    - Email
    - Web
    - File Transfer

14. Click **Next**.
    
    The **Data Loss Prevention Blade Setup is Completed** window opens.

15. 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 R80 SmartConsole, go to **Manage & Settings > Blades**.
2. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.
   
   SmartDashboard opens and shows the **My Organization** page in the **Data Loss Prevention** tab.
3. From the navigation tree, select **Data Types**.
4. Double-click a data type.
   
   The data type properties window opens.
5. From the navigation tree, select **Data Owners**.
6. Click **Add**.
   
   The **Add Data Owners** window opens.
7. 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).
8. Add as many data owners as needed.
9. 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 R80 SmartConsole, go to Manage & Settings > Blades.
2. In the Data Loss Prevention section, click Configure in SmartDashboard.
   SmartDashboard opens and shows the My Organization page in the Data Loss Prevention tab.
3. From the navigation tree, select Policy.
4. Right-click the Track cell of the rule and select Email.
   The Email window opens.
5. Select When data is matched.
   Data Owners are added to the Email Notification list.
6. Optional: Click Add and add more users to send notification emails to.
7. 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
8. 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 SmartConsole 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 R80 SmartConsole and on the Exchange server. For more about configuring an Exchange Security Agent, see sk103166 http://supportcontent.checkpoint.com/solutions?id=sk103166.

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 SmartConsole 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>Who or what starts the connection: Users and Administrators, network, or email domains. If Identity Awareness is enabled, you can use Access Roles.</td>
</tr>
<tr>
<td>Destination</td>
<td>Who or what completes the connection: Users and Administrators, network, or email domains. If Identity Awareness is enabled, you can 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

When a data transmission matches criteria of an exception to a DLP rule, 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 R80 SmartConsole, go to **Manage & Settings > Blades**.
2. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**. 
   SmartDashboard opens and shows the **My Organization** page in the **Data Loss Prevention** tab.
3. From the navigation tree, select **Policy**.
   The **Policy** window opens and shows the DLP Rule Base.
4. Right-click the **Exceptions** cell for a rule and select **Edit**.
   The **Exceptions for Rule** window opens.
5. Click **New Exception**.
6. Configure these settings for the exception: **Data Type, Source, Destination, Protocol.**
7. Click **OK.**
8. 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 the <strong>Logs &amp; Monitor &gt; Logs</strong> view and is available for your review and analysis in the Logs &amp; Monitor Access Control views 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.</td>
</tr>
<tr>
<td></td>
<td><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. By default, all rules are created without a watermark action. Watermarks can be created and edited without having to apply them. 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 Restricted</td>
<td>Log</td>
<td>High</td>
<td>Business</td>
</tr>
<tr>
<td>No Flag</td>
<td>PCI - Credit Card Numbers</td>
<td>PCI - Credit Card Numbers</td>
<td>None</td>
<td>Prevent</td>
<td>Log</td>
<td>Critical</td>
<td>Compliance</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>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</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 R80 SmartConsole clients can help with your DLP analysis:

- SmartView Tracker
- SmartEvent

You can use the Follow Up flag in SmartConsole 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 R80 SmartConsole clients do not show DLP incidents, if these EML files are associated with another application.
Analyzing DLP Incidents in the Logs

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 analyze DLP logs:

1. In R80 SmartConsole, go to Logs & Monitor.
2. In Logs tab, click Favorites (star icon), and select DLP > Incidents.
3. Select a time frame in the search field, to refine the list of incidents:
   - Last Hour
   - Today
   - Last 24 Hours
   - Yesterday
   - This Week
   - Last 7 Days
   - This Month
   - Last 30 Days
   - All Time
   - Custom - specify the Start and End date and time in the window that opens, and click OK

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>Ask User</td>
<td>DLP incident captured and put in Quarantine, user asked to decide what to do.</td>
</tr>
<tr>
<td>Do not Send</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>Send</td>
<td>User decided to continue transmission after DLP capture. 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>Quarantine Expired</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>Prevent</td>
<td>DLP transmission was blocked.</td>
</tr>
<tr>
<td>DLP Action</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow</td>
<td>DLP transmission was allowed; usually by exception to rule.</td>
</tr>
<tr>
<td>Inform User</td>
<td>DLP transmission was detected and allowed, and user notified.</td>
</tr>
<tr>
<td>Deleted Due To Quota</td>
<td>DLP incidents are deleted from gateway for disk space.</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 responses (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>UserCheck</td>
<td>Comment entered by the user in the text box shown in the UserCheck notification.</td>
</tr>
<tr>
<td><strong>Restricted Filters</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UserCheck Message to User</td>
<td>The message shown to the user.</td>
</tr>
<tr>
<td>Interaction Name</td>
<td>The interaction name as shown in SmartConsole.</td>
</tr>
<tr>
<td><strong>Fingerprint</strong></td>
<td></td>
</tr>
<tr>
<td>Matched File</td>
<td>The file name and path in the scanned fingerprint repository that matches the</td>
</tr>
<tr>
<td></td>
<td>inspected message.</td>
</tr>
<tr>
<td>Matched File Percentage</td>
<td>How much is this file similar to Matched File. In &quot;exact match&quot; this will</td>
</tr>
<tr>
<td></td>
<td>always be 100%.</td>
</tr>
<tr>
<td>Matched File Text Segments</td>
<td>In a partial match, the number of file parts/segments that are matched between</td>
</tr>
<tr>
<td></td>
<td>the Matched File and the inspected file (parts/segment may overlap).</td>
</tr>
<tr>
<td><strong>DLP Type</strong></td>
<td></td>
</tr>
<tr>
<td>DLP Rule Name</td>
<td>Name of the DLP rule on which the incident was matched.</td>
</tr>
<tr>
<td>Message to User</td>
<td>Message sent, as configured by administrator, for the rule on which the incident</td>
</tr>
<tr>
<td></td>
<td>was matched.</td>
</tr>
<tr>
<td>DLP Words List</td>
<td>If the Data Type on which the incident was matched included a word list (</td>
</tr>
<tr>
<td></td>
<td>keywords, dictionary, and so on), the list of matched words.</td>
</tr>
<tr>
<td>DLP Relevant Data Types</td>
<td>If matched Data Type is a group Data Type. This field specifies which Data</td>
</tr>
<tr>
<td></td>
<td>Types from that group were matched.</td>
</tr>
<tr>
<td><strong>User Information</strong></td>
<td></td>
</tr>
<tr>
<td>DLP Recipients</td>
<td>For SMTP traffic, list of recipients of captured email.</td>
</tr>
<tr>
<td>Mail Subject</td>
<td>For SMTP traffic, the subject 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</td>
</tr>
<tr>
<td></td>
<td>traffic.</td>
</tr>
<tr>
<td><strong>More</strong></td>
<td></td>
</tr>
<tr>
<td>UserCheck</td>
<td>A Boolean field that shows if the log is produced by UserCheck or by another</td>
</tr>
<tr>
<td></td>
<td>DLP.</td>
</tr>
<tr>
<td>Data Type Name</td>
<td>Name of the matched Data Type.</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>DLP Categories</td>
<td>Category of Data Type on which the incident was matched.</td>
</tr>
<tr>
<td>Restricted Filters</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DLP Template Score</td>
<td>A measurement, expressed as a percentage, that shows how closely a document matches the template file.</td>
</tr>
<tr>
<td></td>
<td>0% - The document and template are very different.</td>
</tr>
<tr>
<td></td>
<td>100% - The document and template are a close match.</td>
</tr>
</tbody>
</table>

Event Analysis Views Available in R80 SmartConsole

As of R80, the Event Analysis views of the SmartEvent GUI have been incorporated into the R80 SmartConsole Logs & Monitor view. They provide advanced analysis tools with filtering, charts, and statistics of all events that pass through enabled Security Gateways.
Maximizing Network Performance

In This Section:
- Check Point Software Acceleration Solutions .......................................................... 109
- CoreXL .................................................................................................................. 109
- Using SecureXL ................................................................................................. 110
- Multi-Queue .......................................................................................................... 111

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 SmartConsole, instead run the applicable commands from the CLI.

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.

When you enable CoreXL, the number of kernel instances is based on the total number of CPU cores.

<table>
<thead>
<tr>
<th>Number of Cores</th>
<th>Number of Kernel 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>6-20</td>
<td>Number of cores, minus 2</td>
</tr>
<tr>
<td>More than 20</td>
<td>Number of cores, minus 4 -- but no more than 30</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.
   If CoreXL is disabled, enable CoreXL and then set the number of firewall instances.
4. 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 SmartConsole 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, `(9) Disable 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>
Configuring the NAT Policy

In This Section:

Translating IP Addresses ................................................................. 112
NAT Rule Base .................................................................................. 115
Configuring Static and Hide NAT ......................................................... 117
Advanced NAT Settings ....................................................................... 122

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 R80 SmartConsole 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.

R80 SmartConsole 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.
• R80 SmartConsole 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 115) to use Port Translation.
Using Hide NAT

For each R80 SmartConsole 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.

<table>
<thead>
<tr>
<th>Internal computer B (10.10.0.37) sends packet to Internet</th>
<th>Firewall translates this address to <strong>192.0.2.16</strong></th>
<th>Internet receives packet from 192.0.2.16</th>
</tr>
</thead>
</table>

**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.

<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 Hide NAT</td>
</tr>
<tr>
<td>3</td>
<td>Internal computers</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Internal computer A (10.10.0.26) sends packet to Internet</th>
<th>Firewall translates this address to 192.0.2.1 port 11000</th>
<th>Internet receives packet from 192.0.2.1 port 11000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal computer A sends packet to Internet</td>
<td>Firewall translates this address to 192.0.2.1 port 11000</td>
<td>Internet receives packet</td>
</tr>
</tbody>
</table>

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 SmartConsole 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 SmartConsole objects:

- Security Gateways
- Nodes
- Networks
- Address Ranges

SmartConsole 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, SmartConsole 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:

<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></td>
<td></td>
<td>N/A (External connections are not allowed)</td>
</tr>
<tr>
<td>External to internal</td>
<td>Rule translates destination IP address</td>
<td></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.

SmartConsole 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**

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**

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 SmartConsole objects.

Configuring Static NAT

When you enable Static NAT, each object is translated to a different IP address. SmartConsole 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 can 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

R80 SmartConsole can automatically create and configure the NAT rules for a network. Enable automatic NAT for every object, for which you are translating the IP address. Then configure the Access Control Rule Base to allow traffic to the applicable objects.

To enable automatic NAT:

1. In R80 SmartConsole, go to Gateways & Servers and double-click the gateway object.
   
   The General Properties window of the gateway opens.

2. From the navigation tree, select NAT > Advanced.

3. Select Add automatic address translation rules to hide this Gateway behind another Gateway.

4. Select the Translation method: Hide or Static.

5. Configure the NAT IP address for the object.
   - Hide behind Gateway - Use the IP address of the Security Gateway
   - Hide behind IP address - Enter the IP address.

6. Click Install on Gateway and select All or the Security Gateway that translates the IP address.

7. Click OK.

After you enable and configure NAT on all applicable gateways, 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 on 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:**

1. In R80 SmartConsole, go to **Gateways & Servers** and double-click the gateway object. The **General Properties** window of the gateway opens.
2. From the navigation tree, select **NAT**.
3. Select **Hide internal networks behind the Gateway's external IP**.
4. Click **OK**.
5. Install the policy.

**Enabling Manual NAT**

For some deployments, it is necessary to manually define the NAT rules. Create SmartConsole 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 122).
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 R80 SmartConsole objects (“Sample Deployment (Manual Rules for Port Translation)” on page 121).

To enable manual Static NAT, follow this workflow:

1. Create a clone from the gateway object.
2. Add a NAT rule that maps the original object to the NATed one.
3. Add Access Control rules that allow traffic to the new NATed objects.

To create a clone gateway object:

1. In R80 SmartConsole, go to Gateways & Servers, right-click the object and select Clone.
2. Enter the Name. We recommend that you name the object <name>_valid_address.
3. Enter the NATed IP address.
4. Click OK.

To add a NAT rule to the Rule Base:

1. In R80 SmartConsole, go to Gateways & Servers >NAT.
2. Add a manual rule above the automatic NAT rules.
3. Configure the manual rule to translate the IP address. For example:
   - Original Source - WebServer
   - Translated Source - WebServer_valid_address

To add Access Control rules:

1. In R80 SmartConsole, go to Security Policies >Access Control >Policy.
2. Add rules that allow traffic to the applicable NATed objects.
3. 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.
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:db8:0: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:db8:0: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.

<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:db8:0:c::1)</td>
</tr>
<tr>
<td>3</td>
<td>DMZ network (Alaska_DMZ 2001:db8:a::/128)</td>
</tr>
<tr>
<td>4</td>
<td>Web server (Alaska_DMZ_Web 2001:db8:a::35:5 translated to 2001:db8:0:c::1)</td>
</tr>
<tr>
<td>5</td>
<td>Mail server (Alaska_DMZ_Mail 2001:db8:a::35:6 translated to 2001:db8:0: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>Source Destination</th>
<th>Original Packet</th>
<th>Service</th>
<th>Translated Packet</th>
<th>Install On</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alaska_DMZ</td>
<td>Alaska_DMZ</td>
<td>Any</td>
<td>Original</td>
<td>Original</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alaska_DMZ</td>
<td>SMTP</td>
<td>Original</td>
<td>Original</td>
<td>All</td>
</tr>
<tr>
<td>2</td>
<td>Alaska_DMZ</td>
<td>Alaska_DMZ</td>
<td>Any</td>
<td>Original</td>
<td>Original</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alaska_DMZ_W</td>
<td>HTTP</td>
<td>Original</td>
<td>Original</td>
<td>All</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Alaska_GW</td>
<td>HTTP</td>
<td>Original</td>
<td>Original</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alaska_DMZ_W</td>
<td>SMTP</td>
<td>Original</td>
<td>Original</td>
<td>All</td>
</tr>
<tr>
<td>4</td>
<td>Any</td>
<td>Alaska_GW</td>
<td>HTTP</td>
<td>Original</td>
<td>Original</td>
<td>All</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 overlapping internal network.

**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.

**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.

Communication Between Internal Networks

<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.

Communication Between an Internal Network and 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 Domain 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 Domain 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 client / SecureClient to MEP (Multiple Entry Point) gateways
- Gateway to MEP gateways

When a connection is opened from a SecuRemote client / 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 client / 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. 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.

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, do the following:
   a) In the network objects tree, right-click **Network Objects** branch and select **New > Address Range** The **Address Range Properties** window opens.
   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 time-out 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 SmartConsole:

- 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.
Monitoring and Logging

In This Section:

Log Analysis .......................................................................................................................... 133
Event Analysis with SmartEvent ............................................................................................ 135
Creating Reports ..................................................................................................................... 135

Log Analysis

R80 SmartConsole lets you transform log data into security intelligence. Search results are fast and immediately show the log records you need. The Security Gateways send logs to the Log Servers on the Security Management Server or on a dedicated server. Logs show on the R80 SmartConsole Logs & Monitor Logs tab. You can:

- Quickly search through logs with simple Google-like searches.
- Select from many predefined search queries to find the applicable logs.
- Create your own queries using a powerful query language.
- Monitor logs from administrator activity and connections in real-time.

Configuring Logging

To configure logging from a Security Gateway to a Security Management Server or a Log Server:

1. Define one or more Log Servers (if necessary).
2. Enable logging on the Management Server and the Log Servers.
3. Configure the Security Gateways to send logs to the Log Servers.
4. Install the Policy.

To enable logging on a server:

1. In R80 SmartConsole, go to Gateways & Servers and double-click the server object. The properties window opens.
3. In the Management tab, select Logging & Status.
4. From the navigation tree, click Logs. This shows the Security Gateways that forward logs to this machine.
5. Make sure that Enable Log Indexing is selected. It is enabled by default optimizes the log search time.
6. Click OK.
To configure a Security Gateway to send logs to log servers:

1. In R80 SmartConsole, go to **Gateways & Servers** and double-click the gateway object.
   The gateway properties window opens.
2. From the navigation tree, click **Logs**.
3. In the **Send gateway logs and alerts to server** section, click the plus sign and select a server.
   Make sure that in the **Type** column, **Send Logs and Alerts** is selected.
4. **Optional** - In the **In case one of the above log servers is unreachable, send logs to**, add backup servers.

To complete the configuration:

1. Click **Publish**.
2. Click **Install Policy**.

### Enabling Log Indexing

Log indexing on the Security Management Server or Log Server reduces the time it takes to run a query on the logs. Log indexing is enabled by default. If you disable log indexing to save disk storage space, queries will take longer.

To manually enable Log Indexing:

1. Open R80 SmartConsole.
2. From the **Gateways & Servers** view, double-click the Security Management Server or Domain Log Server object.
   The **General Properties** window opens.
3. In the **Management** tab, select **Logging & Status**.
4. From the navigation tree, click **Logs**.
5. Select **Enable Log Indexing**.
6. Click **OK**.
7. Click **Publish**.
8. From **Menu**, select **Install Database**.

### Sample Log Analysis

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

To show a log of a dropped connection:

1. Log into R80 SmartConsole.
2. Connect to the IP address of the Security Management Server, not to a Log Server.
3. In the Access Control view, select a rule with the **Drop** action.
4. In the bottom pane, click **Logs**.
   This shows the logs for connections that were dropped by the Rule Base.
5. Double-click a log.
   The **Log Details** window opens.
Event Analysis with SmartEvent

The SmartEvent Software Blade is a unified security event management and analysis solution that delivers real-time, graphical threat management information. R80 SmartConsole, SmartView Web Application, and the SmartEvent GUI client consolidate billions of logs and show them as prioritized security events so you can immediately respond to security incidents, and do the necessary actions to prevent more attacks. You can customize the views to monitor the events that are most important to you. You can move from a high level view to detailed forensic analysis in a few clicks. With the free-text search and suggestions, you can quickly run data analysis and identify critical security events.

Creating Reports

To create a SmartEvent report:
1. In SmartEvent, click the Reports tab.
2. From the navigation tree, select a report.
   A sample report is shown in the window.
3. Click Generate.
   The report is generated and shown in a new window.
4. To save the report as a PDF file, from the navigation tree, select Report History.
5. Click .
Index

A

About this Guide • 12
Account Units • 50
Action • 60
Activating Protections for a Profile • 76
Activating Single Sign On • 31
AD Query • 45
Adding a Server Certificate • 67
Adding an Access Role to a Rule • 55
Adding an IPS Exception • 76
Adding Data Owners • 99
Adding Network Exceptions • 76
Adding Users to the Rule Base • 54
Adding Users to the Security Policy • 45
Additional Activation Fields • 74
Advanced NAT Settings • 122
Allowing Mobile Connections • 31
Allowing VPN Connections • 42
Analyzing and Tracking DLP • 103
Analyzing DLP Incidents in the Logs • 103
Analyzing the Rule Base (Hit Count) • 22
Anti-Bot • 9, 77
Anti-Bot and Anti-Virus Rule Base • 79
Anti-Spam • 93
Anti-Virus • 9, 78
APP Wiki • 9
Authentication Tab • 53
Automatic and Manual NAT Rules • 114
Automatic and Proxy ARP • 122
Automatic Hide NAT to External Networks • 117

B

Basic Rules • 20
Block • 9
Blocking Bots • 88
Blocking Viruses • 90
Bot • 9
Browser-Based Authentication • 45
Browsing IPS Protections • 74

C

Changing the Assigned Profile • 74
Check Point Firewall Security Solution • 14
Check Point Mobile Access Solutions • 27
Check Point Software Acceleration Solutions • 107
Choosing the Level of Protection • 73
Citrix Services • 32
Client-Based vs. Clientless • 28
Communication Between an Internal Network and the Internet • 124
Communication Between Internal Networks • 124
Communication Examples • 124
Compliance Check • 34
Compliance Policy Rules • 35
Components of the Check Point Firewall Solution • 14
Configuring an LDAP Server • 52
Configuring Anti-Spoofing • 21
Configuring Citrix Services for Mobile Access • 33
Configuring Compliance Settings for a Security Gateway • 36
Configuring CoreXL • 107
Configuring HTTPS Inspection Rules • 68
Configuring Inbound HTTPS Inspection • 66
Configuring Inspection Settings • 25
Configuring IP Pool NAT • 130
Configuring IPS Profile Settings • 74
Configuring Logging • 132
Configuring Remote Access to Network Resources • 28
Configuring SecureXL • 109
Configuring Security Gateways to inspect outbound and inbound HTTPS • 63
Configuring Static and Hide NAT • 116
Configuring the Geo Policy • 69
Configuring the Hit Count Display • 23
Configuring the Implied Rules • 20
Configuring the NAT Policy • 111
Configuring the Security Gateway Object • 127
Configuring the Security Management Server Object • 127
Connecting to a Citrix Server • 32
Connecting Translated Objects on Different Interfaces • 123
CoreXL • 9, 107
Creating a Compliance Policy • 35
Creating a Threat Prevention Policy • 71, 83
Creating an Anti-Bot Policy • 87
Creating an Anti-Virus Policy • 90
Creating an Outbound CA Certificate • 63
Creating Anti-Virus Rules • 90
Creating Reports • 134
Creating Rules • 87
Creating VPN Policies • 37
CSCF • 9
Customizing IPS Protections for Your Network • 73

D

Data Loss Prevention Features • 95
DBedit • 9
Default IPS Protection Profiles • 73
Defining Access to Applications • 31
Defining an Internet Access Policy • 56
Deploying Certificates by Using Group Policy • 65
Deploying User Directory • 50
Deployment Configurations • 122
Diameter • 9
Disabling Application • 9
Disabling a Protection on a Specified Server • 89
Disabling NAT in a VPN Tunnel • 123
DLP • 9
DLP Actions • 104
DLP General Columns • 104
DLP Restricted Columns • 105
DLP Rule Actions • 102
DLP Rule Base • 100
DLP Rule Exceptions • 101
DPD • 9
Drop • 9
Dual Stack (IPv4 and IPv6) Network Configuration • 15

E
Editing Profiles • 86
Enabling Anti-Spam • 93
Enabling Automatic NAT • 116
Enabling DLP • 98
Enabling HTTPS Inspection • 63
Enabling Identity Awareness • 46
Enabling Log Indexing • 133
Enabling Manual NAT • 118
Enabling or Disabling Hit Count • 23
Enabling the Anti-Bot Software Blade • 78
Enabling the IPS Software Blade • 73
Enabling URL Filtering and Application Control • 57
Enabling User Directory • 53
Ensuring a Secure Network Access • 20
Event • 9
Event Analysis Views Available in R80 SmartConsole • 106
Event Analysis with SmartEvent • 133
Examining Anti-Bot and Anti-Virus Protections • 78
Excluding Specific Internal Addresses • 22
Exporting a Certificate from the Management Server • 65
Exporting and Deploying the Generated CA • 65

F
Filtering IPS Protections • 75
Firewall • 9

G
General Tab • 51
GGSN • 9
GPRS • 10
Granular Routing Control • 40
GSM • 10
GTP • 10
GuiDBedit • 10

H
Hide NAT • 113
Hide NAT for Address Range • 116
How to Use this Guide • 16
HSPA • 10
HTTPS Inspection • 61
HTTPS Inspection Policy • 67

I
Identifying Bot Infected Computers • 77
Identity Awareness and Remote Access • 47
Identity Sources • 45
IKE • 10
Important Information • 3
Importing an Outbound CA Certificate • 64
Inbound Connections • 62
Inspecting HTTPS Packets • 62
Inspection Settings • 24
Installing the Threat Prevention Policy • 91
Interface A • 124
Interface B • 124
Interface C • 124
Internal Communication with Overlapping Addresses • 123
Introducing the Access Control Policy • 18
IP Pool NAT • 127
IP Pool NAT for Clusters • 131
IP Pool Per Interface • 128
IPS • 10, 72
IPS and Threat Prevention Policy Use Cases • 84
IPS Protections Columns • 75
IPv4 embedded IPv6 address • 10

L
Learning about Malware • 72
Log Analysis • 132
LTE • 10

M
Managing LDAP Information • 54
Managing Network Access Control • 18
Managing the Anti-Bot and Anti-Virus Rule Base • 79
Managing the DLP Rule Base • 100
Managing URL Filtering and Application Control • 56
Maximizing Network Performance • 107
Mobile Access Clients • 28
Mobile Access Web Portal • 28
Monitoring and Logging • 132
Monitoring Bot Activity • 88
Multi-Queue • 109

N
NAT and Anti-Spoofing • 122
NAT Priorities • 128
Overview of Creating a Threat Prevention Policy • 83
Overview of Firewall Features • 14
Overview of IPS • 72

P
PDP • 10
Performance Pack • 10
PLMN • 10
Predefined Rule • 87
Preventing IP Spoofing • 20
Protecting Networks from Bots • 77
Protecting Networks from Viruses • 78
PSWT • 10

R
RB80 SmartConsole Toolbars • 12
Redirecting to a Captive Portal • 48
Remote Access Community • 10
Remote Access to the Network • 27
Remote Access VPN • 10, 40
Removing Activation Overrides • 76
Reusing IP Pool Addresses For Different Destinations • 129
Routing Considerations • 125
Routing VPN Traffic • 40
Rule • 10
Rule Base • 11

S
SA • 11
Sample Anti-Bot and Anti-Virus Rule Base • 80
Sample Automatic Rules • 115
Sample Combination VPN Community • 39
Sample Configuration • 93
Sample Deployment (Manual Rules for Port Translation) • 120
Sample Deployment (Static and Hide NAT) • 119
Sample Deployment with Citrix Server • 33
Sample DLP Deployment • 96
Sample Identity Awareness Rules • 48
Sample Log Analysis • 133
Sample Mail Relay Deployment • 97
Sample Mobile Access Deployment • 29
Sample Mobile Access Workflow • 28
Sample NAT Deployments • 112
Sample Remote Access VPN Workflow • 43
Sample Rule Base • 102
Sample Star Deployment • 41
Sample URL Filtering and Application Control Rules • 60
Sample VPN Access Control Rules • 42
Scheduling Updates • 92
SCTP • 11
Securing Data • 95
Security Gateway • 11
Security Management Behind NAT • 126
Security Management Server • 11
Security Policy • 11
Server Certificates • 66
Services & Applications • 59
SGSN • 11
SIP • 11
Site to Site VPN • 37
SmartEvent Server • 11
Software Blade • 11
Special URL Filtering and Application Control Fields • 58
SSL Network Extender • 28
Static NAT • 112
Static NAT for a Network Object • 115

T
The Check Point Solution for Internet Browsing • 56
The Columns of the Access Control Rule Base • 58
The Need for Threat Emulation • 81
Threat Emulation • 81
Threat Prevention Components • 71
Threat Prevention Profiles • 86
ThreatCloud Emulation • 81
ThreatCloud Repository • 11
ThreatSpect Engine • 11
ThreatSpect Engine and ThreatCloud Repository • 72
To enable automatic Hide NAT: • 117
To get quickly up and running with a Threat Prevention policy: • 84
Translating IP Addresses • 111
Types of Rules in the Rule Base • 18

U
Updating IPS Protections • 92
Updating the IPS and Malware Databases • 92
User Directory Features • 49
UserCheck • 11, 57
UserCheck Actions • 60
Using a Mail Relay and Mail Server • 97
Using Automatic Rules • 114
Using Identity Awareness in the Access Control Policy • 48
Using the Identity Awareness Configuration Wizard • 46
Using the Mobile Access Configuration Wizard • 30
Using User Directory • 49
UTMS • 11

V
VPN Communities • 38
VPN Connectivity Modes • 43

W
Working with Access Roles • 47
Working with LDAP Account Units • 50