Important Information

Latest Software

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

Latest Documentation

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=13089

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

For more about this release, see the home page at the Check Point Support Center (http://supportcontent.checkpoint.com/solutions?id=sk67581).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 November 2012</td>
<td>Updated Gateways protection scope (&quot;Gateway Protection Scope&quot; on page 76).</td>
</tr>
<tr>
<td>9 May 2012</td>
<td>Updated the export CA certificate command syntax (&quot;Exporting a Certificate from the Security Management Server&quot; on page 63)</td>
</tr>
<tr>
<td>16 April 2012</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback

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

Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Check Point IPS R75.40 Administration Guide).
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>The Check Point IPS Solution</td>
<td>7</td>
</tr>
<tr>
<td>Tour of IPS</td>
<td>8</td>
</tr>
<tr>
<td>IPS Terminology</td>
<td>8</td>
</tr>
<tr>
<td>Enforcing Gateways</td>
<td>8</td>
</tr>
<tr>
<td>Protections</td>
<td>8</td>
</tr>
<tr>
<td>Profiles</td>
<td>9</td>
</tr>
<tr>
<td>IPS Overview</td>
<td>9</td>
</tr>
<tr>
<td>In My Organization</td>
<td>10</td>
</tr>
<tr>
<td>Messages and Action Items</td>
<td>10</td>
</tr>
<tr>
<td>Security Status</td>
<td>10</td>
</tr>
<tr>
<td>Security Center</td>
<td>11</td>
</tr>
<tr>
<td>Getting Started with IPS</td>
<td>12</td>
</tr>
<tr>
<td>Choosing the Level of Protection</td>
<td>12</td>
</tr>
<tr>
<td>Basic IPS Protection</td>
<td>12</td>
</tr>
<tr>
<td>Advanced IPS Protection</td>
<td>13</td>
</tr>
<tr>
<td>Changing the Assigned Profile</td>
<td>13</td>
</tr>
<tr>
<td>Recommendations for Initial Deployment</td>
<td>13</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>13</td>
</tr>
<tr>
<td>Protect Internal Hosts Only</td>
<td>14</td>
</tr>
<tr>
<td>Bypass Under Load</td>
<td>14</td>
</tr>
<tr>
<td>Optimizing TCP Logs</td>
<td>14</td>
</tr>
<tr>
<td>Installing the Policy</td>
<td>15</td>
</tr>
<tr>
<td>Managing Gateways</td>
<td>16</td>
</tr>
<tr>
<td>Adding IPS Software Blade Gateways</td>
<td>16</td>
</tr>
<tr>
<td>Adding IPS-1 Sensors</td>
<td>17</td>
</tr>
<tr>
<td>CLI Commands</td>
<td>18</td>
</tr>
<tr>
<td>Managing Profiles and Protections</td>
<td>19</td>
</tr>
<tr>
<td>IPS Profiles</td>
<td>19</td>
</tr>
<tr>
<td>Creating Profiles</td>
<td>19</td>
</tr>
<tr>
<td>Activating Protections</td>
<td>20</td>
</tr>
<tr>
<td>Managing Profiles</td>
<td>24</td>
</tr>
<tr>
<td>Troubleshooting Profiles</td>
<td>26</td>
</tr>
<tr>
<td>Customizing Profiles for IPS-1 Sensors</td>
<td>26</td>
</tr>
<tr>
<td>Protections Browser</td>
<td>27</td>
</tr>
<tr>
<td>Customizing the Protections Browser View</td>
<td>27</td>
</tr>
<tr>
<td>Protection Parameters</td>
<td>30</td>
</tr>
<tr>
<td>Protected Servers</td>
<td>32</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>33</td>
</tr>
<tr>
<td>Web Servers</td>
<td>33</td>
</tr>
<tr>
<td>Mail Servers</td>
<td>34</td>
</tr>
<tr>
<td>Configuring Specific Protections</td>
<td>35</td>
</tr>
<tr>
<td>Configuring Network Security Settings</td>
<td>35</td>
</tr>
<tr>
<td>Streaming Engine Settings</td>
<td>36</td>
</tr>
<tr>
<td>Receiving Block List</td>
<td>36</td>
</tr>
<tr>
<td>Anti Spoofing Configuration Status</td>
<td>36</td>
</tr>
<tr>
<td>Aggressive Aging Configurations</td>
<td>36</td>
</tr>
<tr>
<td>IP Fragments</td>
<td>38</td>
</tr>
<tr>
<td>DShield Storm Center</td>
<td>39</td>
</tr>
<tr>
<td>Configuring Application Intelligence</td>
<td>40</td>
</tr>
<tr>
<td>Mail</td>
<td>40</td>
</tr>
<tr>
<td>FTP</td>
<td>41</td>
</tr>
</tbody>
</table>
Microsoft Networks ................................................................. 41
Peer-to-Peer ............................................................................ 41
Instant Messengers ................................................................. 42
VoIP ....................................................................................... 43
SNMP ...................................................................................... 43
VPN Protocols ........................................................................ 43
Citrix ICA ................................................................................ 43
Remote Control Applications .................................................... 44
MS-RPC .................................................................................... 44
Configuring Web Intelligence .................................................... 44
Configuring Web Intelligence Protections ................................. 44
Customizable Error Page ....................................................... 46
Connectivity/Performance Versus Security ............................... 47
Managing Application Controls ............................................... 48
Configuring Geo Protections .................................................... 48
Controlling Traffic by Country .................................................. 49
The IP Address to Country Database ........................................ 49
Log Aggregation by Country ................................................... 50
Configuring IPS Pattern Granularity ....................................... 50
Activating New Protections ..................................................... 50
Network Exceptions for the New Protections ............................ 50
Handling Multiple Matches of a Pattern ................................. 51
Configuring Implied IPS Exceptions ........................................ 51
Monitoring Traffic .................................................................... 52
Monitoring Events using SmartView Tracker ............................. 52
Viewing IPS Events ............................................................... 52
Viewing IPS Event Details ...................................................... 53
Opening Protection Settings .................................................... 53
Working with Packet Information ............................................. 54
Attaching a Packet Capture to Every Log ................................. 54
Viewing Packet Capture Data in SmartView Tracker ................. 54
Allowing Traffic using Network Exceptions ................................ 55
Viewing Network Exceptions .................................................. 56
Configuring Network Exceptions ............................................. 56
Tracking Protections using Follow Up ....................................... 57
Marking Protections for Follow Up .......................................... 58
Unmarking Protections for Follow Up ....................................... 59
HTTPS Inspection on Non-Standard Ports ................................ 60
HTTPS Inspection ..................................................................... 60
How it Operates ....................................................................... 61
Configuring Outbound HTTPS Inspection ................................. 61
Configuring Inbound HTTPS Inspection .................................... 64
The HTTPS Inspection Policy .................................................. 65
Gateways Pane ........................................................................ 68
Adding Trusted CAs for Outbound HTTPS Inspection ............... 68
HTTPS Validation ..................................................................... 70
HTTP/HTTPS Proxy ............................................................... 72
HTTPS Inspection in SmartView Tracker ................................... 73
HTTPS Inspection in SmartView .............................................. 74
Optimizing IPS ....................................................................... 76
Managing Performance Impact ............................................... 76
Gateway Protection Scope ...................................................... 76
Web Protection Scope ............................................................ 77
Bypass Under Load ................................................................... 77
Cluster Failover Management ................................................ 78
Tuning Protections ................................................................... 79
Profile Management ............................................................... 79
IPS Policy Settings ................................................................. 79
Enhancing System Performance .............................................. 80
Chapter 1

The Check Point IPS Solution

In This Chapter

Tour of IPS 8
IPS Terminology 8
IPS Overview 9

Check Point IPS is an Intrusion Prevention System (IPS). Whereas the Security Gateway firewall lets you block traffic based on source, destination and port information, IPS adds another line of defense by analyzing traffic contents to check if it is a risk to your network. IPS protects both clients and servers, and lets you control the network usage of certain applications. The new, hybrid IPS detection engine provides multiple defense layers which allows it excellent detection and prevention capabilities of known threats, and in many cases future attacks as well. It also allows unparalleled deployment and configuration flexibility and excellent performance.

Check Point IPS is available in two deployment methods:

- **IPS Software Blade** - integrated with the Check Point Security Gateway to provide another layer of security in addition to the Check Point firewall technology.
- **IPS-1 Sensor** - installed without the Check Point Firewall and dedicated to protecting network segments against intrusion.

**Layers of Protection**

The layers of the IPS engine include:

- Detection and prevention of specific known exploits.
- Detection and prevention of vulnerabilities, including both known and unknown exploit tools, for example protection from specific CVEs.
- Detection and prevention of protocol misuse which in many cases indicates malicious activity or potential threat. Examples of commonly manipulated protocols are HTTP, SMTP, POP, and IMAP.
- Detection and prevention of outbound malware communications.
- Detection and prevention of tunneling attempts. These attempts may indicate data leakage or attempts to circumvent other security measures such as web filtering.
- Detection, prevention or restriction of certain applications which, in many cases, are bandwidth consuming or may cause security threats to the network, such as Peer to Peer and Instant Messaging applications.
- Detection and prevention of generic attack types without any pre-defined signatures, such as Malicious Code Protector.

In all, IPS has deep coverage of dozens of protocols with thousands of protections. Check Point constantly updates the library of protections to stay ahead of the threats.

**Capabilities of IPS**

The unique capabilities of the Check Point IPS engine include:

- Clear, simple management interface
- Reduced management overhead by using one management console for all Check Point products
- Unified control of both the IPS-1 Sensors and the integrated IPS Software Blade
- Easy navigation from business-level overview to a packet capture for a single attack
- Up to 15 Gbps throughput with optimized security, and up to 2.5 Gbps throughput with all IPS protections activated
# Security Coverage

- **#1 security coverage for Microsoft and Adobe vulnerabilities**
- Resource throttling so that high IPS activity will not impact other blade functionality
- Complete integration with Check Point configuration and monitoring tools, such as SmartEvent, SmartView Tracker and SmartDashboard, to let you take immediate action based on IPS information

As an example, some malware can be downloaded by a user unknowingly when browsing to a legitimate web site, also known as a drive-by-download. The malware may exploit a browser vulnerability by creating a special HTTP response and sending it to the client. IPS can identify and block this type of attack even though the firewall may be configured to allow the HTTP traffic to pass.

## Tour of IPS

The IPS tree in provides easy access to IPS features, specific protections, and expert configurations. The tree is divided into the following sections:

- **Overview**
  - Dashboard for viewing IPS status, activity and updates ("IPS Overview" on page 9)

- **Enforcing Gateways**
  - List of gateways enforcing IPS protections ("Assigning Profiles to Gateways" on page 24)

- **Profiles**
  - Settings for IPS profiles (see "IPS Profiles" on page 19)

- **Protections**
  - Settings for individual protections ("Protections Browser" on page 27)

- **Geo Protection**
  - Protection enforcement by source or destination country ("Configuring Geo Protections" on page 48)

- **Network Exceptions**
  - Resources that are not subject to IPS inspection ("Allowing Traffic using Network Exceptions" on page 55)

- **Download Updates**
  - Manual or Automatic updates to IPS protections ("Updating Protections" on page 81)

- **Follow Up**
  - Protections marked for follow up action (see "Tracking Protections using Follow Up" on page 57)

## IPS Terminology

The following terms are used throughout this guide:

### Enforcing Gateways

- **IPS Software Blade**: the Software Blade that can be installed on a Security Gateway for enforcing IPS Software Blade protections.

- **IPS-1 Sensor**: a device that has only the IPS-1 sensor software installed for enforcing IPS-1 sensor protections. A sensor does not have any routing capabilities.

### Protections

- **Protection**: a configurable set of rules which IPS uses to analyze network traffic and protect against threats
**Activation Settings**
- **Active**: the protection action that activates a protection to either Detect or Prevent traffic
- **Detect**: the protection action that allows identified traffic to pass through the gateway but logs the traffic or tracks it according to user configured settings
- **Inactive**: the protection action that deactivates a protection
- **Prevent**: the protection action that blocks identified traffic and logs the traffic or tracks it according to user configured settings

**Types of Protections**
- **Application Controls**: the group of protections that prevents the use of specific end-user applications
- **Engine Settings**: the group of protections that contain settings that alter the behavior of other protections
- **Protocol Anomalies**: the group of protections that identifies traffic that does not comply with protocol standards
- **Signatures**: the group of protections that identifies traffic that attempts to exploit a specific vulnerability

**Protection Parameters**
- **Confidence Level**: how confident IPS is that recognized attacks are actually undesirable traffic
- **Performance Impact**: how much a protection affects the gateway's performance
- **Protection Type**: whether a protection applies to server-related traffic or client-related traffic
- **Severity**: the likelihood that an attack can cause damage to your environment; for example, an attack that could allow the attacker to execute code on the host is considered Critical

**Functions for Monitoring**
- **Follow Up**: a method of identifying protections that require further configuration or attention
- **Network Exception**: a rule which can be used to exclude traffic from IPS inspection based on protections, source, destination, service, and gateway.

**Profiles**
- **IPS Mode**: the default action, either Detect or Prevent, that an activated protection takes when it identifies a threat
- **IPS Policy**: a set of rules that determines which protections are activated for a profile
- **Profile**: a set of protection configurations, based on IPS Mode and IPS Policy, that can be applied to enforcing gateways
- **Troubleshooting**: options that can be used to temporarily change the behavior of IPS protections, for example, Detect-Only for Troubleshooting

**IPS Overview**
The IPS Overview page provides quick access to the latest and most important information.
In My Organization

IPS in My Organization summarizes gateway and profile information.

The table of the configured profiles displays the following information:

- **Profile** — the name of the profile
- **IPS Mode** — whether the profile is set to just Detect attacks or to prevent them as well
- **Activation** — the method of activating protections; either **IPS Policy** or **Manual**
- **Gateways** — the number of gateways enforcing the profile

Double-clicking a profile opens the profile’s Properties window.

Messages and Action Items

Messages and Action Items provides quick access to:

- Protection update information
- Protections marked for Follow Up
- IPS contract status
- Links to events and reports

Security Status

Security Status provides an up-to-the-minute display of the number of Detect and Prevent events that IPS handled over a selected time period, delineated by severity. You can rebuild the chart with the latest statistics by clicking on **Refresh**.

**Note** - Security Status graphs compile data from gateways of version R70 and above.
The **Average** shows the number of handled attacks that is average for the selected time period in your company.

For example, if you choose to see the status of attacks in the past 24 hours and the average of critical attacks is 45, this indicates that in your organization the average number of attacks during a 24-hour period is 45.

- If the current number of attacks is much higher than the average, it may indicate a security issue that you should handle immediately. For example, if more than 500 critical attacks were handled by IPS in the past 24 hours, and the average is 45, you can see quickly that your organization has been targeted with critical attacks in a persistent manner and you should handle this urgently.

- If the current number of attacks is much lower than the average, it may indicate an issue with IPS usage that you should troubleshoot. For example, if less than 10 critical attacks were handled by IPS in the past 24 hours, with the average of 45, you can see that there is a possible issue with IPS configuration; perhaps a gateway was installed with a policy that didn't include an IPS profile.

**Security Center**

Security Center is a scrolling list of available protections against new vulnerabilities. The **Open** link next to a Security Center item takes you to the associated Check Point Advisory.

<table>
<thead>
<tr>
<th>Date</th>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thu, 19 Feb 2009</td>
<td>Critical</td>
<td>Update Protection against Oracle Database SYS.0LA_API_MPL_T Package ODCITABLESTART Buf...</td>
</tr>
<tr>
<td>Thu, 19 Feb 2009</td>
<td>High</td>
<td>Update Protection against Recent Malware Threats (19-Feb-09)</td>
</tr>
<tr>
<td>Mon, 16 Feb 2009</td>
<td>Medium</td>
<td>Update Protection against Alar...</td>
</tr>
</tbody>
</table>
Chapter 2

Getting Started with IPS

In This Chapter
- Choosing the Level of Protection 12
- Changing the Assigned Profile 13
- Recommendations for Initial Deployment 13
- Installing the Policy 15

IPS can be configured for many levels of control over network traffic, but it is also designed to provide IPS protection right out of the box for IPS Software Blades and IPS-1 Sensors.

- IPS Software Blades - When you enable the IPS Software Blade on a Security Gateway object, the gateway is automatically added to the list of Enforcing Gateways and it is assigned the Default Protection profile. You also have the option to assign the Recommended Protection profile to the gateway or to create a customized profile and assign it to the gateway.

- IPS-1 Sensors - When you add a new IPS-1 Sensor object, the sensor is automatically added to the list of Enforcing Gateways and it is assigned the IPS-1 Recommended Protection profile.

The next time you install a policy on the gateway, the IPS profile is also installed on the gateway and the gateway immediately begins enforcing IPS protection on network traffic.

In addition to assigning your gateway an IPS profile, you should also review the Recommendations for Initial Deployment (on page 13).

Choosing the Level of Protection

Check Point IPS is a system that can give you instant protection based on pre-defined profiles, or it can be customized and controlled on a very detailed level.

To learn more about profiles, see IPS Profiles (on page 19).

Basic IPS Protection

IPS provides three pre-defined profiles that can be used to immediately enforce IPS protection in your environment:

- Default Protection - provides excellent performance with a sufficient level of protection using only IPS Software Blade protections.

- Recommended Protection - provides the best security with a sufficient level of performance using only IPS Software Blade protections.

- IPS-1_Recommended_Protection - provides a sufficient level of protection using both IPS Software Blade and IPS-1 Sensor protections.

Application Control protections are not activated by default in any of the pre-defined profiles.

Default Protection

The Default Protection profile is defined with these parameters:

- IPS Mode: Prevent
- IPS Policy: All Signature protections with Very Low Performance Impact are activated
- Updates Policy: Protections downloaded using Online Updates are set to Prevent.
Recommended Protection
The Recommended Protection profile is defined with these parameters:

- IPS Mode: Prevent
- IPS Policy: All Signature and Protocol Anomaly protections with Low Severity and Medium or higher Confidence-level are activated, excluding protections with Critical Performance Impact.
- Updates Policy: Protections downloaded using Online Updates are set to Detect.

IPS-1 Recommended Protection
The IPS-1 Recommended Protection profile is defined with these parameters:

- IPS Mode: Prevent
- IPS Policy: All Signature and Protocol Anomaly protections with Low Severity and Medium-low or higher Confidence-level are activated, excluding protections with Critical Performance Impact.
- Updates Policy: Protections downloaded using Online Updates are set to Detect.

Advanced IPS Protection
For organizations particularly focused on network security, IPS allows you to customize profiles that will meet the needs of your organization.

Ideally, you might want to set all IPS protections to Prevent in order to protect against all potential threats. However, to allow your gateway processes to focus on handling the most important traffic and to report on only the most concerning threats, you will need to determine the most effective way to apply the IPS protections.

By making a few policy decisions, you can create an IPS Policy which activates only the protections that you need and prevents only the attacks that most threaten your network.

To apply protections based on an IPS Policy, create a new profile and select Activate protections according to IPS Policy in the IPS Policy page. For more information, see Creating Profiles (on page 19) and Activating Protections (on page 20).

Changing the Assigned Profile
To assign an IPS profile:
1. Select IPS > Enforcing Gateways. This page lists all gateways with the IPS Software Blade enabled.
2. Select a gateway and click Edit.
3. In Assign IPS Profile, select the profile that you want to assign to this gateway. The gateway will begin enforcing the protections according to the assigned profile after you install the policy.

Recommendations for Initial Deployment
In addition to choosing a level of IPS Protection, we recommend that you use certain IPS settings for your initial deployment of IPS.

Once you are satisfied with the protection and performance of IPS, you can change the system's settings to focus on the attacks that concern you the most. (Optimizing IPS on page 76)

Troubleshooting
It is recommended to enable Detect-Only for Troubleshooting on the profile during the initial installation of IPS. This option overrides any protections that are set to Prevent so that they will not block any traffic. During this time you can analyze the alerts that IPS generates to see how IPS will handle network traffic, while avoiding any impact on the flow of traffic. Once you have used this information to customize the IPS
protections to suit your needs, disable Detect-Only for Troubleshooting to allow IPS protections set to Prevent to block identified traffic on the gateways.

**Protect Internal Hosts Only**

IPS is designed to detect attacks threatening the internal network, as well as those which may originate from the internal network. However, most organizations’ primary concern is on the traffic which enters the organizations’ internal networks. In the initial deployment, it is recommended to set the enforcing gateways’ Protection Scope to only protect internal hosts. This will focus the gateway’s inspection efforts to traffic which may directly threaten the internal network.

For information on Protection Scope, see Gateway Protection Scope (on page 76).

**Bypass Under Load**

To help customers easily integrate the use of IPS into their environment, activating the Bypass Under Load feature will disengage IPS activities during times of heavy network usage. IPS will allow traffic to pass smoothly through the gateway without inspection, and IPS will resume inspection once the high traffic levels have been reduced.

Because this feature creates a situation where IPS protections are temporarily disabled, it is recommended only to apply it during the initial deployment of IPS. After optimizing the protections and performance of your gateway, it is recommended to disable Bypass Under Load to ensure that your network is always protected against attack.

For information, see Bypass Under Load (on page 77).

**Optimizing TCP Logs**

**Improving TCP Streaming**

You can configure the `psl_tab_enable` parameter to improve the TCP Streaming performance in Security Gateways that use TAP mode.

*Note* - When you enable mirror port, TCP Streaming performance is automatically improved. It is not necessary to make any changes to the Security Gateway.

To improve TCP Streaming:

1. From the CLI of the Security Gateway, open `FWDIR/modules/fwkernel.conf`
2. Add this line to the file:
   ```
   psl_tap_enable=1
   ```
3. Save the file.
4. Reboot the Security Gateway.

**Reducing TCP Logs in Inline Gateways**

Use the `fwpslglue_log_ctrl` global parameter to reduce the TCP streaming logs on inline gateways. These are the values for this parameter:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Print all the logs</td>
</tr>
<tr>
<td>1</td>
<td>Print one log per connection or window</td>
</tr>
<tr>
<td>2</td>
<td>Do not print any logs</td>
</tr>
</tbody>
</table>

To reduce TCP streaming logs in inline gateways:

1. From the CLI of the Security Gateway, open `FWDIR/modules/fwkernel.conf`
2. Add this line to the file:
fwpslglue_log_ctrl =2
3. Save the file.
4. Reboot the Security Gateway.

Installing the Policy

After preparing the IPS profiles according to your needs, apply the IPS changes to your gateway by installing the policy.

To install the policy:
1. Select File > Save.
2. Select Policy > Install.
3. Click OK.
4. Select the gateways on which the policy is to be installed, and click OK.

Your environment is now protected by Check Point IPS.

Periodically review IPS events in SmartView Tracker to see the traffic that IPS identifies as a result of your IPS configuration. For more information, see Monitoring Traffic (on page 52).
Chapter 3

Managing Gateways

In This Chapter

Adding IPS Software Blade Gateways 16
Adding IPS-1 Sensors 17
CLI Commands 18

IPS protections are enforced by Security Gateways with the IPS Software Blade enabled and by IPS-1 Sensors. The Enforcing Gateways page shows the list of all gateways enforcing IPS protections and the profile that is assigned to each gateway.

IPS protections are divided into two main groups:

- **IPS Software Blade protections** - protections that can be enforced only by a Check Point Security Gateway with the IPS Software Blade enabled
- **IPS-1 Sensor protections** - protections that can be enforced only by an IPS-1 Sensor

**General IPS Settings**

In the Enforcing Gateways page, you can select whether the IPS profiles will manage only IPS Software Blade protections or if they will also manage IPS-1 Sensor protections. If you choose to manage IPS-1 Sensor protections, you can add IPS-1 Sensors to your list of enforcing gateways and assign profiles to the sensors.

If you choose to manage IPS-1 Sensors as well, the IPS-1_Recommended_Protection profile will be available in the list of Profiles. The Recommended_IPS-1_Protection profile contains recommended settings for both IPS Software Blade protections and IPS-1 Sensor protections. It can also be imported at a later time from the command line with the `ips_expor import` command.

⚠️ Important - The Remove button will DELETE the selected gateway object.

- To remove a Security Gateway from Enforcing Gateways, disable the Software Blade on the gateway.
- To remove an IPS-1 Sensor from Enforcing Gateways, delete the IPS-1 Sensor object.

**Adding IPS Software Blade Gateways**

When you enable the IPS Software Blade on a Security Gateway object, the gateway is automatically added to the list of Enforcing Gateways and it is assigned the Default Protection profile.

**To create a new gateway object with IPS enforcement:**

1. In the IPS tab of SmartDashboard, select Enforcing Gateways.
2. Click Add and choose Security Gateway.
3. Enter the properties of the Security Gateway, including selecting IPS.
   - In Classic mode, select IPS in the Network Security tab.
   - In Simple mode, select one of the Check Point products options that includes IPS.

The Firewall Software Blade must be enabled to enable the IPS Software Blade.
Adding IPS-1 Sensors

When you add a new IPS-1 Sensor object, the sensor is automatically added to the list of Enforcing Gateways and it is assigned the **IPS-1 Recommended Protection** profile. By default, the sensor is configured as **IPS-Inline** with fail-open bypass mode.

When adding an IPS-1 Sensor, you can also define these settings which are unique to IPS-1 Sensors:

**Working Mode**

- **IDS - Passive**: The IPS-1 Sensor is not placed in the path of traffic. Packets are processed for attack detection without any impact on the flow of network traffic.
- **IPS - Inline, Detect only**: Inline intrusion detection. Packets are forwarded through to the network before processing for attack detection. In fault conditions, all packets are allowed. Detect only mode is also useful for checking whether an IPS-mode Sensor is responsible for dropped traffic.
- **IPS - Inline, fail-open**: Inline intrusion prevention. Packets are processed for attack detection and are forwarded to the network only in accordance with protection settings. In fault conditions, all packets are allowed.
- **IPS - Inline, fail-closed**: Inline intrusion prevention. Packets are processed for attack detection and are forwarded to the network only in accordance with protection settings. In fault conditions, all packets are dropped.

**Warning** - Changing the Working Mode may stop the flow of network traffic. Make sure that your network topology is correct for the IPS-1 Sensor Working Mode that you choose.

**Topology**

By default, the IPS-1 Sensor inspects all traffic that passes through its interfaces. We recommend that you manually define the protected networks in the IPS-1 Sensor’s Topology page. The Topology options are:

- **All IPs** lets the IPS-1 Sensor protections react to all traffic with the highest level of inspection. Most organizations will choose not to use this setting because it requires a high level of inspection of traffic even of traffic that does not impact the organization's security.
- **Manually defined** lets you specify the group of hosts or networks that the IPS-1 Sensor protects. This reduces the load on the sensor by focusing the sensor’s resources on traffic that relates to internal networks.
- **None** does not specify a group of hosts or networks for protection. When no topology is configured, the IPS-1 Sensor inspects all traffic with a lower level of intensity. The IPS-1 Sensor will inspect traffic faster but without the high level of inspection provided by the **All IPs** and **Manually defined** settings.

**Latency Threshold**

The Latency Threshold suspends IPS inspection when the average latency of traffic passing through the sensor exceeds a specified threshold. The specified latency level will be treated as a Fail State. Then, traffic will be passed or dropped based on the Sensor bypass mode of the IPS-1 Sensor's General Properties. By default, this setting is off, but you can enable it from the IPS-1 Sensor’s IPS page.

**To create an IPS-1 Sensor object:**

1. If there is a Security Gateway between the management server and the IPS-1 Sensor, make sure **Accept IPS-1 management connections** is selected in the **Global Properties > Firewall** page.
2. In the **IPS** tab, select **Enforcing Gateways**.
3. Click **Add** and choose **IPS-1 Sensor**.
4. Enter the properties of the IPS-1 Sensor.
5. If there is a Security Gateway between the management server and the IPS-1 Sensor, install the policy on the gateway.
6. Open the IPS-1 Sensor object and click **Communication** to initiate SIC.
7. Once **SIC** is initialized, click **Close**.
8. Click **OK**.

The IPS-1 Sensor object is created and you can now include the IPS-1 Sensor in policy installation.
Note - If policy installation fails when the IPS-1 Sensor is set to an IPS-Inline Working Mode, log into the sensor’s CLI and check that the interfaces are set to work as inline pairs. Refer to the R71 IPS-1 Sensor Administration Guide.

CLI Commands

You can use these CLI commands to manage IPS on your gateways. You must be in expert mode to use the commands.

To see all available commands:
1. Open the CLI of a gateway.
2. Enter expert mode.
3. Type `ips` and press Enter.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ips stat</code></td>
<td>Show the IPS status of the gateway.</td>
</tr>
<tr>
<td>`ips on</td>
<td>off`</td>
</tr>
<tr>
<td><code>ips bypass stat</code></td>
<td>Show the Bypass Under Load status.</td>
</tr>
<tr>
<td>`ips bypass on</td>
<td>off`</td>
</tr>
<tr>
<td>`ips bypass set cpu</td>
<td>mem low</td>
</tr>
<tr>
<td><code>ips debug [-e filter] -o &lt;output_file&gt;</code></td>
<td>Create an IPS debug file.</td>
</tr>
<tr>
<td><code>ips refreshcap</code></td>
<td>Refresh the sample capture repository.</td>
</tr>
<tr>
<td><code>ips stats [-t &lt;timeout&gt;] -o &lt;output_file&gt;</code></td>
<td>Print IPS performance statistics. &lt;timeout&gt; is the period of time in which the statistics are gathered.</td>
</tr>
<tr>
<td><code>ips pmstats reset</code></td>
<td>Reset pattern matcher statistics.</td>
</tr>
<tr>
<td><code>ips pmstats -o &lt;output_file&gt;</code></td>
<td>Print pattern matcher statistics.</td>
</tr>
</tbody>
</table>
Chapter 4

Managing Profiles and Protections

IPS Profiles

IPS profiles enable you to configure sets of protections for groups of gateways. Without profiles you would have to configure IPS in a global policy for all your devices and network behavior, or configure each device separately. With profiles, you have both customization and efficiency.

Up to 20 profiles may be created. IPS profiles are available for all Check Point NGX gateways.

Note - For Connectra, IPS profiles are available for all NGX R66 gateways and above. Earlier versions of Connectra gateway do not receive an IPS profile from Security Management server. Every profile created takes 2 MB of RAM from the user console machine on both Windows and Motif.

Creating Profiles

When you create a profile, you create a new SmartDashboard object. Protections can be activated, deactivated or given specific settings to allow the profile to focus on identifying certain attacks. The profiles can then be applied to groups of devices that need to be protected against those certain attacks.

To create a profile:
1. In the IPS tab, select Profiles.
2. Click New and choose an option:
   - Create New Profile: Opens empty Profile Properties window for new configuration.
   - Clone Selected Profile: Creates copy of selected profile. Select the cloned profile and click Edit to make changes (including providing a new name) in the Profile Properties window.
Managing Profiles and Protections

3. Configure the **General** properties.
   - **Profile Name**: Mandatory, cannot contain spaces or symbols.
   - **Comment**: Optional free text.
   - **Color**: Optional color for SmartDashboard object mapping.
   - **IPS Mode**: The default action that a protection will take when it is enabled.
     - **Prevent**: Activated protections will block traffic matching the protection's definitions.
     - **Detect**: Activated protections will track traffic matching the protection's definitions.
   - **Protections Activation**: Protections can be enabled automatically or manually.
     - **Activate according to IPS Policy**: Let IPS activate protections automatically according to the IPS Policy criteria. (see "Automatically Activating Protections" on page 20)
     - **Manually activate protections**: Do not let IPS automatically activate protections; activate them as needed. (see "Manually Activating Protections" on page 22)

4. Select **IPS Policy > Updates Policy** and select whether newly downloaded protections should be set by default to **Prevent** or **Detect**.

5. Click **OK** to create the profile.

**Activating Protections**

Each profile is a set of activated protections and instructions for what IPS should do if traffic inspection matches an activated protection. The procedures in this section explain how to activate protections for a profile.

**Automatically Activating Protections**

IPS protections include many protections that can help manage the threats against your network. Care should be taken to understand the complexity of the IPS protections before manually modifying their settings.

To simplify the management of the IPS protections settings, a profile can be configured to automatically enable protections based on user defined criteria by selecting **Activate according to IPS Policy** in the Profile’s General properties.

When the IPS Policy activates a protection, the protection will enforce the action set in the IPS Mode, either **Detect** or **Prevent**. In some instances a protection will be set to **Detect** if it meets the criteria to be set to **Inactive** but does not support the Inactive status.

---

Check Point IPS Administration Guide R75.40 | 20
There are numerous protections available in IPS. It will take some time to become familiar with those that are relevant to your environment; some are easily configured for basic security without going too deeply into the details of the threat and the protection. Many protections can be safely activated automatically.

It is recommended that you allow IPS to activate protections according to the IPS policy in the beginning. Then you can manually modify the protection settings as needed according to your monitored traffic.

**To automatically activate protections in a profile:**
1. In the Profiles page, double-click a profile, or click New to create a new profile.
2. Select IPS Policy.
3. Set automatic activation by type:
   - **Client Protections**: activate protections specific to clients.
   - **Server Protections**: activate protections specific to servers.
   - **Both**: all protections will be activated, except for those that are:
     - Excluded by the options selected here
     - Application Controls or Engine Settings
     - Defined as Performance Impact — Critical
4. Set activation according to protection criteria. In the Protections to Deactivate area, select relevant criteria and then select the value that fits:
   - **Protections have severity**: Activate protections only if their Severity level is higher than the value you select in the drop-down list.
     For example: you can set protections with low severity to not be activated automatically (Do not activate protections with severity Low or below). You can always activate the protections that you want later, if analysis proves they are needed.
   - **Protections have confidence level**: Activate protections only if their Confidence Level is higher than the selected value.
     For example: Do not activate protections if with confidence-level Low or below. The higher the Confidence Level of a protection, the more confident Check Point is that recognized attacks are indeed attacks; lower Confidence Levels indicate that some legitimate traffic may be identified as an attack.
   - **Protections have performance impact**: Activate protections only if their Performance Impact is lower than the selected value.
     For example: Do not activate protections with performance impact High or higher. Some activated protections may cause issues with connectivity or performance. You can set protections to not be activated if they have a higher impact on gateway performance.
   - **Protocol Anomalies**: Do not automatically activate Protocol Anomaly protections.

**To exclude protection categories from the IPS Policy:**
1. In Profile Properties > IPS Policy, select Protections are in following categories and click Configure.
2. Click Add.

   The Select Category window opens.

3. Expand the tree nodes and select the categories, at any level that you want, that you do not want to be activated by the IPS Policy.

   For example, if you selected to automatically activate Server Protections and then add Syslog to the categories in the Non-Auto Activation window, the Syslog protections (such as Apply Malicious Code Protector) will not be automatically activated in this profile.

4. Click OK to close the Select Category window.
5. Click OK to close the Non-Auto Activation window.
6. Click OK to apply the Automatic Activation configuration and close the Profile Properties window.

**Manually Activating Protections**

You may need to activate protections that are not activated automatically. For example, you may have reason to suspect a specific threat against a gateway.
Note If you manually activate protections for a profile that has Detect-Only for Troubleshooting enabled, traffic will only be blocked once the Detect-Only for Troubleshooting has been disabled.

Activating Protections for All Profiles
To manually activate a protection in all profiles:
- In the Protections Browser, right-click on the protection that you want to activate and select the action that you want to apply to the protection.

Activating Protections for a Specific Profile
To manually activate a protection for a specific profile:
1. Find the protection that you want to activate using the Protections Browser and click Edit.
2. Select the profile for which you want to activate this protection and click Edit.
   The protection can be activated for one profile and inactive for another; thus, it will be activated for some gateways and inactive for others.
   If the protection is inactive and Action according to IPS Policy: Inactive is selected, this protection is inactive due to the IPS Policy for this profile. You can override this setting or change the IPS Policy criteria. For instructions on changing IPS Policy, see Automatically Activating Protections (on page 20).
   To override the settings for this protection, continue with this procedure.
3. Select Override IPS Policy and select the action that you want to apply.
   - Prevent: Activate IPS inspection for this protection and run active preventions on the gateways to which this profile is assigned.
   - Detect: Activate IPS inspection for this protection, tracking related traffic and events.
   - Inactive: Do not enforce this protection.
4. If available, configure the Additional Settings that are relevant for its individual configurations and options.
   Some common settings include:
   - Track: allows the administrator to define how he should be alerted about the protection.
     Examples of Track Actions: Log, Alert, Mail.
   - Capture Packets: allows the packets relevant to the protection to be captured for additional analysis at a later time. The packet capture can be viewed from the event in SmartView Tracker. Note that a packet capture is automatically attached to the first log of an attack even if this option is not selected. For more information see Working with Packet Information (on page 54).

Removing Activation Overrides
While configuring a profile, at any time you can manually set the activation of individual protections, overriding the automatic activation setting. If the result is not relevant, you can remove the overrides.

To remove overrides:
1. In the IPS tab, select Profiles.
2. Select a profile from the list and click **Actions > Remove overrides.**

   A message appears:
   
   Are you sure you want to reapply the profile’s IPS Mode and Activation settings to the protections?

3. To confirm, click **Yes.**

   A message appears:
   
   All protections have been reset to the profile’s settings.

4. Click **OK.**

### Managing Profiles

#### Assigning Profiles to Gateways

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

1. In the **IPS** tab, select **Enforcing Gateways.**
2. Select a gateway and click **Edit.**
   
   The **IPS** page of the gateway properties opens.
3. Select a profile from the **Assign profile** list.
4. Click **OK.**

**View Protected Gateways by Profile**

**To view a list of gateways that are protected by a specific profile:**

1. In the **IPS** tab, select **Profiles**
2. Select a profile from the list and click **Actions > Show Protected Gateways.**
   
   The **ProtectedGateways** window appears with the list of gateways that are assigned to the selected profile.

### Viewing Profile Modification Data

You can see data about modifications made to a selected profile.

**To see modification data:**

1. In the **IPS** tab, select **Profiles.**
2. Select a profile from the list and click **Actions > Last Modified.**
Managing Profiles and Protections

The **Last Modification** window opens.

- **Last modified at**: Date and time of last modification.
- **From client**: Name of client machine from which the profile was modified.
- **By Administrator**: Username of the administrator who did the modifications.

**Importing and Exporting Profiles**

IPS lets you import and export profiles using the `ips_export_import` command from the CLI. This command will let you copy profile configurations from one R71 management server to another R71 or R75 management server, or from one R75 management server to another R75 management server. This command is supported in both Security Management Server and Multi-Domain Security Management environments.

The exported profile is stored in a tar archive. The archive includes all protection settings but does not include:

- Network Exceptions
- Network object information that is specified in the protection settings

On a Multi-Domain Server, you must use one of these methods to set the environment in which the command will run:

- Run `mdsenv` to set the environment (Multi-Domain Server or specific Domain Management Server) where the IPS profile is configured.
- Use `-p <ip>` to enter the IP address of the Multi-Domain Server or Domain Management Server where the IPS profile is configured.

**To export an IPS profile**:

- From the command line, run:
  ```bash
  ips_export_import export <profile-name> [-o <export-file-name>] [-p <ip>]
  ```

  You must enter the exact name of the profile that you want to export.

  The archive will be named `<profile-name>.tar` and is saved to your present working directory. You can also use the `-o <file-name>` to give the archive a specific name.

**To import an IPS profile**:

- From the command line, run:
  ```bash
  ips_export_import import <new-profile-name> -f <file-name> [-p <ip>]
  ```

  You must enter a name for the profile and the location of the archive. You can either import an archive that is in your present working directory or enter the exact location of the archive that you want to import.

**Deleting Profiles**

You can easily delete a profile (except for the **Default_Protection** profile), but it should be done carefully, as it may affect gateways, other profiles, or SmartDashboard objects.
To delete a profile:
1. In the IPS tab, select Profiles.
2. Select the profile you want to delete and click Delete.
   The message appears: Are you sure you want to delete object <profile_name>?
3. Click Yes.
   If the profile contains references to/from other objects, another message appears:
   <profile_name> is used in another object.
   Are you sure you want to delete it?
4. Click Where Used?
   The Object References window opens.

For each object that references the profile, there is a value in the Is Removable? column. If this value is Yes for all objects, you can safely delete the profile. Otherwise, you should discover the relationship before deciding to delete this profile.

Troubleshooting Profiles
IPS includes the ability to temporarily stop protections set to Prevent from blocking traffic. This is useful when troubleshooting an issue with network traffic.

To enable Detect-Only for Troubleshooting:
1. Select IPS > Profiles.
2. Select a profile and click Edit.
   The Profile Properties window appears.
3. Select Troubleshooting.
4. Click on the Detect-Only for Troubleshooting icon.

Once you have done this, all protections set to Prevent will allow traffic to pass, but will continue to track threats according to its Track configuration.

Customizing Profiles for IPS-1 Sensors
Protections enforced by the IPS-1 Sensor offer certain configuration options that differ from the options available for protections enforced by the IPS Software Blade. Some of these options are:
- Configuring the number of packets to capture when Capture Packets is enabled
- Automatically blocking, or quarantining, connections from a specific IP address for a set period of time once an attack from that address has been detected
- Dynamically changing the Confidence Level for a protection based on the type of traffic that passes through the IPS-1 Sensor
- Blocking an attack by dropping the connection without notifying the sender or by sending a Reject packet back to the sender to notify the sender that the traffic was not received
- Grouping recurring alert logs into Summary logs which indicate how frequently the alert has occurred without adding unnecessary log entries to the database

These are the IPS-1 Sensor settings that you can define in the IPS Profile:

**Capture Packets**
- **Turn on capture packets for all protections** automatically captures packets for all active protections that have this capability.
- **Turn on capture packets according to protections settings** relies on the protections' settings to determine when packet captures are saved.
- **Number of packets to capture** specifies the number of packets you will be able to look at for each time packets are captured.

**Quarantine**
- **Quarantined IP addresses will be released after X seconds** specifies how long all traffic from a particular IP address will be rejected once that IP address has been identified as a threat.

**Dynamic Confidence Level**
- **Automatically deactivate protections when their dynamic Confidence-Level falls below the threshold** allows IPS to dynamically change turn off protections when an internal IPS algorithm determines that IPS is not identifying the attack with sufficient accuracy. This option is only available when protections are activated according to the IPS Policy, and the IPS Policy is set to deactivate protections based on Confidence-Level.

**Connection Refusal Method**
- **Drop** blocks the connection without notifying the sender of the failure.
- **Reject (TCP Reset)** blocks the connections and sends the sender a Reject packet to indicate that the connection was not accepted.

**Log Flood Suppression**
- **Enable Log Suppression** enables you to receive summary logs for frequently identified attacks. Specify settings for this feature using the **Advanced** button.

### Protections Browser

The Protections Browser provides quick access to IPS protections and displays them with a summary of important information and usage indicators.

#### Customizing the Protections Browser View

The Protections page shows a table of the protections, with each column a different type of information.

**Protections Columns**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>See for details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>Name of the protection</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Protocol category and bread-crumbs to find the protection in the category tree</td>
<td></td>
</tr>
</tbody>
</table>
### Managing Profiles and Protections

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>See for details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Probable severity of a successful attack on your environment</td>
<td>Severity (on page 32)</td>
</tr>
<tr>
<td>Confidence Level</td>
<td>How confident IPS is that recognized attacks are actually undesirable traffic</td>
<td>Confidence Level (on page 32)</td>
</tr>
<tr>
<td>Performance Impact</td>
<td>How much this protection affects the gateway's performance</td>
<td>Performance Impact (on page 32)</td>
</tr>
<tr>
<td>Industry Reference</td>
<td>International CVE or CVE candidate name for attack</td>
<td></td>
</tr>
<tr>
<td>Release Date</td>
<td>Date the protection was released by Check Point</td>
<td></td>
</tr>
<tr>
<td>Protection Type</td>
<td>Whether the protection is for servers, clients, or both</td>
<td>Type (on page 30)</td>
</tr>
<tr>
<td>Follow Up</td>
<td>Whether the protection is marked for Follow Up</td>
<td>Tracking Protections using Follow Up (on page 57)</td>
</tr>
<tr>
<td>Follow Up Comments</td>
<td>Text to comment on the protection</td>
<td></td>
</tr>
<tr>
<td>Products</td>
<td>Whether the protection is enforced by IPS Software Blades or IPS-1 Sensors</td>
<td></td>
</tr>
<tr>
<td>&lt;profile_name&gt;</td>
<td>Activation setting of the protection in the profile</td>
<td>Protection Mode (on page 31)</td>
</tr>
</tbody>
</table>

### To change which columns are visible:
1. Click View > Customize.
   The Customize window opens.
2. Any column you do not want to appear, move to the Available fields list; any you do want to see, let them remain in the Visible fields list.
3. Click OK.

### Finding Protections

Use the Protections page for filtering the complete protections list. You can filter by protection name, CVE number, or by any information type that is displayed in the columns.

#### To filter by protection name:
1. Leave the Search In box at the default All, or select Protection.
2. Start to type the name in the Look for text box.
   The displayed list filters as you type. Note that the results include not only the name of the specific protection, but also the category tree in which it is contained.
   For example, to see ICMP protections, type icmp in Look for, and select Protection in Search In. The list shows protections that have ICMP in their name, and all protections in the Network Security > IP and ICMP category. If you hover over a listed protection, the category tree is shown as a tooltip.

### Filtering Protections

You can filter the list of protections by any criteria that is displayed in the Customizing the Protections Browser View (on page 27) table.

#### To filter by any information:
1. Select the information type from the search In drop-down menu.
   By default, the search will return protections that have your search term in any field.
2. In the **Look for** text box, type a value for the information.
   For example, to see only protections who have a value of *Severity: Critical*, type **critical** in **Look for** and select **Severity** in **In**.

### Sorting Protections

Filtering by information type has a draw-back: you have to know valid values for the information. In the beginning, you might find it more convenient to sort the list rather than filter it.

**To sort the protections list by information:**

- Click the column header of the information that you want.
  
  For example, to see protections ordered by **Severity**, beginning with **Critical**, click the **Severity** column header.

### Advanced Sorting

You can sort the list with multiple criteria: first sort by criteria A and then by criteria B.

For example, if you wanted to see protections that are marked for **Follow Up**, but you want to start with the most critical protections, you can sort by **Follow Up** and by **Severity**.

**To sort by multiple values:**

1. Click **View > Sort**.

   The Sort window opens.

   2. Choose the column headers by which you want to sort the list and then click **OK**.
Exporting Protections List

To enable administrators to analyze protections in alternative applications, you can export the Protections list as a comma-delimited file. The exported information includes all protections, with all table fields regardless of any applied sorting or filtering.

To export the Protections list:
1. Click View > Export View.
2. In the Save As dialog box, provide a filename and click Save.

Protection Parameters

Most protections have graded parameters, provided to help you decide which protections to activate for security and which can be safely deactivated, for connectivity and performance.

The protection parameters and their values for a specific protection appear at the top of the protection window.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Indicates</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong> (on page 30)</td>
<td>Type of machine that can be affected/protected</td>
<td>Signature, Protocol Anomaly, Application Control, Engine Settings</td>
</tr>
<tr>
<td><strong>Severity</strong> (on page 32)</td>
<td>How severely a successful attack would affect your environment</td>
<td>Low, Medium, High, Critical</td>
</tr>
<tr>
<td><strong>Confidence Level</strong> (on page 32)</td>
<td>How well an attack can be correctly recognized</td>
<td>Low, Medium-Low, Medium, Medium, Medium-High, High</td>
</tr>
<tr>
<td><strong>Performance Impact</strong> (on page 32)</td>
<td>How much this protection affects the gateway’s performance</td>
<td>Low, Medium, High, Critical</td>
</tr>
<tr>
<td><strong>Protection Type</strong> (on page 32)</td>
<td>Type of machine that can be affected/protected</td>
<td>Servers, Clients, Servers and Clients</td>
</tr>
</tbody>
</table>

Type

The Type is whether the protection is a Signature, Protocol Anomaly, Application Control, or Engine Setting.
### Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Usage Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature</td>
<td>Prevent or detect threats by identifying an attempt to exploit a specific vulnerability</td>
<td>Microsoft Message Queuing contains a vulnerability that could allow an attacker to remotely execute code; you activate the applicable Microsoft Message Queuing protection to protect against such an attack.</td>
</tr>
<tr>
<td>Protocol Anomaly</td>
<td>Prevent or detect threats by identifying traffic that does not comply with protocol standards</td>
<td>An attacker can send HTTP packets with invalid headers in an attempt to gain access to server files; you activate the Non Compliant HTTP protection to protect against such an attack.</td>
</tr>
<tr>
<td>Application Control</td>
<td>Enforce company requirements of application usage</td>
<td>Your organization decides that users should not use Peer to Peer applications at the office; you activate the Peer to Peer Application Control protections.</td>
</tr>
<tr>
<td>Engine Setting</td>
<td>Configure IPS engine settings</td>
<td>Configuring settings will influence other protections; be sure to read any notes or warnings that are provided.</td>
</tr>
</tbody>
</table>

IPS protections are divided by these types under **Protections > By Type**.

For example, view all Application Controls supported by IPS by selecting **Protections > By Type > Application Control**.

### Protection Mode

Each protection has a mode, which determines whether IPS inspects packets for this protection, and if so, what it does if the packet matches a threat symptom.

- **Inactive**: Packets are not inspected for this protection.
- **Active**: Packets are inspected and actions taken (depending on Detect or Prevent).
- **Prevent**: Packets are inspected and threatening packets or connections are dropped.
- **Detect**: Packets are inspected and threatening packets or events are tracked.

The next sections, that explain the protections in detail, assume that the protection is Activated, to explain the configuration options that are available only when the protection is Active.

If the IPS policy settings cause a protection to be **Inactive**, and you want to activate it, select **Override with the action**: and choose **Prevent** or **Detect** from the drop-down list.

Some protections may be **Partially active**: the protection settings configured to activate the protection for specific protocols or situations, leaving it inactive for others. For example, in **DNS - General Settings**, you can select to activate DNS protections only for TCP or only for UDP, so the protections in the DNS category...
are **Partially active**. If you select to activate DNS protections for both TCP and UDP, the protections will be **Active**.

The mode of a protection is per-profile. See Managing Profiles (on page 24).

### Severity

You should activate protections of **Critical** and **High Severity**, unless you are sure that you do not want this particular protection activated.

For example, if a protection has a rating of **Severity: High**, and **Performance Impact: Critical**, you might want to determine whether the protection is necessary for your specific environment before activating the protection.

### Confidence Level

Some attack types are more subtle than others, and legitimate traffic may sometimes be mistakenly recognized as a threat. The confidence level value indicates how well this particular protection can correctly recognize the specific attack.

The Confidence parameter can help you troubleshoot connectivity issues with the firewall. If legitimate traffic is blocked by a protection, and the protection has a **Confidence** level of **Low**, you have a good indication that more specific configurations might be needed on this protection.

### Performance Impact

Some protections by necessity use more resources or apply to common types of traffic, causing an adverse effect on the performance of the gateways on which they are activated.

**Note** - The Performance Impact of protections is rated based on how they will affect gateways of this version running SecurePlatform and Windows operating systems. The Performance Impact on other gateways may vary from the rating listed on the protection.

For example, you might want to ensure that protections that have a Critical or High Performance Impact are not activated unless they have a Critical or High Severity, or you know the protection is specifically needed.

If your gateways experience heavy traffic load, be careful about activating High/Critical Performance Impact protections on profiles that affect a large number of mixed (client and server) machines.

Using the value of this parameter to decide upon an optimal protection profile will prevent overloading your gateway's resources.

### Protection Type

Signature and Protocol Anomaly protections are designed to protect against threats that target either Servers or Clients. You can use this information to define a profile that will only focus on the threats that can exploit the network resources behind your enforcing gateway, thereby reducing the performance impact on the gateway and the amount of logs which the gateway will produce.

For example, if you have an enforcing gateway which protects servers in a DMZ, you can apply a profile that deactivates the Client protections because the client vulnerabilities are most likely not present on the protected resources.

### Protected Servers

Certain protections are designed to inspect traffic based on the type of server that the traffic is coming to or from. To allow these protections to identify the traffic that should be inspected, IPS requires you to identify the DNS, Web and Mail servers you want to protect.
**DNS Servers**

The DNS protocol protections prevent illegal DNS packets over TCP or UDP, prevents users from accessing blocked domain addresses, protect from DNS Cache Poisoning, and block DNS traffic to non-DNS destinations.

These protections will only apply to servers that are defined as DNS Servers in Protections > By Protocol > IPS Software Blade > Application Intelligence > DNS > DNS Servers View.

**Defining DNS Servers**

Configure a list of DNS servers in your environment to ensure that IPS enforces the DNS protections on the relevant devices.

**To define a host as a DNS server:**
1. Make sure the host is defined as a SmartDashboard object.
2. In the DNS Servers View, click Add to add another host to the list of DNS servers.
3. Select the host that you want to add to the DNS server list.
   - Click Edit to view or change the properties of the host before defining it as a DNS server.
   - Click OK to add the host to the list of DNS servers.

**Editing DNS Servers**

After a host is defined as a DNS server (added to the DNS Servers View list), it gains the DNS Server properties in its Host Node properties.

**To edit a DNS server:**
1. Select the host in the DNS Servers View list and click Edit.
2. In the left-hand category tree of the Host Node window, click Protections under the DNS Server category.

The Protections page displays a note that although you can select specific security settings for this server, the enforcement of this protection depends on the IPS profile to which this server is assigned. See "IPS Profiles" for more information on profiles.

**Web Servers**

The Web protocol protections prevent attacks that use web protocols and vulnerabilities to damage your network or use your network resources to attack other networks. Web servers require special protection from these attacks.

You can manage the use of these protections on Web Server from Protections > By Protocol > IPS Software Blade > Web Intelligence > Web Servers View.

**Defining Web Servers**

Configure a list of Web servers in your environment to ensure that IPS enforces the Web Server protections on the relevant devices.

**To define a host as a Web server:**
1. Make sure the host is defined as a SmartDashboard object.
2. In the IPS tab, open Protections > By Protocol > Web Intelligence > Web Servers View.
3. Click Add to add another host to the list of Web servers.
4. Select the host that you want to add to the Web server list.
   - Click Edit to view or change the properties of the host before defining it as a Web server.
   - Click OK to add the host to the list of Web servers.
Editing Web Servers

After a host is defined as a Web server (added to the Web Servers View list), it gains the Web Server properties in its Host Node properties.

To edit a Web server:
1. Select the host in the Web Servers View list and click Edit.
2. In the left-hand category tree of the Host Node window, click Protections under the Web Server category.

   The Protections page displays a note that although you can select specific settings for this server, the enforcement of this protection depends on the IPS profile to which this server is assigned. See IPS Profiles (on page 19) for more information on profiles.

Mail Servers

The Mail protocol protections prevent improper POP3, IMAP and SMTP traffic from damaging your network. These protections will only apply to servers that are defined as Mail Servers in Protections > By Protocol > IPS Software Blade > Application Intelligence > Mail > Mail Servers View.

Defining Mail Servers

Configure a list of Mail servers in your environment to ensure that IPS enforces the Mail protections on those devices.

To define a host as a Mail server:
1. Make sure the host is defined as a SmartDashboard object.
2. In the IPS tab, open Application Intelligence > Mail > Mail Servers View.
3. Click Add to add another host to the list of Mail servers.
4. Select the host that you want to add to the Mail server list.
5. Click OK to add the host to the list of Mail servers.

Editing Mail Servers

After a host is defined as a Mail server (added to the Mail Servers View list), the Mail Server properties page is added to the object’s Host Node properties.

To edit a Mail server:
1. Select the host in the Mail Servers View list and click Edit.
2. Click Protections under the Mail Server category.

   The Protections page displays a note that, although you can select specific security settings for this server, the enforcement of this protection depends on the IPS profile to which this server is assigned.
Chapter 5

Configuring Specific Protections

In This Chapter

Configuring Network Security Settings 35
Configuring Application Intelligence 40
Configuring Web Intelligence 44
Managing Application Controls 48
Configuring Geo Protections 48
Configuring IPS Pattern Granularity 50
Configuring Implied IPS Exceptions 51

IPS contains a large array of protections that prevent attacks, protect against vulnerabilities in network protocols, and close unnecessary entry points into the network. In SmartDashboard, each protection is accompanied by a description of the protection as well as other useful information.

You can find here instructions for configuring some of the more commonly used protections.

Included Protections:

- Aggressive Aging Configurations 36
- Anti Spoofing Configuration Status 36
- Citrix ICA 43
- Configuring Web Intelligence Protections 44
- Connectivity/Performance Versus Security 47
- Customizable Error Page 46
- DShield Storm Center 39
- FTP 41
- Instant Messengers 42
- IP Fragments 38
- Mail 40
- Microsoft Networks 41
- MS-RPC 44
- Peer-to-Peer 41
- Receiving Block List 36
- Remote Control Applications 44
- SNMP 43
- Streaming Engine Settings 36
- VoIP 43
- VPN Protocols 43

Configuring Network Security Settings

These pages allow you to configure protection against attacks which attempt to target network components or the firewall directly.

Some of the Network Security protections apply to the firewall in general, providing quick access to specific firewall features. The following sections will help you become familiar with these protections.
Streaming Engine Settings

The Streaming Engine Settings protect against improper use of the TCP or UDP protocols. IPS analyzes the TCP and UDP packets to verify that they conform to proper communication conventions.

Changing the default settings will enable crafted traffic to bypass IPS protections and is not recommended.

Receiving Block List

The security administrator configures the IPS Block List option by selecting Network Security > DShield Storm Center > Retrieve and Block Malicious IPS. Malicious IPS can be blocked for all gateways or for specific gateways.

An agent (daemon) on each enforcing gateway for which malicious IP are to be blocked receives the Block List of malicious IP addresses from [http://secure.dshield.org/block_list_info.html](http://secure.dshield.org/block_list_info.html). Following every refresh interval (by default, three hours), the agent takes the Block List and updates the security policy with the IP address ranges in the Block List. This process is logged in the SmartView Tracker.

Anti Spoofing Configuration Status

Anti Spoofing is an integral protection of Check Point hosts. The Network Security > Anti Spoofing Configuration Status page shows which on which Check Point hosts this feature is not enabled, and provides direct access to enabling it.

To enable Anti Spoofing:

1. In the IPS tab, open Protections > By Protocol > Network Security > Anti Spoofing Configuration Status.
2. Select a gateway in the list and click Edit.
3. In Check Point Gateway > Interface Properties > Topology, select any option other than Internal > Not Defined.

   Thus, to enable Anti-Spoofing, you must first be able to define or estimate the topology of the selected gateway.
4. Select Perform Anti-Spoofing based on interface topology, and any of the relevant Anti-Spoofing features.
5. Click OK.

   The gateway is immediately removed from the Anti Spoofing Configuration Status list.

Aggressive Aging Configurations

Within the Denial of Service category is Aggressive Aging, a protection page whose configurations affect protections of various categories. Aggressive Aging manages the connections table capacity and the memory consumption of the firewall to increase durability and stability. It allows a gateway to handle large amounts of unexpected traffic, especially during a DoS attack.

Normally, sessions have a regular timeout, defined in the Stateful Inspection page of Global Properties (see Policy menu > Global Properties > Stateful Inspection). When a connection is idle for longer than its defined timeout, it is marked as Eligible for Deletion.

With this protection you can:

- Set faster timeouts, aggressive timeouts, ensuring that sessions are dropped faster during times of heavy load, maintaining overall connectivity
- Set the connections table and memory consumption thresholds that determine when the aggressive timeouts are used rather than the normal timeouts

Configuring Aggressive Timeouts

You configure the aggressive timeouts for all profiles. Each timeout value is for a different type of session.

To configure aggressive timeouts:

2. Select the aggressive timeouts that you want to be enforced, and change the default values as needed. The Aggressive Aging value must be lower than the default session timeouts. As the regular values can also be changed, it is recommended that you review them before changing the aggressive timeout values.

To see regular timeouts: click Policy menu > Global Properties > Stateful Inspection. These settings are global to all profiles and all gateways.

### Aggressive Aging Timeouts

<table>
<thead>
<tr>
<th>IP Protocol/State</th>
<th>Aggressive Timeout (sec)</th>
<th>Regular Timeout (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Start Session</td>
<td>5</td>
<td>25</td>
</tr>
<tr>
<td>TCP Session</td>
<td>600</td>
<td>3600</td>
</tr>
<tr>
<td>TCP End Session</td>
<td>3</td>
<td>20</td>
</tr>
<tr>
<td>UDP virtual session</td>
<td>15</td>
<td>40</td>
</tr>
<tr>
<td>ICMP virtual session</td>
<td>3</td>
<td>30</td>
</tr>
</tbody>
</table>

**Note** - If you want to set an aggressive timeout on another protocol, you can select Other IP Protocols Virtual Session. The default for the Stateful Inspection timeout is 60 seconds. If you select this option in the Aggressive Timeout page, the default aggressive timeout is 15 seconds.

### Configuring Thresholds

Now that you have the two different sets of timeouts, when is Aggressive Aging enforced over the regular timeouts?

The major benefit of Aggressive Aging is that it starts to operate when the machine still has available memory and the connections table is not entirely full. Thus, it reduces the chances of connectivity problems that might have occurred under low-resource conditions.

Aggressive Aging is activated according to thresholds to the memory consumption or the connections capacity that you configure. If a defined threshold is exceeded, each incoming connection triggers the deletion of ten connections from the Eligible for Deletion list. An additional ten connections are deleted with every new connection until the threshold falls below the enforcement limit. If there are no Eligible for Deletion connections, no connections are deleted at that time, but the list is checked after each subsequent connection that exceeds the threshold.

**To configure Aggressive Aging thresholds:**

1. Select the profile for which you want to edit the settings and click **Edit**.
2. Activate the **Aggressive Aging** protection.

3. Configure the limits for the Connections table and Memory consumption.

   Default is 80%, with connections from the Eligible for Deletion list being deleted if either the Connections table or Memory consumption passes this limit. You can change this default by selecting one or the other:
   - Connections table exceeds ___% of its limit
   - Memory consumption exceeds ___% of the gateway’s capacity

   The limits for the Connections table and Memory consumption are set for each profile, so may be different for different gateways.

   Timeout settings are a key factor in memory consumption configuration. When timeout values are low, connections are deleted faster from the table, enabling the firewall to handle more connections concurrently. When memory consumption exceeds its threshold, it is best to work with shorter timeouts that can maintain the connectivity of the vast majority of the traffic.

   **Note** - If a SecureXL device does not support Aggressive Aging, the feature is disabled. When this happens, the action is logged and a console message is generated.

---

**IP Fragments**

IP packets may legitimately be fragmented. For example, some connections might go through a network with an MTU with a smaller packet size limit. This MTU will then break up larger packets into IP fragments, and the destination re-assembles the fragments into packets.

A security threat exists, with the possibility of an attacker deliberately breaking a packet into fragments and inserting malicious data, or holding back some fragments to cause a Denial of Service attack by consuming the resources needed to store the fragments until the packets can be re-assembled.

IPS provides optional protections against IP fragment threats.

- **Forbid IP Fragments**: the most secure option, but it may block legitimate traffic.
- **Configure IP Fragment limits**: set the maximum number of packets that the gateway will hold, with a timeout, to release resources and prevent DoS attacks.
- **Capture Packets**: track IP fragments and capture the data for observation and troubleshooting (see Working with Packet Information (on page 54)).
Configuring IP Fragments Thresholds

The IP Fragment protection is configured for each profile, so different gateways may be configured differently.

To configure a IPS profile to handle IP fragments:
1. Open the Network Security > IP and ICMP > IP Fragments protection.
2. Select the profile for which you want to edit the settings and click Edit.
3. Select Allow IP Fragments.
4. Set the value for Maximum number of incomplete packets.
   If this threshold is exceeded, the oldest fragments are dropped (default is 200).
5. Set the value for Discard incomplete packets after __ seconds.
   If fragments of a packet are held after this threshold, waiting for the missing fragments, they are all dropped (default is one second).

Blocking IP Fragments

To configure a IPS profile to block all IP fragments:
1. Open the Network Security > IP and ICMP > IP Fragments page.
2. Select Forbid IP Fragments.
   All IP fragments will be blocked; fragmented packets will be dropped.

DShield Storm Center

The range and sophistication of the techniques used by hackers to penetrate private networks is ever increasing. However, few organizations are able to maintain up-to-date protection against the latest attacks. Network Storm Centers are collaborative initiatives that were set up to help security administrators maintain the most up-to-date solutions to security threats to their networks. Storm Centers achieve this by gathering logging information about attacks and sharing it with other organizations from around the world. Storm Centers collate and present reports on threats to network security in a timely and effective manner.

The IPS Storm Center module is included in the Check Point Security Gateway. It enables communication between the Network Storm Centers and the organizations requiring network security information.


IPS integrates with the SANS DShield.org Storm Center. The DShield.org Storm Center produces a Block List report which is a frequently updated list of address ranges that are recommended for blocking. The IPS Storm Center module retrieves and adds this list to the security policy.

Retrieving and Blocking Malicious IPS

To retrieve and block malicious IPS:
1. In the Firewall Rule Base, define appropriate rules as necessary. Security Gateways and Security Management servers must be able to connect to the Storm Center using HTTPS.
2. In the IPS tab, select Network Security > DShield Storm Center > Malicious IPS.
3. Select the profile for which you want to edit the settings and click Edit.
   Note - Ensure that the Block List is enforced on perimeter gateways ONLY.
4. Install the security policy.

Manually Configuring the Blocking of Malicious IPS

When configured through IPS, the DShield Block List is enforced before the Rule Base. Because DShield uses statistical analysis and the Block List is made up of /24 (Class C) networks, not all of those IP addresses are necessarily malicious. Therefore, in order to prevent reputable IP addresses from being blocked, you can manually add a Block List rule in the Firewall Rule Base.
To manually configure blocking malicious IPS:

1. In IPS, select **Network Security > DShield Storm Center**.
2. Clear the **Retrieve and Block Malicious IPS** option.
3. Add the Block List rule:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Install On</th>
<th>Track</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPDSshield</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
<td>Policy Targets</td>
<td>UserDefined</td>
<td>Block List Rule</td>
</tr>
</tbody>
</table>

4. Place the Block List rule as high as possible in the Firewall Rule Base, but below all authentication rules and any other rules for trusted sources that should not be blocked.

5. To retrieve and block malicious IPS only at particular gateways, specify them in the **Install On** cell of the rule.

   ![Note](Note: Ensure that the Block List is enforced on perimeter gateways ONLY.)

6. Install the security policy.

**Authenticity is Assured**

The Block List is securely transferred and authenticated through SSL. The Certificate of the Storm Center Certificate Authority, which comes with the Storm Center module, is stored locally and serves to verify the authenticity of the origin of the received Block List.

The Certificate Authority of SANS DShield.org is Equifax. **equifax.cer** is the file name of the locally stored certificate, which is stored in the **conf** directory of the Storm Center module installation.

**Log Size and Effect on Gateway Performance**

Receiving the Block List does not affect gateway performance because only a very small amount of data is received.

**Configuring Application Intelligence**

A growing number of attacks attempt to exploit vulnerabilities in network applications rather than targeting the firewall directly. Application Intelligence is a set of advanced capabilities that detects and prevents application layer attacks. Based on the INSPECT intelligent inspection technology, Application Intelligence gives IPS the ability to protect against application attacks and hazards.

**Mail**

You can activate protections for the protocols that your environment uses for mail, adding customized security to the Mail servers that are already in place.

Various settings and specific definitions are available in the **Mail** protection pages; see the following subsections.

**Setting POP3/IMAP Scope**

By default, the configurations of **Application Intelligence > Mail > POP3/IMAP Security** are applied to all hosts defined as Mail servers depending upon the Action settings of each IPS profile. However, you can limit the scope of this protection by selecting to only apply this protection to specific Mail servers.

To specify hosts that will get these protection settings:

2. Select the profile for which you want to edit the settings and click **Edit**.
3. In the **Protection Scope** area, click **Apply to selected mail servers**.
4. Click **Customize**.
The **Select Servers** window appears with all of the Mail servers selected by default.

5. Clear the servers on which POP3 and IMAP protections should not be enforced, or click **Add** to add more hosts to this list, if needed.

**Defining POP3 Commands**

The **POP3/IMAP Security** protection has a list of commands that IPS will recognize and inspect. The definitions of the POP3 commands apply to all IPS profiles.

**To change the list of POP3 commands:**

1. In the IPS tab, open **Application Intelligence > Mail > POP3/IMAP Security**.
2. In the **Relative Distinguished Names** section, click **Edit**.
   
   The **Add custom POP3 command** window appears.
   
   a) To add a new command, click **Add**. A new item in the list is created. Provide the command that you want to add and then click **OK**.
   
   b) To change an existing command, select the command and click **Edit**. Change the command as needed and then click **OK**.

   The new or changed commands appear immediately in the commands list.

**To block or allow a POP3 command for a profile:**

1. In the IPS tab, open **Application Intelligence > Mail > POP3/IMAP Security**.
2. Select the profile for which you want to edit the settings and click **Edit**.
3. In the list of **Known POP3 commands**, clear any command that you do not want blocked.

**FTP**

You can configure various protections related to the FTP protocol. For example, activating (on Prevent) the Block Port Overflow protection, will check and prevent any attempt to use an FTP server as an agent for a malicious operation.

You can create a Black List of FTP commands that will be blocked, by moving commands to the Blocked Commands list on the Blocked FTP Commands page.

**Microsoft Networks**

The protections in this category refer to the CIFS protocol and protection against File and Print Sharing worms.

IPS uses pattern matching to recognize and block worms. You can add or edit to the pattern lists in the File and Print Sharing protection against worms. These definitions apply to all profiles.

**To define patterns to be blocked:**

1. In the IPS tab, open **Application Intelligence > Microsoft Networks > File and Print Sharing**.
2. In the **Block File and Print Sharing Worms** list, make sure that the worms that you want to block are selected.
3. At the top of the page, click **Edit**.
4. Click **Add** to add a new worm pattern, or select an existing worm name and click **Edit**.
5. Provide a name for the known worm pattern.
6. Provide the pattern string, or click **Paste from clipboard**, if the string has been copied to the clipboard.
7. Click **Recalculate** to get the real Checksum.
8. Click **OK**.

The new or changed worm name appears immediately in the **Block File and Print Sharing Worms** list.

**Peer-to-Peer**

IPS can block peer-to-peer traffic by identifying the proprietary protocols, even if the application switches ports, and preventing the initial connection to the peer to peer networks. This not only prevents, but also searches operations. The pages in this category are all Application Control: activate them to enforce company policy against peer-to-peer applications; they do not protect against malicious behavior.
Peer to Peer General Exclusion Settings

Note - The Peer to Peer General Exclusion Settings option is replaced with Network Exceptions for R70 gateways and above. It still applies to gateways of pre-R70 versions.

General Exclusion Settings allow you to exclude services or network objects from IPS detection and blocking; to allow specific services or gateways to pass without inspection.

To exclude services or objects from peer-to-peer application control:
1. In the IPS tab, open Application Intelligence > Peer to Peer - Global Exclusion Settings.
2. Choose the exclusion settings that you want:
   - Exclude specific services from <application type> detection: allow certain services to pass without detection or blocking.
   - Exclude network objects from <application type> detection: allow certain machines to use the application services.
3. For each setting selected, click Configure.
4. In the window that opens, select each service or object that you want to exclude from these application blocking controls and click Add.

Defining Peer to Peer HTTP Headers

Each protection under Peer to Peer has a Masquerading over HTTP Protocol section. In this section you can add patterns or regular expressions to match in the HTTP header of the Request or Response.

To configure peer to peer pattern matching:
1. Open a protection page under Application Intelligence > Peer to Peer.
   The blocked patterns are shown in the list at the bottom of the page.
2. Click Edit Patterns at the top of the protection page.
3. Click Add or select an existing pattern and click Edit.
4. In Header Name, provide the header name of the HTTP Request/Response to match.
5. In Header Value, provide a regular expression that the header value of the HTTP Request/Response to match.
   For more information, see Regular Expressions (on page 84).
6. Click OK.

The new or changed header pattern is added immediately to the list on the bottom of the page.

Instant Messengers

You can block Instant Messaging applications, or any of the features. For example, you could allow MSN Messenger Chat, but block Video.

Instant Messengers General Exclusion Settings

Note - The Peer to Peer General Exclusion Settings option has been replaced with Network Exceptions for R70 gateways and above. It still applies to gateways of pre-R70 versions

General Exclusion Settings allow you to exclude services or network objects from IPS detection and blocking; to allow specific services or gateways to pass without inspection.

To exclude services or objects from instant messenger application control:
1. In the IPS tab, open Application Intelligence > Instant Messengers - Global Exclusion Settings.
2. Choose the exclusion settings that you want:
   - Exclude specific services from <application type> detection: allow certain services to pass without detection or blocking.
• **Exclude network objects from <application type> detection**: allow certain machines to use the application services.

3. For each setting selected, click **Configure**.
4. In the window that opens, select each service or object that you want to exclude from these application blocking controls and click **Add**.

**VoIP**

Voice and video traffic must be protected as it enters and leaves a network. Potential threats to voice and video traffic are:

* Call redirections whereby calls intended for one recipient are redirected to another.
* Stealing calls, where the caller pretends to be someone else.
* System hacking using ports opened for VoIP connections.

VoIP calls involve a series of complex protocols, each of which can carry potentially threatening information through many ports.

IPS ensures that caller and recipient addresses are valid and that the caller and recipient can make and receive VoIP calls. IPS also examines the contents of the packets passing through every allowed port to ensure that they contain the proper information. Full stateful inspection on H.323, SIP, MGCP and SCCP commands ensures that all VoIP packets are structurally valid and that they arrive in a valid sequence.

**SNMP**

IPS enables you to protect against SNMP vulnerabilities by providing the option of enforcing SNMPv3 (the latest SNMP version) while rejecting previous versions. In addition, IPS can allow all SNMP versions while dropping requests with SNMPv1 and SNMPv2 default community strings.

**VPN Protocols**

IPS enables you to configure enforcement of RFC 2637: Point-to-Point Tunneling Protocol on Virtual Private Networks.

**Citrix ICA**

The Independent Computing Architecture (ICA) protocol specifies platform-independent data transfer between server and clients over the Internet and intranets. Applications built on ICA are numerous: browsers, Microsoft Accessories, mail clients, and more. IPS can protect against various ICA-related vulnerabilities and can enforce protocol compliance.

**Defining Allowed Applications**

Citrix ICA applications are blocked, when this protection is activated in Prevent mode. You can define which of these applications to allow.

**To define the Authorized Applications list:**

1. In the IPS tab, open **Application Intelligence > Citrix ICA > Citrix ICA Unauthorized Application**. The Authorized Applications list shows applications that have already be entered into the list.

   To block an authorized application, select a profile and then deselect the application in the Authorized Applications list.

2. To configure the Authorized Applications list, click **Configure**.

3. To add an application to the list, click **Add**.

   In the new entry that is created, provide the application name. Double-click the identifier entry and provide the application identifier.

4. To edit an application in the list, click **Edit**.

   Change the application name as needed, and then double-click the identifier and change it as needed.

5. Click **OK**.
The new or changed application names appear immediately in the **Authorized Applications** list.

**Remote Control Applications**

IPS can block a variety remote control applications which allow remote control over a host. Most remote control applications have the capacity to tunnel into an organization through an outbound connection initiated by the client to a “broker” over HTTP. This enables remote control applications to gain access to internal hosts from the internet enabling attackers to, for example, take over hosts in the network or open a hole for data leakage.

Standard firewall rules cannot sufficiently protect against remote control applications. IPS uses specialized protections to combat these attacks.

**MS-RPC**

IPS contains a variety of protections which prevent attacks that use the MS-RPC protocol. This group of protections primarily checks that the MS-RPC packets meet the protocols standards, but also prevents the use of MS-RPC operations that can be used to gain access to internal information.

The MS-RPC protection group also protects against improper use of DCOM.

- **Note** - By default, DCOM is blocked. To allow DCOM traffic, navigate to the **DCOM - General Settings** protection and select the **Allow DCE-RPC interfaces other than End-Point Mapper (such as DCOM) on Port 135** checkbox.

Additionally, IPS includes protections specifically for MS-RPC over CIFS which block certain functions of MS-RPC interfaces that may be misused.

**Configuring Web Intelligence**

Web Intelligence focuses on protecting Web servers and Web clients against attacks. After you define a gateway or host object as a Web server/client object, Web Intelligence protections are applied to all Web traffic unless you configure the protection to inspect connections with specific Web servers.

Web Intelligence not only protects against a range of known attacks, but also incorporates intelligent security technologies that protect against entire categories of emerging or unknown attacks. Unlike Web firewalls and traditional intrusion protection systems, Web Intelligence provides proactive attack protections. This ensures that communication between clients and Web servers complies with published standards and security best practices, restricts hackers from executing irrelevant system commands, and inspects traffic passing to Web servers to ensure that it does not contain malicious code. Web Intelligence allows organizations to permit access to their Web servers and applications without sacrificing either security or performance.

Web Intelligence uses the **Check Point Stateful Inspection** technology. Stateful Inspection analyzes the information flow into and out of a network so that real-time security decisions are based on communication session information as well as on application information. It accomplishes this by tracking the state and context of all communications traversing the firewall gateway, even when the connection involves complex protocols.

**Configuring Web Intelligence Protections**

**Malicious Code**

Malicious Code Protector is a Check Point patent-pending technology that blocks hackers from sending malicious code to target Web servers and applications. It can detect malicious executable code within Web communications by identifying not only the existence of executable code in a data stream but its potential for malicious behavior. Malicious Code Protector is a kernel-based protection delivering almost wire-speed performance.

These protections prevent attacks that attempt to run malicious code on Web servers.
Defining HTTP Worm Patterns

IPS uses pattern matching to recognize worms and to block them. You can add or edit the pattern lists. These definitions apply to all profiles.

**To define patterns to be blocked:**
1. In the IPS tab, open **Protection > By Protocol > Web Intelligence > Malicious Code > General HTTP Worm Catcher**.
2. In the **Block HTTP Worms** list, leave the checkboxes of the worms that you want to block as selected.
3. At the top of the page, click **Edit**.
4. Click **Add** to add a new worm pattern, or select an existing worm name and click **Edit**.
5. Provide a name for the known worm pattern.
6. Provide the pattern string, or click **Paste from clipboard**, if the string has been copied to the clipboard. See Regular Expressions (on page 84) for pattern syntax.
7. Click **Recalculate** to get the real Checksum.
8. Click **OK**.
   The Block HTTP Worms list is updated immediately.

Malicious Code: Connectivity Versus Security

The Malicious Code Protector protection has security level settings. If a connectivity problem arises on a specific Web server, the security level can be lowered for that Web server.

**To configure connectivity-security levels for Malicious Code Protector:**
1. In the IPS tab, open **Malicious Code Protector** and scroll down to the **Malicious Code Protection Configuration** area.
2. Click **Configure**.
3. Choose a preference between **Memory Consumption and Speed**.
4. Choose a preference between security and performance, in the **Search Method** options.
5. Click **OK**.

Application Layer

This class of protection prevents hackers from introducing text, tags, commands, or other characters that a Web application will interpret as special instructions.

Introducing such objects into forms or URLs can allow a hacker to steal private data, redirect a communication session to a malicious website, steal information from a database, gain unauthorized access, or execute restricted commands.

Defining Commands and Distinguished Names

The **Web Intelligence > Application Layer** category includes the **Cross-Site Scripting**, **LDAP Injection**, **SQL Injection**, and **Command Injection** protections. These protections have lists of commands or Distinguished Names for IPS to recognize.

Define commands or DNs to:
- Allow a command (exclude it from inspection and blocking) for a profile: select a profile, scroll down to the list of commands, and clear the command checkbox.
- Add a command to the blocked list (inclusive to all profiles).
- Edit a blocked command (inclusive to all profiles).

**To edit a blocked command/DN list:**
1. In the IPS tab, open a protection in **Protection > By Protocol > Web Intelligence > Application Layer**, such as:
   - **Cross-Site Scripting**
   - **LDAP Injection**
   - **SQL Injection**
Configuring Specific Protections

- Command Injection
  2. Click **Edit** (in the upper part of the page).
  3. Do one of the following:
     - To add a new command or DN, click **Add**. A new item in the list is created. Provide the command or DN that you want to add and then click **OK**.
     - To change an existing command or DN, select the command and click **Edit**. Change the command or DN as needed and then click **OK**.
  The block list is updated immediately.

Information Disclosure

Application Intelligence is a set of technologies that detect and prevent application-level attacks by integrating a deeper understanding of application behavior into network security defenses.

These protections prevent an attacker from gathering information about a website. The goal of information disclosure is to obtain information from the Web server that can be used to tailor an attack.

HTTP Protocol Inspection

HTTP Protocol Inspection provides strict enforcement of the HTTP protocol, ensuring that sessions comply with RFC standards and common security practices.

**Improving Security for Specific HTTP Formats**

If you can configure HTTP Format Sizes for specific traffic, IPS will be able to apply best-practice security and inspection, without adversely affecting connectivity.

**To set specific header lengths:**

2. In the Specific Headers Lengths area, click **Add**.
3. Provide the actual name of the header that IPS is to recognize.
4. Provide the maximum length of the header.
5. Click **OK**.

Customizable Error Page

Many Web Intelligence protections allow the administrator to define an error page that can be sent back to the user whose browsing was blocked. This page can be used (in conjunction with SmartView Tracker) to pinpoint the reason that caused the connection to be closed. Also, if users see the Customized Error Page, they can call Help Desk and offer real help in protecting their environment.

Although many Web Intelligence protections have an option to configure an Error Page, any configuration changes are applied to all protections: configure an Error Page that applies to all Web Intelligence protections.

**To configure a Web Error Page:**

1. Open an activated Web Intelligence protection with the **Send error page** option in the Action area.
2. Select the **Send error page** checkbox.
3. Click **OK** to continue.
4. Click **Configure**.
5. Decide whether to configure an Error Page here or redirect to a URL that shows an error page:
   - **Send a pre-defined HTML error page**: sends the page that you configure here. You can have the page show your company logo, error code, Reject ID (detailed status code), and any text you choose (Description). Click **Page Preview** to see how the page will appear in client browsers.
   - **Redirect to other URL**: sends the browser to the URL that you configure here. If you select the **Send error code** checkbox, the reject ID and error code are sent to the client browser as parameters in the redirect response to the new location.
6. Click **OK**.
Reject ID

The Reject ID that appears on the error page, or is sent after a redirect, delivers information to the administrator without exposing it to a potential attacker.

The Reject ID is unique for each rejected connection. The Reject ID also appears in the SmartView Tracker and allows the administrator to correlate between an error and a log record of a specific connection. The log record contains attack information, such as "Cross site scripting detected".

Note - Sometimes an Error Description ID may also be sent. It is used to identify attacks detected by specific protections. It appears in the SmartView Tracker log and corresponds to a SecureKnowledge solution about the attack: a SecureKnowledge search for the ID will give you information about the attack.

Connectivity/Performance Versus Security

Web Intelligence can be tuned for greater Web server security at the expense of connectivity and performance, or vice versa.

Improving Connectivity by Setting Scope

Some inspection settings that are too severe can affect connectivity to and from valid Web servers.

- The **HTTP Format sizes** protection restricts URL lengths, header lengths or the number of headers. This is good practice because these elements can be used to perform a Denial of Service attack on a Web server.

- The **ASCII Only Request** protection can block connectivity to Web pages that have non-ASCII characters in URLs. This is good practice because non-ASCII headers or form fields open vulnerabilities to certain attacks, such as Code Injection.

- The **HTTP Methods** protection can block certain HTTP methods, known to be unsafe, because they can be used to exploit vulnerabilities on a Web server.

Although applying these restrictions (activating these protections) is in general good practice, they may potentially block valid sites or important applications. Applying these protections to specific Web servers can solve the connectivity problems, and may enhance CPU performance. This exclusion of a Web server from a particular protection is global to all profiles.

To configure Web Protection scope:

1. Scroll down on a Web Intelligence protection page, to see the Protection Scope area.
2. To apply this protection to a defined set of Web servers, rather than to all of them, select Apply to selected web servers.
3. Click Customize.
   - To exclude a Web server from the protection, clear its checkbox.
   - To add a gateway object to the list of Web servers, click Add. From the Set Hosts as Web Servers window, select the hosts that you want and click OK.
4. To edit a Web server, select the Web server in the list and click Edit.

The Check Point Host window opens, displaying the Web Server category, which is added to a host that is defined as a Web server.

You can configure connectivity-security balance for each type of Web Intelligence protection in the Web Server -> Protections window, but enforcement of these configurations always depends on whether they are activated by the Web server's IPS profile.

Protections Implemented in Kernel Versus Security Server

Web Intelligence features are implemented in the kernel Inspection Module, providing a significant higher performance than inspection in Security Servers.
The Check Point Security Gateway provides a number of Web security capabilities that do not require the Web Intelligence feature. These capabilities make use of the HTTP Security server. The performance provided by the HTTP Security server is not as high as that provided by the kernel. These capabilities are available by defining a URI Resource and using it the Firewall Rule Base.

**Adjusting Allowed Concurrent HTTP Connections**

You can adjust the resources available for HTTP connections to the gateway. If the traffic volume is greater than 1000 concurrent connections, you can increase the allowed maximum number of concurrent HTTP connections. Conversely, if there is a problem installing the security policy due to a lack of memory, you can decrease the allowed maximum number of concurrent connections.

**To configure number of allowed concurrent HTTP connections:**
1. From the SmartDashboard main menu, click *Policy > Global Properties*.
2. Click the *SmartDashboard Customization* category.
3. Click *Configure*.
4. Open the *FireWall-1 > Web Security > Tuning* category.
5. Adjust the value of the *http_max_concurrent_connections* parameter. The default value is 1000.

**Managing Application Controls**

IPS provides administrators with the ability to track the installation and usage of specified applications, and to choose to block these applications.

For example, you can choose to block Peer-to-Peer applications, such as Kazaa and Gnutella. You can choose to configure the block as an automated event, or to receive notification whenever a client attempts to use an unauthorized application.

To see the applications that are supported by IPS, in the IPS tree select *Protections > By Type > Application Control*.

From this view, if you are familiar with the applications you want to control, you can select the protection in the table and then click *Protection Actions > Prevent on all Profiles, Detect on all Profiles, or Deactivate on all Profiles* as needed.

To see the description and further information on each application, technical details on how IPS controls it, or why it may be a threat, click *View > Show Description*. The description of each protection is displayed in the bottom pane as you browse through the displayed list.

A number of the Application Control protections have further options, providing more detailed control. To see these options of a selected protection, click *Protection Actions > See Details*. Then, select a profile and click *Edit*. The settings are applied to the selected profile only.

**Configuring Geo Protections**

Geo Protection allows you to control traffic by country. You can define a policy to block or allow traffic to or from specific countries, and a policy that applies to all other countries.

- **Note** - If Geo Protection is set to block traffic to a country and Mobile Access is set to allow an application or site in that country, the traffic will be allowed.

Country information is derived from IP addresses in the packet by means of an IP-to-country database. Private IP addresses are always allowed unless the other side of the connection is explicitly blocked. Check Point control connections (such as between Security Gateways and the Security Management Server) are always allowed, regardless of the Geo Protection policy.

To operate Geo Protection, you are required to have:

- A valid IPS contract.
- A Software Blade license for each Security Gateway that enforces Geo Protection, and for the Security Management Server.
## Configuring Traffic by Country

You can define a policy to block or allow traffic to or from specific countries, and a policy that applies to all other countries.

### Before configuring Geo Protection:

Confirm that you have:

- A valid IPS contract.
- A Software Blade license for each Security Gateway that enforces Geo Protection, and for the Security Management Server.

Note - This protection is enforced only by Gateways of version R70.20 and above.

### To block, allow or monitor traffic by country:

1. In the SmartDashboard IPS tab, select Geo Protection from the navigation tree.
2. In the Geo Protection page, choose an IPS Profile.

Note - Geo Protection settings are per-profile. You must configure this protection on the profile used by the Gateways.

3. Set the Action for this protection: Prevent or Detect or Inactive. When protection is in Detect mode, all traffic is allowed (even for rules where the Action is set to Block), but traffic that matches the rules is logged. Use Detect to try out the protection, or for troubleshooting. When the protection is in Prevent mode, the rules are applied as configured.

4. Define a Policy for Specific Countries. To configure a policy for a specific country that is different than the Policy for Other Countries:

   a) Click Add.

   The Geo Protection window opens.

   b) In the Geo Protection window, select a Country. To quickly find the country, start typing the name in the search box.

   c) Choose:

   - **Direction**: Either From Country to the Gateway, or To Country from the Gateway, or From and to Country. If From Country or To Country is selected, connections in the other direction are handled according to the Policy for Other Countries.

   - **Action**: Either Allow or Block.

   - **Track**: Any setting other than None generates a log for every connection that is tracked by this protection. If a connection matches two rules, the first rule is logged.

   d) Click OK.

5. Configure a Policy for Other Countries. These settings apply to all countries and IP addresses that are not included in the Policy for Specific Countries. Configure whether to Allow or Block, and a Track setting.

6. If necessary define Exceptions (see "Configuring Network Exceptions" on page 56). Exceptions are applied before any other defined rule.

### After you have configured the protection:

1. Examine the Policy Preview map. Red countries are blocked and green countries are allowed.
2. Let the protection operate for a while and then review the logs.

### To view Geo Protection logs:

In the Geo Protection page of IPS, click View Logs. The logs are for both the Policy for Specific Countries and for the Policy for Other Countries.

## The IP Address to Country Database

Country information is derived from IP addresses in the packet by means of an IP-to-country database. To ensure that the information in the IP-to-country database is up-to-date, the database is regularly and automatically downloaded to the Security Gateway from a Check Point data center.
**Configuring Specific Protections**

**Note** - To ensure that the most recent IP-to-country database is being used, the Security Gateway must be connected to the Internet. If the Gateway cannot access the Internet the database may not be completely accurate.

If the Security Gateway needs to access the Internet via a proxy, you need to define the proxy in SmartDashboard.

**To define a proxy for the Security Gateway:**
1. In SmartDashboard, Edit the Security Gateway.
2. Select the **Topology > Proxy** page.
3. Configure the required settings.

**Log Aggregation by Country**

Geo Protection logs are aggregated by default. This means that a single log is generated every aggregation interval, for every country that is part of the Policy for Specific Countries. Logs that relate to other countries are aggregated to a single log.

It is possible to turn off log aggregation by country. In that case, a log is created for every connection that is tracked by this protection. Turning off log aggregation by country may result in a significant increase in the number of generated logs, and in increased CPU utilization on the Security Gateway.

**To configure log aggregation by country:**
1. In the SmartDashboard **IPS** tab, select **Geo Protection** from the navigation tree.
2. In the **Geo Protection** page, choose an **IPS Profile**.

   **Note** - Geo Protection settings are per-profile. You must configure this protection on the profile used by the Gateways.

3. Click **Advanced**.
   The Advanced Geo Protection Enforcement window opens. **Aggregate logs by country** is selected by default.
4. To turn off log aggregation, deselect **Aggregate logs by country**.

**Configuring IPS Pattern Granularity**

After the first update of IPS protections, all patterns of Header rejection, Http worm catcher, and Cifs worm catcher protections are converted into new protections (dated to January 1, 2007). The three protections and the patterns under them are kept for NGX R65 and user-defined pattern support.

**Activating New Protections**

The activation mode of the new protections is set according to the IPS policy of the associated profile (the Severity and Confidence levels). You can change the settings as for other IPS protections. For example, you can change the action from Detect to Prevent.

Only the settings of patterns that were manually modified before upgrade are assigned to their converted protections. Those protections are marked as **Override** and do not get updates.

You cannot change the signature of the new protections. After upgrade, the previous patterns under the three protections are enforced only on NGX R65 gateways. The user-defined patterns are enforced on all gateways, including R7x and above, because they are not converted to protections.

**Network Exceptions for the New Protections**

If you added Network Exceptions to the Header rejection, Http worm catcher, or Cifs worm catcher protections before upgrade to R75.40, then after the upgrade, they are valid only for user-defined patterns.
To apply the Network Exceptions to a pattern, add them to the new protection converted from the relevant pattern.

**Handling Multiple Matches of a Pattern**

If you changed the value of a pattern before upgrade, the pattern shows under the previous pattern list (Header rejection, Http worm catcher, Cifs worm catcher), as user-defined patterns. The pattern is also included as a new protection, marked for Follow Up. Sometimes, this causes multiple matches. To avoid this, turn off the modified patterns, or turn off the new protections.

**Configuring Implied IPS Exceptions**

Check Point components can use non-standard HTTP and SSL ports to communicate. Implied exceptions exclude this traffic from IPS inspection.

- **Note** - To use implied exceptions in Provider-1 you must activate the R71.40 plug-in for the customer.

To view the implied exceptions:

- In the View menu, select IPS Implied Exceptions.
  
  You can see the implied exceptions in the Network Exceptions page of the IPS tab.

We do not recommend that you disable the implied exceptions. But, you can disable them from the IPS page of the Global Properties (Policy > Global Properties > IPS). To disable the implied exceptions, clear the Enable implied exceptions in my environment option.

- **Note** - If you disable the implied exceptions and you do not add exceptions for the non-standard HTTP and SSL traffic manually, it is possible that some Check Point products will not work.
Chapter 6

Monitoring Traffic

In This Chapter

Monitoring Events using SmartView Tracker  
Working with Packet Information  
Allowing Traffic using Network Exceptions  
Tracking Protections using Follow Up  
HTTP Inspection on Non-Standard Ports  
HTTPS Inspection

Monitoring Events using SmartView Tracker

After initial configuration of IPS, monitor traffic with SmartView Tracker. The information you gain here will help you understand how to change the IPS configuration for optimal security and connectivity.

SmartView Tracker offers a number of queries that can help you focus on the events that most interest you.

- **Most Important** - events for protections with Severity values of High or Critical and Confidence Level values of Medium-high or High. These events typically require the most attention.
- **Critical Not Prevented** - events for protections with a Severity value of Critical but are set to Detect.
- **All** - all IPS events.
- **Protocol Anomaly** - events for Protocol Anomaly protections.
- **Follow Up** - events for protections marked for Follow Up.
- **Application Control** - events for Application Control protections.

**Viewing IPS Events**

To view the logs that result from IPS activity:

1. In SmartDashboard, select Window > SmartView Tracker.
3. Double-click All.

   The events log displays all events that were generated by the IPS Blade, including information about the data, the protection and the action taken.
**Viewing IPS Event Details**

To view details about the event:

- In a records list in SmartView Tracker, double-click on the event that you want more information about.

  The **Record Details** window opens.

---

**Opening Protection Settings**

To open the protection from a SmartView Tracker log item:

- Right-click on the event and select **Open Protection**.
Monitoring Traffic

SmartDashboard opens to the specific protection in the IPS tab.

Working with Packet Information

If you are familiar with network protocols, you can view packets that were tracked by IPS using an internal viewer or a third-party packet capture application. This can help you understand the nature of the attack.

Capturing a Packet for Every Log

To capture packet data for a protection for every malicious packet that is logged, turn on the packet capture option in that protection. This attaches a packet capture to every log generated by the protection.

Automatic Packet Capture in the First Log

Captured malicious traffic is automatically attached to the first log generated by a protection since policy installation, even if the packet capture option in the protection is not turned on. This is economical with system resources because only one packet capture is saved for each attack.

Attaching a Packet Capture to Every Log

A packet capture is automatically attached to the first log generated by a protection. However, if you want to capture packet data for a protection for every malicious packet that is logged, turn on the packet capture option in that protection.

To attach a packet capture to every log
1. Open the protection for which you want to track the packet data.
2. Make sure the protection is activated (either Detect or Prevent).
3. Double-click on the profile for which you want packet capture data.
4. In the Action area, select any tracking action other than None and then select Capture Packets.

Viewing Packet Capture Data in SmartView Tracker

A packet capture is automatically attached to the first packet logged by a protection since policy installation. If packet capture is turned on for a protection, a packet capture is attached to every log generated by the protection.
To view packet captures in SmartView Tracker
1. From the protection page that has **Capture Packets** selected, click **View Logs**.
   SmartView Tracker opens. Wait until the log window for the specific protection opens.
   
   **Note** - SmartView Tracker displays the current log file. If you have performed a log switch and the capture is in a different file, open that log file instead.

2. If searching for automatically captured packets, make sure the **Packet Capture** column is showing.
3. Locate the item
4. Right-click the item in the protection's SmartView Tracker log and select **View packet capture**.

5. Select **Internal Viewer** and click **OK**.
   You may also use a third-party packet capture application by selecting **Choose program** and specifying the application in the **Program Name** field.

### Allowing Traffic using Network Exceptions

**Note** - Network Exceptions are only supported on R70 gateways and above.
Viewing Network Exceptions

You can configure exceptions for a protection in order to prevent certain traffic from being identified by that specific protection. This may be useful when traffic that is legitimate for some machines or services meets the criteria set in the protection as being an attack, or when using a server that does not comply with RFC standards.

In IPS, right-click an IPS item and select Exception. The Network Exceptions window appears, displaying the exceptions that apply to that specific protection.

Configuring Network Exceptions

You can configure exact, particularized exceptions to an IPS protection on a profile or for all gateways of a similar version. This can be done from one of the following locations in SmartDashboard:

- Network Exceptions - the exception can be specified for any protection, gateway, and/or traffic definition.
- Protection - the exception can be specified for this protection, but can be applied to any gateway and/or traffic definition.
- SmartView Tracker - by right-clicking a log entry, a network exception can be made to apply to this specific traffic definition, but can be applied to any protection and/or gateway.

For example, let’s assume you have created a number of profiles and activated the relevant protections. Afterwards, you decide that a specific gateway should allow instant messaging. The profile of this gateway blocks instant messaging, and other gateways have the same profile. You can make an exception for the one gateway without creating another profile or changing your requirements.

To configure an exception:
1. Open the Network Exceptions page.
2. Click New.
   The Add/Edit Exception Rule window opens.
3. From the Profile drop-down list, select an existing profile to which this exception will be added, or select Any, to apply the network exception to all profiles.
4. In the Scope area, select the protection that will be affected by this exception:
   - All supported protections: IPS will exclude traffic from inspection based on source, destination, or service; this effectively turns off IPS inspection for the traffic that matches the exceptions. Protections that do not support the Network Exceptions feature will not be affected.
   - Single enforcement: Click Select and select a protection. This selected protection will not inspect traffic that matches the exceptions, even if it is activated in the profile.
5. Define the Source and Destination:
   Select Network Object and then click Manage; or select IP Address and provide the IP Address in the field.
   - **Source:** Provide the SmartDashboard Network Object that represents the source for the exception. The selected protection will not be inspected if the traffic comes from this source. For example, you could provide the static IP Address of the CEO's laptop, ensuring that anything coming from this laptop is allowed.
   - **Destination:** Provide the SmartDashboard Network Object that represents the destination for the exception. The selected protection will not be inspected if the traffic is going to this destination. For example, you could provide the DMZ network object as the destination, allowing all traffic to reach the outer walls of your network.
   If you want to make the exception applicable to all machines, basing it on a service or protection rather than source or destination, select Any.

6. Define the Service:
   - Leave Any selected if this exception is to be applicable to all services on provided Source or Destination.
   - Click Manage and select a service to allow traffic of this service to be passed without exception.

7. Select the gateways on which this exception is to be installed:
   - **Apply this exception on all R70 gateways (and above):** The exception will be applied to all matching gateways.
   - **Apply this exception on:** From the drop-down list of gateways of version R70 and above, select a single gateway.

8. Add a comment for management and click OK.

**Tip:** When creating a Network Exception, you define a rule that includes Source, Destination, and Service. If you set all three of these parameters to Any, you are essentially deactivating the protection. If this is what you want, you should not create the Network Exception; you should deactivate the protection from its page. When the protection is set to Inactive from its page, it is easy to see its action mode, to understand why its traffic is not blocked, and to change the action if needed. If a protection is deactivated by a Network Exception, it may appear to be activated while not actually protecting your environment.

### Tracking Protections using Follow Up

The Follow Up mark provides monitoring features for IPS protections: one-stop page for protections to monitor, quick view of protection parameters, and easy access to newly updated protections.

**To view protections marked for Follow Up:**
- Select Follow Up in the IPS tree.


Marking Protections for Follow Up

Marking Protections from Follow Up Page

You can mark individual protections for Follow Up, allowing you to quickly review the identified protections in the Follow Up screen. The date and time when the protection was marked for Follow Up is added to the Follow Up Comment field, but you can also edit the field to add any other significant information.

To mark more protections from the Follow Up page:
1. In the Follow Up page, click Mark.

   - The Select Protection window opens. Here you may select a single protection; you cannot select categories or settings.

   - Select the protection you want to mark for Follow Up.

   - Click OK.
The Follow Up Comment window opens.

4. Edit the comment, if you want. By default, it shows that the protection was marked for Follow Up (manually) on the current date and time.

5. Click OK.

**Marking Protections from Protection Details**

As you access protection pages, you can mark a protection for Follow Up. This will ensure that the protection is listed in the Follow Up page; and for profiles that are configured to set marked protections to Detect, the protection will be in Detect mode while you monitor its effects.

**To mark a protection for Follow Up from the protection details:**

1. In the protection details, click Follow Up.
2. In the menu that appears, click Mark for Follow Up.
   
   The Follow Up Comment window opens.

3. Edit the comment, if you want. By default, it shows that the protection was marked for Follow Up (manually) on the current date and time.

4. Click OK.

**Automatically Marking New Protections for Follow Up**

Check Point provides new and updated protections as they become available (see Updating Protections). To give you complete control over the process of integrating new IPS protections, you can have them automatically marked for Follow Up and set to Detect, giving you time to evaluate the impact the protections will have on your environment.

**To have new protections automatically marked:**

- In the Follow Up page, select the Mark newly downloaded protections for Follow Up checkbox.

**Unmarking Protections for Follow Up**

To make the Follow Up feature efficient, make sure to keep the list of marked protections as short as possible. Do mark newly downloaded protections and any protection that you want to monitor; but remember to remove protections from this list when you are more confident that you have configured them in the best way for your environment, for now. The longer the Follow Up list is, the more difficult it will be to use it as a workable task list.
Unmarking Protections from Follow Up Page

To unmark individual protections from the Follow Up page:
1. In the Follow Up page, select a protection and click Unmark.
   A message appears:
   This action will remove the Follow Up state from <protection>. Are you sure?
2. Click Yes.

To unmark all protections:
1. In the Follow Up page, click View > Unmark All.
2. In the confirmation dialog box that opens, click Yes.
   All protections are unmarked; the Follow Up list is empty.

Unmarking Protections from Protection Details

The following are the functions that can be performed from the Protection Details window:

- Click the Unmark link to unmark a protection and remove it from the Follow Up list.
- Click the Undo link to change back to being marked.
- Click the Hide link to remove the "Follow Up Removed" banner.

HTTP Inspection on Non-Standard Ports

Applications that use HTTP normally send the HTTP traffic on TCP port 80. Some applications send HTTP traffic on other ports also. You can configure some Software Blades to only inspect HTTP traffic on port 80, or to also inspect HTTP traffic on non-standard ports.

When selected, IPS inspects all HTTP traffic, even if it is sent using non-standard ports. This option is cleared by default. You can configure this option in the Advanced section of the IPS tab.

HTTPS Inspection

You can enable HTTPS traffic inspection on Security Gateways to inspect traffic that is encrypted by the Secure Sockets Layer (SSL) protocol. SSL secures communication between internet browser clients and web servers. It supplies data privacy and integrity by encrypting the traffic, based on standard encryption ciphers.

However, SSL has a potential security gap. It can hide illegal user activity and malicious traffic from the content inspection of Security Gateways. One example of a threat is when an employee uses HTTPS (SSL based) to connect from the corporate network to internet web servers. Security Gateways without HTTPS Inspection are unaware of the content passed through the SSL encrypted tunnel. This makes the company vulnerable to security attacks and sensitive data leakage.

The SSL protocol is widely implemented in public resources that include: banking, web mail, user forums, and corporate web resources.

There are two types of HTTPS inspection:
- **Inbound HTTPS inspection** - To protect internal servers from malicious requests originating from the internet or an external network.
- **Outbound HTTPS inspection** - To protect an organization from malicious traffic being sent by an internal client to a destination outside of the organization.
The Security Gateway acts as an intermediary between the client computer and the secure web site. The Security Gateway behaves as the client with the server and as the server with the client using certificates.

All data is kept private in HTTPS Inspection logs. This is controlled by administrator permissions. Only administrators with HTTPS Inspection permissions can see all the fields in a log. Without these permissions, some data is hidden.

**How it Operates**

In outbound HTTPS inspection, when a client in the organization initiates an HTTPS connection to a secure site, the Security Gateway:

1. Intercepts the request.
2. Establishes a secure connection to the requested web site and validates the site's server certificate.
3. Creates a new SSL certificate for the communication between the Security Gateway and the client, sends the client the new certificate and continues the SSL negotiation with it.
4. Using the two SSL connections:
   a) It decrypts the encrypted data from the client.
   b) Inspects the clear text content for all blades set in the policy.
   c) Encrypts the data again to keep client privacy as the data travels to the destination web server resource.

In inbound HTTPS inspection, when a client outside of the organization initiates an HTTPS connection to a server behind the organization's gateway, the Security Gateway:

1. Intercepts the request.
2. Uses the server's original certificate and private key to initiate an SSL connection with the client.
3. Creates and establishes a new SSL connection with the web server.
4. Using the two SSL connections:
   a) It decrypts the encrypted data from the client.
   b) Inspects the clear text content for all blades set in the policy.
   c) Encrypts the data again to keep client privacy as the data travels to the destination server behind the gateway.

**Configuring Outbound HTTPS Inspection**

To enable outbound HTTPS traffic inspection, you must do these steps:

- Set the Security Gateway for HTTPS Inspection.
- Generate a CA certificate on the Security Management Server or import a CA certificate already deployed in your organization.
  - If you created a CA certificate, you must deploy it in the Trusted Root Certification Authorities Certificate Store on the client computers. This lets the client computers trust all certificates signed by this certificate.
- Generate an HTTPS inspection policy by defining relevant rules in the HTTPS inspection Rule Base.
- Configure the conditions for dropping traffic from a web site server.

When required, you can update the trusted CA list in the Security Gateway.

**Enabling HTTPS Inspection**

You must enable HTTPS inspection on each gateway. From Security Gateway > HTTPS Inspection > Step 3 > Select Enable HTTPS Inspection.

The first time you enable HTTPS inspection on one of the 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 gateways managed on the Security 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 gateways use this password to sign certificates for the sites accessed. You must keep the password as it also used by other Security 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 ("Troubleshooting" on page 71).

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

To create an outbound CA certificate:

1. In SmartDashboard, right-click the gateway object and select Edit. The Gateway Properties window opens.
2. In the navigation tree, select HTTPS Inspection.
3. In the HTTPS Inspection page, click Create.
4. Enter the necessary information:
   - Issued by (DN) - Enter the domain name of your organization.
   - Private key password - Enter the password that is used to encrypt the private key of the CA certificate.
   - Retype private key password - Retype the password.
   - Valid from - Select the date range for which the CA certificate is valid.
5. Click OK.
6. Export and deploy the CA certificate ("Exporting and Deploying the Generated CA" on page 63).

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 Security Management Server to use on another Security Management Server.

Important - If you are importing a CA certificate created on another Security Management Server, make sure the initial certificate was exported ("Exporting a Certificate from the Security Management Server" on page 63) from the Security Management Server on which it was created.

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

- Import the CA certificate.
- Enter the password the Security 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 Security Management Server.

Important - After you import a certificate from another Security Management Server, make sure to export the certificate and deploy it ("Exporting and Deploying the Generated CA" on page 63) on the client machines if it has not already been deployed.

To import a CA certificate:

1. In SmartDashboard, right-click a gateway object, select Edit > HTTPS Inspection > Import
   Or
   From the HTTPS Inspection > Gateways pane of a supported blade, click the arrow next to Create Certificate and select Import certificate from file.
   The Import Outbound Certificate window opens.
2. Browse to the certificate file.
3. Enter the private key password.
4. Click OK.
Exporting a Certificate from the Security Management Server

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

Usage:

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

To export the CA certificate:

- On the Security Management Server, run:
  
  ```
  /$FWDIR/bin/export_https_cert 
  -local 
  -f [certificate file name under FWDIR/tmp]
  ```
  
  For 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 machines.

When users do 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
   
   Or
   
   From the HTTPS Inspection > Gateways pane in a supported blade, click Export.

2. Save the CA certificate file.

3. Use the Group Policy Management Console ("Deploying Certificates by Using Group Policy" on page 63) to add the certificate to the Trusted Root Certification Authorities certificate store.

4. Push the policy to the client machines in the organization.

   **Note** - Make sure that the CA certificate is pushed to the client machines' 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. 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 SmartDashboard.

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, you must do these steps:

- Set the Security Gateway for HTTPS Inspection (if it is not already configured). From Security Gateway > HTTPS Inspection > Step 3 > Select Enable HTTPS Inspection.

- Import server certificates for servers behind the organizational gateways ("Server Certificates" on page 64).

- Generate an HTTPS inspection policy by defining relevant rules in the HTTPS inspection Rule Base ("The HTTPS Inspection Policy" on page 65).

- Make sure to configure the relevant server certificate in the HTTPS inspection Rule Base ("Certificate" on page 68).

Server Certificates

When a client from outside the organization initiates an HTTPS connection to an internal server, the Security Gateway intercepts the connection. 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.

For inbound HTTPS inspection, do these steps:

- Add the server certificates to the Security Gateway - This creates a server certificate object ("Adding a Server Certificate" on page 64).

- Add the server certificate object to the Certificate column in the HTTPS Inspection Policy to enforce it in rules ("Certificate" on page 68).

The Server Certificates window in SmartDashboard includes 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 SmartDashboard, 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.
The HTTPS Inspection Policy

The HTTPS inspection policy determines which traffic is inspected. The primary component of the policy is the Rule Base. The rules use the categories defined in the Application Database, network objects and custom objects (if defined).

The HTTPS Rule Base lets you inspect the traffic on other network blades. The blades that HTTPS can operate on are based on the blade contracts and licenses in your organization and can include:

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

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

To access the HTTPS inspection Rule Base:

- In SmartDashboard, open the Policy page from the specified blade tab:
  - For Application and URL Filtering, Anti-Bot, Anti-Virus, and IPS - Select Advanced > HTTPS Inspection > Policy.
  - For DLP - Select Additional Settings > HTTPS Inspection > Policy.

Predefined Rule

When you enable HTTPS inspection, a predefined rule is added to the HTTPS Rule Base. This rule defines that all HTTPS and HTTPS proxy traffic from any source to the internet is inspected on all blades enabled in the Blade column. By default, there are no logs.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Site Category</th>
<th>Action</th>
<th>Track</th>
<th>Blade</th>
<th>Install On</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predefined Rule</td>
<td>Any</td>
<td>Internet</td>
<td>HTTPS</td>
<td>Any</td>
<td>Inspect</td>
<td>-</td>
<td>All</td>
<td>All</td>
<td>Outbound Certificate</td>
</tr>
</tbody>
</table>

Parts of the Rule

The columns of a rule define the traffic that it matches and if that traffic is inspected or bypassed. When traffic is bypassed or if there is no rule match, the traffic continues to be examined by other blades in the gateway.

**Number (No.)**

The sequence of rules is important because the first rule that matches is applied.

For example, if the predefined rule inspects all HTTPS traffic from any category and the next rule bypasses traffic from a specified category, the first rule that inspects the traffic is applied.

**Name**

Give the rule a descriptive name. The name can include spaces.

Double-click in the Name column of the rule to add or change a name.

**Source**

The source is where the traffic originates. The default is Any.

⚠️ **Important** - A rule that blocks traffic, with the Source and Destination parameters defined as Any, also blocks traffic to and from the Captive Portal.
Put your mouse in the column and a plus sign shows. Click the plus sign to open the list of network objects and select one or multiple sources. The source can be an Access Role object, which you can define when Identity Awareness is enabled.

**Destination**

Choose the destination for the traffic. The default is the Internet, which includes all traffic with the destination of DMZ or external. If you delete the destination value, the rule changes to Any, which applies to traffic going to all destinations.

**Important** - A rule that blocks traffic, with the Source and Destination parameters defined as Any, also blocks traffic to and from the Captive Portal.

To choose other destinations, put your mouse in the column and a plus sign shows. Click the plus sign to open the list of network objects and select one or multiple destinations.

**Services**

By default, HTTPS traffic on port 443 and HTTP and HTTPS proxy on port 8080 is inspected. You can include more services and ports in the inspection by adding them to the services list.

To select other HTTPS/HTTP services, put your mouse in the column and a plus sign shows. Click the plus sign to open the list of services and select a service. Other services, such as SSH are not supported.

**Site Category**

The Site Category column contains the categories for sites and applications that users browse to and you choose to include. One rule can include multiple categories of different types.

**Important** - A valid URL Filtering blade contract and license are necessary on the relevant Security Gateways to use the Site Category column.

**Important** - To perform categorization correctly, a single connection to a site must be inspected in some cases regardless of the HTTPS inspection policy. This maps the IP address of a site to the relevant domain name.

You can also include custom applications, sites, and hosts. You can select a custom defined application or site object with the Custom button or create a new host or site with the New button at the bottom of the page.

**Note** - You can only use custom objects that specify the domain name or host part of a URL. URLs that contain paths are not supported. For example, you can use an object defined as ww.gmail.com but not www.gmail.com/myaccount.

**To add site categories to a rule:**

Put your mouse in the column and a plus sign shows. Click the plus sign to open the Category viewer. For each category, the viewer shows a description and if there are applications or sites related with it.

- To filter the Available list by categories or custom-defined sites, click the specified button in the toolbar of the viewer. The Available list opens in the left column and then you can add items to the rule.
- To add a category object to the rule, click the checkbox in the Available list.
- To see the details of category without adding it to the rule, click the name of the item in the Available list.
- You can only select a category to add to the rule from the Available list.
- If a category is already in a rule, it will not show in the Category viewer.
- If you know the name of a category, you can search for it. The results will show in the Available list.
- You can add a new host site with the New button.
Adding a New Host Site

You can create a new host site object to use in the HTTPS Rule Base if there is no corresponding existing category. Only the domain name part or hosts part of the URL is supported.

**To create a new host site:**
1. Click the plus icon in the Site Category column.
2. In the Category viewer, select New.
   The Hosts/Sites window opens.
3. Enter a name for the host site.
4. Set a color for the host site icon (optional).
5. Enter a comment for the host site (optional).
6. In Hosts List, enter a valid URL and click Add.
7. If you used a regular expression in the URL, click Hosts are defined as regular expressions.
8. Click OK.
   The new host site is added to the Selected list and can be added to the Rule Base.

**Action**
The action is what is done to the traffic. Click in the column to see the options and select one to add to the rule.

- **Inspect** - The traffic is inspected on the blades set in the Blades column.
- **Bypass** - The traffic of source and destination traffic in rules that include the bypass action are not decrypted and inspected. You can bypass HTTPS inspection for all Check Point objects. This is recommended for Anti-Bot, Anti-Virus, URL Filtering, and IPS updates. Other HTTPS protections that already operate on traffic will continue to work even when the HTTPS traffic is not decrypted for inspection.

**Track**
Choose if the traffic is logged in SmartView Tracker or if it triggers other notifications. Click in the column and the options open. The options include:

- **None** - Does not record the event
- **Log** - Records the event’s details in SmartView Tracker. This option is useful for obtaining general information on your network’s traffic. There is one or more log for each session depending on the suppression option.
- **Alert** - Logs the event and executes a command, such as display a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in Policy > Global Properties > Log and Alert > Alert Commands
- **Mail** - Sends an email to the administrator, or runs the mail alert script defined in Policy > Global Properties > Log and Alert > Alert Commands
- **SNMP Trap** - Sends a SNMP alert to the SNMP GUI, or runs the script defined in Policy > Global Properties > Log and Alert > Alert Commands
- **User Defined Alert** - Sends one of three possible customized alerts. The alerts are defined by the scripts specified in Policy > Global Properties > Log and Alert > Alert Commands

**Blade**
Choose the blades that will inspect the traffic. Click in the column and the options open. The options include:

- Application Control
- Data Loss Prevention
- IPS
- URL Filtering
- Anti-Virus
- Anti-Bot
Important - The blade options you see are based on the blade contracts and licenses in your organization.

Install On
Choose which gateways the rule will be installed on. The default is All, which means all gateways that have HTTPS inspection enabled. Put your mouse in the column and a plus sign shows. Click the plus sign to open the list of available gateways and select.

Certificate
Choose the certificate that is applicable to the rule. The Security Gateway uses the selected certificate for communication between the Security Gateway and the client.

- For outbound HTTPS inspection - choose the Outbound Certificate object (default) that reflects the CA certificate you created/imported and deployed on the client machines in your organization.
- For inbound HTTP inspection - choose the server certificate applicable to the rule. Put your mouse in the column and a plus sign shows. Click the plus sign to open the list of available server certificates and select one. When there is a match to a rule, the Security Gateway uses the selected server certificate to communicate with the source client. You can create server certificates from HTTPS Inspection > Server Certificates > Add.

Bypassing HTTPS Inspection to Software Update Services
Check Point dynamically updates a list of approved domain names of services from which content is always allowed. This option makes sure that Check Point updates or other 3rd party software updates are not blocked. For example, updates from Microsoft, Java, and Adobe.

To bypass HTTPS inspection to software updates:
1. In the HTTPS Inspection > Policy pane, select Bypass HTTPS Inspection of traffic to well known software update services (list is dynamically updated). This option is selected by default.
2. Click list to see the list of approved domain names.

Gateways Pane
The Gateways pane lists the gateways with HTTPS Inspection enabled. Select a gateway and click Edit to edit the gateway properties. You can also search, add and remove gateways from here.

For each gateway, you see the gateway name, IP address and comments.

In the CA Certificate section, you can renew the certificate's validity date range if necessary and export it for distribution to the organization's client machines.

If the Security Management Server managing the selected gateway does not have a generated CA certificate installed on it, you can add it with Import certificate from file. There are two options:
- You can import a CA certificate already deployed in your organization.
- You can import a CA certificate from another Security Management Server. Before you can import it, you must first export ("Exporting a Certificate from the Security Management Server" on page 63) it from the Security Management Server on which it was created.

Adding Trusted CAs for Outbound HTTPS Inspection
When a client initiates an HTTPS connection to a web site server, the Security Gateway intercepts the connection. The Security Gateway inspects the traffic and creates a new HTTPS connection from the gateway to the designated server.

When the Security Gateway establishes a secure connection (an SSL tunnel) to the designated web site, it must validate the site's server certificate.

HTTPS Inspection comes with a preconfigured list of trusted CAs. This list is updated by Check Point when necessary and is automatically downloaded to the Security Gateway. The system is configured by default to notify you when a Trusted CA update file is ready to be installed. The notification in SmartDashboard shows as a pop-up notification or in the Trusted CAs window in the Automatic Updates section. After you install
the update, make sure to install the policy. You can choose to disable the automatic update option and manually update the Trusted CA list.

If the Security Gateway receives a non-trusted server certificate from a site, by default the user gets a self-signed certificate and not the generated certificate. A page notifies the user that there is a problem with the website's security certificate, but lets the user continue to the website.

You can change the default setting to block untrusted server certificates ("Server Validation" on page 70). The trusted CA list is based on the Microsoft Root Certificate Program (http://technet.microsoft.com/en-us/library/cc751157.aspx).

**Automatically Updating the Trusted CAs List**

Updates for the trusted CA list will be published from time to time on the Check Point web site. They are automatically downloaded to the Security Management Server by default. When you are sent a notification that there is an update available, install it and do the procedure. The first notification is shown in a popup balloon once and then in the notification line under HTTPS Inspection > Trusted CAs. You can disable automatic updates if necessary.

**To update the Trusted CA list:**
1. In SmartDashboard, select HTTPS Inspection > Trusted CAs.
2. In the Automatic Updates section, click Install Now.
   - You see the certificates that will be added or removed to the list and the validity date range of the certificates.
3. Click Proceed to confirm the update.
   - The certificates will be added or removed respectively from the list.
4. Install the policy.

**To disable automatic updates:**
1. In SmartDashboard, select HTTPS Inspection > Trusted CAs.
2. In the Automatic Updates section, clear the Notify when a Trusted CA update file is available for installation checkbox.

**Manually Updating a Trusted CA**

To add a trusted CA manually to the Security Gateway, you must export the necessary certificate from a non-trusted web site and then import it into SmartDashboard.

**To export a CA certificate to add to the Trusted CAs list:**
2. Install the security policy.
3. Browse to the site to get the certificate issued by the CA.
4. Go to the Certification Path of the certificate.
5. Select the root certificate (the top most certificate in the list).
6. In Internet Explorer and Chrome:
   a) Click View Certificate.
   b) From the Details tab, click Copy to File.
   c) Follow the wizard steps.
7. In Firefox, export the certificate.

**To import a CA certificate to the Trusted CAs list:**
1. In SmartDashboard, open HTTPS Inspection > Trusted CAs.
2. Click Actions > Import certificate, browse to the location of the saved certificate and click Open.
   - The certificate is added to the trusted CAs list.
3. Install the security policy on gateways enabled with HTTPS Inspection.
Saving a CA Certificate

You can save a selected certificate in the trusted CAs list to the local file system.

To export a CA certificate:
1. In SmartDashboard, open HTTPS Inspection > Trusted CAs.
2. Click Actions > Export to file.
3. Browse to a location, enter a file name and click Save. A CER file is created.

HTTPS Validation

Server Validation

When a Security Gateway receives an untrusted certificate from a web site server, the settings in this section define when to drop the connection.

- **Untrusted server certificate**
  - When selected, traffic from a site with an untrusted server certificate is immediately dropped. The user gets an error page that states that the browser cannot display the webpage.
  - When cleared, a self-signed certificate shows on the client machine when there is traffic from an untrusted server. The user is notified that there is a problem with the website's security certificate, but lets the user to continue to the website (default).

- **Revoked server certificate (validate CRL)**
  - When selected, the Security Gateway validates that each server site certificate is not in the Certificate Revocation List (CRL) (default).
  - If the CRL cannot be reached, the certificate is considered trusted (this is the default configuration). An HTTPS Inspection log is issued that indicates that the CRL could not be reached. This setting can be changed with GuiDBedit. Select Other > SSL Inspection > general_confs_obj and change the attribute drop_if_crl_cannot_be_reached from false to true.
  - To validate the CRL, the Security Gateway must have access to the internet. For example, if a proxy server is used in the organization's environment, you must configure the proxy for the Security Gateway.
  - To configure the proxy:
    a) From the Firewall tab, double-click the Security Gateway that requires proxy configuration.
    b) Select Topology > Proxy.
    c) Select Use custom proxy settings for this network object and Use proxy server and enter the proxy IP address.
    d) Optionally, you can use the default proxy settings.
    e) Click OK.

    **Important** - Make sure that there is a rule in the Rule Base that allows outgoing HTTP from the Security Gateway.

  - When cleared, the Security Gateway does not check for revocations of server site certificates.

- **Expired server certificate**
  - When selected, the Security Gateway drops the connection if the server certificate has expired.
  - When cleared, the Security Gateway creates a certificate with the expired date. The user can continue to the website (default).

- **Track validation errors**
  - Choose if the server validation traffic is logged in SmartView Tracker or if it triggers other notifications. The options include:
    - **None** - Does not record the event.
    - **Log** - Records the event's details in SmartView Tracker.
Monitoring Traffic

- **Alert** - Logs the event and executes a command, such as shows a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in Policy > Global Properties > Log and Alert > Alert Commands
- **Mail** - Sends an email to the administrator, or runs the mail alert script defined in Policy > Global Properties > Log and Alert > Alert Commands
- **SNMP Trap** - Sends an SNMP alert to the SNMP GUI, or runs the script defined in Policy > Global Properties > Log and Alert > Alert Commands
- **User Defined Alert** - Sends one of three possible customized alerts. The alerts are defined by the scripts specified in Policy > Global Properties > Log and Alert > Alert Commands

Automatically retrieve intermediate CA certificates

- When selected, intermediate CA certificates issued by trusted root CA certificates that are not part of the certificate chain are automatically retrieved using the information on the certificate (default).
- When cleared, a web server certificate signed by an intermediate CA certificate which is not sent as part of the certificate chain, will be considered untrusted.

Certificate Blacklisting

You can create a list of certificates that are blocked. Traffic from servers using the certificates in the blacklist will be dropped. If a certificate in the blacklist is also in the Trusted CAs list, the blacklist setting overrides the Trusted CAs list.

- **Add** - Lets you add a certificate. Enter the certificate's serial number (in hexadecimal format HH:HH) and a comment that describes the certificate.
- **Edit** - Lets you change a certificate in the blacklist.
- **Remove** - Lets you delete a certificate in the blacklist.
- **Search** - Lets you search for a certificate in the blacklist.

Track dropped traffic

Choose if the dropped traffic is logged in SmartView Tracker or if it triggers other notifications. The options include:

- **None** - Does not record the event.
- **Log** - Records the event's details in SmartView Tracker
- **Alert** - Logs the event and executes a command, such as shows a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in Policy > Global Properties > Log and Alert > Alert Commands
- **Mail** - Sends an email to the administrator, or runs the mail alert script defined in Policy > Global Properties > Log and Alert > Alert Commands
- **SNMP Trap** - Sends an SNMP alert to the SNMP GUI, or runs the script defined in Policy > Global Properties > Log and Alert > Alert Commands
- **User Defined Alert** - Sends one of three possible customized alerts. The alerts are defined by the scripts specified in Policy > Global Properties > Log and Alert > Alert Commands

Troubleshooting

Secure connections between a client and server with no traffic create logs in SmartView Tracker labeled as "Client has not installed CA certificate". This can happen when an application or client browser fails to validate the server certificate. Possible reasons include:

- The generated CA was not deployed on clients ("Exporting and Deploying the Generated CA" on page 63).
- The DN in the certificate does not match the actual URL (for example, when you browse to https://www.gmail.com, the DN in the certificate states mail.google.com).
- Applications (such as FireFox and anti-viruses) that use an internal trusted CAs list (other than Windows). Adding the CA certificate to the Windows repository does not solve the problem.

The option in the HTTPS Validation pane:

- **Log connections of clients that have not installed the CA certificate**
• When selected, logs are recorded for secure connections between a client and server with no traffic in SmartView Tracker (default). Logs are recorded only when a server certificate is trusted by the Security Gateway. If the server certificate is untrusted, a self-signed certificate is created and always results in a log labeled as “Client has not installed CA certificate”.

• When cleared, logs are not recorded for secure connections without traffic that can be caused by not installing the CA certificate on clients or one of the above mentioned reasons.

**HTTP/HTTPS Proxy**

You can configure a gateway to be an HTTP/HTTPS proxy. When it is a proxy, the gateway becomes an intermediary between two hosts that communicate with each other. It does not allow a direct connection between the two hosts.

Each successful connection creates two different connections:

• One connection between the client in the organization and the proxy.

• One connection between the proxy and the actual destination.

**Proxy Modes**

Two proxy modes are supported:

• **Transparent** - All HTTP traffic on configured ports and interfaces going through the gateway is intercepted and proxied. No configuration is required on the clients.

• **Non Transparent** - All HTTP/HTTPS traffic on configured ports and interfaces directed to the gateway is proxied. Configuration of the proxy address and port is required on client machines.

**Access Control**

You can configure one of these options for forwarding HTTP requests:

• **All Internal Interfaces** - HTTP/HTTPS traffic from all internal interfaces is forwarded by proxy.

• **Specific Interfaces** - HTTP/HTTPS traffic from interfaces specified in the list is forwarded by proxy.

**Ports**

By default, traffic is forwarded only on port 8080. You can add or edit ports as required.

**Advanced**

By default, the HTTP header contains the **Via** proxy related header. You can remove this header with the **Advanced** option.

You can also use the Advanced option to configure the **X-Forward-For header** that contains the IP address of the client machine. It is not added by default because it reveals the internal client IP.

**Logging**

The Security Gateway opens two connections, but only the Firewall blade can log both connections. Other blades show only the connection between the client and the gateway. The Destination field of the log only shows the gateway and not the actual destination server. The Resource field shows the actual destination.

**To configure a Security Gateway to be an HTTP/HTTPS proxy:**

1. From the **General Properties** window of a Security Gateway object, select **HTTP/HTTPS Proxy** from the tree.

2. Select **Use this gateway as a HTTP/HTTPS Proxy**.

3. Select the **Transparent** or **Non Transparent** proxy mode.

   - **Note** - If you select **Non Transparent** mode, make sure to configure the clients to work with the proxy.

4. Select to forward HTTP requests from one of these options:

   • **All Internal Interfaces**
• **Specific Interfaces** - Click the plus sign to add specified interfaces or the minus sign to remove an interface.

5. To enter more ports on which to forward traffic, select **Add**.

6. To include the actual source IP address in the HTTP header, select **Advanced > X-Forward-For header (original client source IP address)**.

   **Note** - The X-Forward-For header must be configured if traffic will be forwarded to Identity Awareness gateways that require this information for user identification.

7. Click **OK**.

### HTTPS Inspection in SmartView Tracker

Logs from HTTPS Inspection are shown in SmartView Tracker. There are two types of predefined queries for HTTPS Inspection logs in SmartView Tracker:

- **HTTPS Inspection queries**
- **Blade queries** - HTTPS Inspection can be applied to these blades:
  - Application Control
  - URL Filtering
  - IPS
  - DLP
  - Anti-Virus
  - Anti-Bot

To open SmartView Tracker do one of these:

- From the SmartDashboard toolbar, select **Window > SmartView Tracker**.
- Press Control + Shift + T.

### HTTPS Inspection Queries

These are the predefined queries in **Predefined > Network Security Blades > HTTPS Inspection**.

- **All** - Shows all HTTPS traffic that matched the HTTPS Inspection policy and was configured to be logged.

- **HTTPS Validations** - Shows traffic with connection problems.
  - Action values include rejected or detected. The actions are determined by the SSL validation settings (**"HTTPS Validation"** on page 70) for HTTPS Inspection.
  - HTTPS Validation values include:
    - **Untrusted Server Certificate**
    - **Server Certificate Expired**
    - **Revoked Certificate or Invalid CRL**
    - **SSL Protocol Error** - For general SSL protocol problems

### Blade Queries

When applying HTTPS Inspection to a specified blade:

- There is an **HTTPS Inspection predefined query** for each of the blades that can operate with HTTPS Inspection. The query shows all traffic of the specified blade that passed through HTTPS inspection.

- The log in the blade's queries includes an **HTTP Inspection field**. The field value can be inspect or bypass. If the traffic did not go through HTTPS inspection, the field does not show in the log.

### Permissions for HTTPS Logs

An administrator must have HTTPS inspection permissions to see classified data in HTTPS inspected traffic.
To set permissions for an administrator in a new profile:
1. In the Users and Administrators tree, select an administrator > Edit.
2. In the Administrator Properties > General Properties page in the Permissions Profile field, click New.
3. In the Permissions Profile Properties window:
   - Enter a Name for the profile.
   - Select Customized and click Edit.
   The Permissions Profile Custom Properties window opens.
4. In the Monitoring and Logging tab, select HTTPS Inspection logs for permission to see the classified information in the HTTPS Inspection logs.
5. Click OK on all of the open windows.

To edit an existing permissions profile:
1. From the SmartDashboard toolbar, select Manage > Permissions Profiles.
2. Select a profile and click Edit.
3. Follow the instructions above from step 3.

HTTPS Inspection in SmartEvent

Events from HTTPS Inspection are shown in SmartEvent. There are two types of predefined queries for HTTPS Inspection events in SmartEvent:
- HTTPS Inspection queries for HTTPS validations
- Blade queries - HTTPS Inspection can be applied to these blades:
  - Application Control
  - URL Filtering
  - IPS
  - DLP
  - Anti-Virus

To open SmartEvent do one of these:
- From the SmartDashboard toolbar, select Window > SmartEvent.
- Press Control +Shift +T.

Event Analysis in SmartEvent

SmartEvent supplies advanced analysis tools with filtering, charts, reporting, statistics, and more, of all events that pass through enabled Security Gateways. SmartEvent shows all HTTPS Inspection events. You can filter the HTTPS Inspection information for fast monitoring on HTTPS Inspection traffic.
- Real-time and history graphs of HTTPS Inspection traffic.
- Graphical incident timelines for fast data retrieval.
- Easily configured custom views to quickly view specified queries.
- Incident management workflow.

SmartEvent shows information for all Software Blades in the environment.

Viewing Information in SmartEvent

There are two types of predefined queries for HTTPS Inspection events in SmartEvent:
- HTTPS Inspection queries
- Blade queries
HTTPS Inspection Queries

- Go to **Events > Predefined > HTTPS Inspection > HTTPS Validation** to show the SSL validation events that occurred.
- The **Details** and **Summary tabs** in the event record show if the traffic was detected or rejected due to SSL Validation settings.

Blade Queries

- There is an **HTTPS Inspection predefined query** for each of the blades that can operate with HTTPS Inspection. The query shows all traffic of the specified blade that passed through HTTPS inspection.
- The **Summary tab** in the event record in the blade's queries includes an **HTTPS Inspection field**. The field value can be inspect or bypass. If the traffic did not go through HTTPS inspection, the field does not show in the event record.
Chapter 7

Optimizing IPS

IPS is a robust solution for protecting your network from threats. Implementing the following recommendations will help maintain optimal security and performance.

During the tuning process, keep in mind that Check Point bases its assessment of performance impact and severity on an industry standard blend of traffic, placing greater weight on protocols such as HTTP, DNS, and SMTP. If your network traffic has high levels of other network protocols, you will need to take that into consideration when assessing inspection impact on the gateway or severity of risk to an attack.

Managing Performance Impact

A Check Point Security Gateway performs many functions in order to secure your network. At times of high network traffic load, these security functions may weigh on the gateway's ability to quickly pass traffic. IPS includes features which balance security needs with the need to maintain high network performance.

Gateway Protection Scope

By default, gateways using the current release inspect inbound and outbound traffic for threats. This behavior not only protects your network from threats that come from outside of your network, but also ensures that you will detect threats that may originate from your network. Changing this setting to only protect internal hosts will improve the performance of your gateway.

Note - Application Controls are not affected by the Protection Scope setting.

To change the scope of traffic that a gateway inspects:

1. Select IPS > Enforcing Gateways.
2. Select a gateway and click Edit.
3. For Security Gateways, select one of these options in the Protection Scope section:
   - Protect internal hosts only: If you select this option, the gateway protects only the internal network. This does not mean that only internal traffic is inspected. If a network object protected by one of the server-client protections is attacked, IPS inspects the internal to external traffic as well.
   - Perform IPS inspection on all traffic: the gateway will inspect all traffic regardless of its origin or destination.

For IPS-1 Sensors, select one of these options in the Topology page:

- All IPs lets the IPS-1 Sensor protections react to all traffic with the highest level of inspection. Most organizations will choose not to use this setting because it requires a high level of inspection of traffic even of traffic that does not impact the organization's security.
- Manually defined lets you specify the group of hosts or networks that the IPS-1 Sensor protects. This reduces the load on the sensor by focusing the sensor's resources on traffic that relates to internal networks.
None does not specify a group of hosts or networks for protection. When no topology is configured, the IPS-1 Sensor inspects all traffic with a lower level of intensity. The IPS-1 Sensor will inspect traffic faster but without the high level of inspection provided by the All IPs and Manually defined settings.

**Web Protection Scope**

Web Protection Scope is a feature of Web Intelligence protections which allows the administrator to choose only to apply a protection to traffic associated with specific servers. This limits the inspection activities for that protection only to the traffic which is most likely to be subjected to a given attack. For example, HTTP protections should be applied only to servers or clients involved in HTTP traffic. For more information about Web Protection Scope, see Connectivity/Performance Versus Security (on page 47).

**Bypass Under Load**

Bypass Under Load allows the administrator to define a gateway resource load level at which IPS inspection will temporarily be suspended until the gateway's resources return to acceptable levels.

IPS inspection can make a difference in connectivity and performance. Usually, the time it takes to inspect packets is not noticeable; however, under heavy loads it may be a critical issue.

You have the option to temporarily stop IPS inspection on a gateway if it comes under heavy load.

See CLI Commands (on page 18) for CLI commands related to Bypass Under Load.

**To bypass IPS inspection under heavy load:**

1. In the IPS tab, select Enforcing Gateways.
2. Select a gateway with critical load issues and click **Edit**. The **IPS** page of the **Gateway Properties** window opens.

3. Select **Bypass IPS inspection when gateway is under heavy load**.

4. To set logs for activity while IPS is off, in the **Track** drop-down list, select a tracking method.

5. To configure the definition of heavy load, click **Advanced**.

6. In the **High** fields, provide the percentage of **CPU Usage** and **Memory Usage** that defines Heavy Load, at which point IPS inspection will be bypassed.

7. In the **Low** fields, provide the percentage of **CPU Usage** and **Memory Usage** that defines a return from Heavy Load to normal load.

8. Click **OK** to close the **Gateway Load Thresholds** window.

### Cluster Failover Management

You can configure how IPS is managed during a cluster failover (when one member of a cluster takes over for another member to provide High Availability).

**To configure failover behavior for a cluster:**

1. In the **IPS** tab, select **Enforcing Gateways**.
2. Select a cluster object and click **Edit**.
The IPS page of the Gateway Cluster Properties window opens.

3. In the Failover Behavior area, select an option:
   - Prefer security - Close connections for which IPS inspection cannot be guaranteed
   - Prefer connectivity - Keep connections alive even if IPS inspections cannot be guaranteed
4. Click OK.

Tuning Protections

Profile Management

IPS profiles allow you to apply all of the protections as a group to specific gateways.

Separate Profiles by Segment

It is recommended to create separate profiles for different gateway location types. For example, the group of gateways at the perimeter should have a separate profile than the group of gateways protecting the data centers.

Separate Profiles by Gateway Version

Because this version includes some features that are not supported by older gateways (or have a different effect there), it is recommended to apply different profiles for current gateways and for older gateways.

IPS Policy Settings

The IPS Policy settings allow you to control the entire body of protections by making a few basic decisions. Activating a large number of protections, including those with low severity or a low confidence level, protects against a wide range of attacks, but it can also create a volume of logs and alerts that is difficult to manage. That level of security may be necessary for highly sensitive data and resources; however it may create unintended system resource and log management challenges when applied to data and resources that do not require high security.

It is recommended to adjust the IPS Policy settings to focus the inspection effort in the most efficient manner. Once system performance and log generation reaches a comfortable level, the IPS Policy settings can be changed to include more protections and increase the level of security. Individual protections can be set to override the IPS Policy settings.

For more information on IPS Policy, see Automatically Activating Protections (on page 20).

Note - A careful risk assessment should be performed before disabling any IPS protections.

Focus on High Severity Protections

IPS protections are categorized according to severity. An administrator may decide that certain attacks present minimal risk to a network environment, also known as low severity attacks. Consider turning on only protections with a higher severity to focus the system resources and logging on defending against attacks that pose greater risk.

Focus on High Confidence Level Protections

Although the IPS protections are designed with advanced methods of detecting attacks, broad protection definitions are required to detect certain attacks that are more elusive. These low confidence protections may inspect and generate logs in response to traffic that are system anomalies or homegrown applications, but not an actual attack. Consider turning on only protections with higher confidence levels to focus on protections that detect attacks with certainty.
IPS Network Exceptions can also be helpful to avoid logging non-threatening traffic. ("Allowing Traffic using Network Exceptions" on page 55)

Focus on Low Performance Impact Protections
IPS is designed to provide analysis of traffic while maintaining multi-gigabit throughput. Some protections may require more system resources to inspect traffic for attacks. Consider turning on only protections with lower impact to reduce the amount system resources used by the gateway.

Enhancing System Performance

Performance Pack

CoreXL
For SecurePlatform gateways running on multi-core hardware, installing CoreXL on the gateway will allow the gateway to leverage the multiple cores to more efficiently handle network traffic. For more information on CoreXL and optimizing the CoreXL configuration, see the R75.40 Firewall Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk67581).
Chapter 8

 Updating Protections

In This Chapter

IPS Services 81
Managing IPS Contracts 81
Updating IPS Protections 81

IPS Services

IPS Services maintains the most current preemptive security for the Check Point security infrastructure. To help protections stay continuously ahead of today's constantly evolving threat landscape, IPS Services provide ongoing and real-time updates and configuration advice for protections and security policies found in IPS.

IPS Services include useful tools such as:

- Protection Updates — Preemptive, ongoing and real-time protection updates, including new protection capabilities for emerging protocols and applications
- Advisories — Step-by-step instructions on how to activate and configure protections against emerging threats and vulnerabilities, usually before exploits are created by hackers
- Security Best Practices — The latest security recommendations from Check Point
- Microsoft Security Page — Extensive coverage of Microsoft SecurityBulletins and methods to protect your Microsoft environment

For more information about the full range of IPS Services, go to:


Managing IPS Contracts

To begin using IPS, enter the contract information in SmartUpdate.

If the contract is not applied properly or if it is expired, you will be notified with a message stating that the gateway does not have an IPS contract. New protections will not be downloaded if the IPS contract is expired.

Updating IPS Protections

Check Point is constantly working to improve its protections and develop protections to protect against the latest threats. You can update your IPS protections manually at any time. You can also download and install updates with a schedule.

Note - You must re-install the security policy on the Enforcing Gateways after running an update before the gateways will receive the updates.
Configuring Update Options

Before downloading the latest protections, configure the following options:

- **Mark new protections for Follow Up** can be configured in the Follow Up page. When selected, protections that are downloaded during an update will be automatically marked with a Follow Up flag and will be listed in the Follow Up page.

- **Using a proxy server** lets you enter proxy server information for IPS to use during manual and scheduled updates. Manual Updates require that the SmartDashboard host connects to the internet. Scheduled Update requires that the Security Management Server connects to the internet. To receive updates connecting these computers to the internet, enter proxy server information in Download Updates.

- **Apply Revision Control** automatically creates a Database Revision before the update occurs. Restoring this database version will allow you to revert the database back to the state that it was in before the update was performed. For more information about Database Revision Control, see the R75.40 Security Management Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk67581).

- **Check for new updates while the SmartDashboard is active** automatically checks for new updates while you have SmartDashboard open. If there are new updates, you will be prompted to Update Now or view the Version Information which details the updates that are available. You may also close the notification without updating.

**Updating IPS Manually**

You can immediately update IPS with real-time information on attacks and all the latest protections from the IPS website.

**To obtain updates of all the latest protections from the IPS website:**

- In the IPS tab, select Download Updates and click Update Now.

If you chose to automatically mark new protections for Follow Up, you have the option to open the Follow Up page directly to see the new protections.

**Scheduling IPS Updates**

You can configure a schedule for downloading the latest IPS protections and protections descriptions. Because policy installation is required in order to install the newly downloaded protections on devices, you can also choose to install the policy automatically after the new IPS information is downloaded.

**To schedule IPS protections updates:**

1. In the IPS tab, select Download Updates and click Scheduled Update.
2. Select Enable IPS scheduled update.
3. Click Edit Schedule to create a schedule for the updates.

   The Scheduled Event Properties window opens.
   a) In the General tab, enter the name of the schedule and the time that the update will run. You can choose to run the update either:
      - At a specified hour
Updating Protections

- At time intervals, such as every 12 hours
  
  To run the updates at a time interval, you must choose **Every day** in the **Days** tab.

b) In the **Days** tab, choose the days that the update will run. You can choose to run the update either:
   - Every day
   - On specified days of the week
   - On specified days of the month

c) Click **OK** to save the schedule.

The resulting schedule is shown in the Scheduled Event Properties window.

4. Click **User Center credentials** to enter your User Center username and password.
   
The User Center credentials are stored. These credentials are also used to check the status of your IPS contracts.

Once you set up a schedule, you can also choose these options:

- **On update failure perform X retries** lets you specify how many tries the Scheduled Update will make if it does not complete successfully the first time.
- **On successful update, perform Install Policy** automatically installs the policy on the devices selected using **Edit Settings** once the IPS update is completed. Both the IPS and Firewall policies install on gateways with the IPS Software Blade enabled.

**Importing an Update Package**

If Check Point Support needs to give you a special update package, you can use Offline Update to import the update package.

**To update protections from an update package:**

1. In the IPS tab, select **Download Updates** and click **Offline Update**.
2. Browse to the update package.
3. Click **OK**.

**Reviewing New Protections**

To see newly downloaded protections:

1. In the **IPS was successfully updated** message box, select **Switch to the Follow Up topic to see the new protections**.
   
   You can also go to **IPS > Protections**.
2. Sort the Protections by **Release Date** to see the latest protections.
Appendix A

Regular Expressions

Regular expressions are special characters that match or capture portions of a field. This sections covers special characters supported by Check Point and the rules that govern them.

In This Appendix

Overview of Regular Expressions 84
Metacharacters 84
Internal Options 88
Earlier Versions 88

Overview of Regular Expressions

Some IPS protections allow granular configuration with regular expressions. A regular expression is made up of two basic types of characters:

Metacharacters: characters that have special meaning, such as \ ( . | and *.

Simple characters: Any character that is not a metacharacter, for example, an alpha-numeric char that is not preceded by a backslash. These characters are treated as literals.

For example, in the Header Rejection protection, you can configure header patterns with regular expressions. The protection blocks packets with matching headers. The Header Rejection protection blocks PeoplePage Spyware by matching packet headers with the \(O|o)(C|c)(S|s)\lab\(A|a)uto(U|u)pdater regular expression.

Metacharacters

Some metacharacters are recognized anywhere in a pattern, except within square brackets; other metacharacters are recognized only in square brackets.

The Check Point set of regular expressions has been enhanced for R70 and above. The following table indicates if earlier versions do not support use of a given metacharacter.

<table>
<thead>
<tr>
<th>Metacharacter</th>
<th>Meaning</th>
<th>Earlier?</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>\ (backslash)</td>
<td>escape character, and other meanings</td>
<td>partial</td>
<td>Backslash (on page 85)</td>
</tr>
<tr>
<td>[ ] (square brackets)</td>
<td>character class definition</td>
<td>yes</td>
<td>Square Brackets (on page 86)</td>
</tr>
<tr>
<td>( ) (parenthesis)</td>
<td>subpattern</td>
<td>yes</td>
<td>Parentheses (on page 86)</td>
</tr>
<tr>
<td>{ } (curly brackets)</td>
<td>min/max quantifier</td>
<td>no</td>
<td>Curly Brackets (on page 87)</td>
</tr>
<tr>
<td>. (dot)</td>
<td>match any character</td>
<td>yes</td>
<td>Dot (on page 86)</td>
</tr>
<tr>
<td>? (question mark)</td>
<td>zero or one quantifier</td>
<td>yes</td>
<td>Question Mark (on page 87)</td>
</tr>
<tr>
<td>* (asterisk)</td>
<td>zero or more quantifier</td>
<td>yes</td>
<td>Asterisk (on page 87)</td>
</tr>
<tr>
<td>+ (plus)</td>
<td>one or more quantifier</td>
<td>yes</td>
<td>Plus (on page 87)</td>
</tr>
<tr>
<td>Metacharacter</td>
<td>Meaning</td>
<td>Earlier?</td>
<td>See</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------</td>
<td>----------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td></td>
<td>(vertical bar)</td>
<td>start alternative branch</td>
<td>yes</td>
</tr>
<tr>
<td>^ (circumflex anchor)</td>
<td>anchor pattern to beginning of buffer</td>
<td>yes</td>
<td>Circumflex Anchor (on page 88)</td>
</tr>
<tr>
<td>$ (dollar anchor)</td>
<td>anchor pattern to end of buffer</td>
<td>yes</td>
<td>Dollar Anchor (on page 88)</td>
</tr>
</tbody>
</table>

**Backslash**

The meaning of the backslash (\) character depends on the context. The following explanations are not all supported in earlier versions; see Earlier Versions (on page 88) for details.

In R70 and above, backslash escapes metacharacters inside and outside character classes.

**Escaping Symbols**

If the backslash is followed by a non-alphanumeric character, it takes away any special meaning that character may have. For example, \* matches an asterisk, rather than any character. Also, you can escape the closing bracket with a backslash [\]].

If the protection against the pattern is for earlier gateways as well as for newer ones, do not write one backslash inside square brackets. Instead, write two backslashes if you want to have a literal backslash inside square brackets.

You cannot use \ to escape a letter that is not a metacharacter. For example, because "g" is not a metacharacter, you cannot use \g.

**Encoding Non-Printable Characters**

To use non-printable characters (such as tab, return, and so on) in patterns, use the backslash before a character set reserved for non-printable characters.

<table>
<thead>
<tr>
<th>Character</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>\a</td>
<td>alarm; the BEL character (hex 07)</td>
</tr>
<tr>
<td>\cx</td>
<td>&quot;control-x&quot;, where x is any character</td>
</tr>
<tr>
<td>\e</td>
<td>escape (hex 1B)</td>
</tr>
<tr>
<td>\f</td>
<td>formfeed (hex 0C)</td>
</tr>
<tr>
<td>\n</td>
<td>newline (hex 0A)</td>
</tr>
<tr>
<td>\r</td>
<td>carriage return (hex 0D)</td>
</tr>
<tr>
<td>\t</td>
<td>tab (hex 09)</td>
</tr>
<tr>
<td>\ddd</td>
<td>character with octal code ddd</td>
</tr>
<tr>
<td>\xhh</td>
<td>character with hex code hh</td>
</tr>
</tbody>
</table>
Specifying Character Types
To specify certain types of characters (such as digits, whitespace, words) in patterns, use the backslash before a character set reserved for character types.

<table>
<thead>
<tr>
<th>Character</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>\d</td>
<td>any decimal digit</td>
</tr>
<tr>
<td>\D</td>
<td>any character that is not a decimal digit</td>
</tr>
<tr>
<td>\s</td>
<td>any whitespace character</td>
</tr>
<tr>
<td>\S</td>
<td>any character that is not whitespace</td>
</tr>
<tr>
<td>\w</td>
<td>any word character (underscore or alphanumeric character)</td>
</tr>
<tr>
<td>\W</td>
<td>any non-word character (not underscore or alphanumeric)</td>
</tr>
</tbody>
</table>

Square Brackets
Square brackets ([ ]) designate a character class and match a single character in the string. Inside a character class, only the character class metacharacters (backslash, circumflex anchor and hyphen) have special meaning.

You must use a backslash when you use character class metacharacters as literals inside a character class only. Square brackets that are used as literals must always be escaped with backslash, both inside and outside a character class.

For example, [[abc]] should be written: \[[abc]\]

Character Class Metacharacters

<table>
<thead>
<tr>
<th>Metacharacter</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>general escape character</td>
</tr>
<tr>
<td>^</td>
<td>negate the class, if this is the first character in the brackets (If ^ is not the first, it is not a metacharacter.)</td>
</tr>
<tr>
<td>-</td>
<td>indicates character range</td>
</tr>
</tbody>
</table>

Parentheses
Parentheses ( ) designate a subpattern. To match with either an open-parenthesis or closing-parenthesis, use the backslash to escape the symbol.

Hyphen
A hyphen '-' indicates a character range inside a character class. When used as a simple character in a character class, it must be escaped by using a backslash '\'.

For example: [a-z] matches the lower-case alphabet.

Dot
Outside a character class, a dot (.) matches any one character in the string.
For example: \* matches zero or more occurrences of any character
Inside a character class, it matches a dot (\.).

Quantifiers
Various metacharacters indicate how many instances of a character, character set or character class should be matched. A quantifier must not follow another quantifier, an opening parenthesis, or be the expression's first character.
These quantifiers can follow any of the following items:
• a literal data character
• an escape such as \d that matches a single character
• a character class
• a sub-pattern in parentheses

Curly Brackets
Curly brackets (\{\}) are used as general repetition quantifiers. They specify a minimum and maximum number of permitted matches.
For example: a\{2,4\} matches aa, aaa, or aaaa
If the second number is omitted, but the comma is present, there is no upper limit; if the second number and the comma are both omitted, the quantifier specifies an exact number of required matches.
For example:
• [aeiou]\{3,\} matches at least 3 successive vowels, but may match many more
• \d\{8\} matches exactly 8 digits

Note - A closing curly bracket '}' that is not preceded by an opening curly bracket '{' is treated as a simple character. However, it is good practice to use a backslash, '\}', when using a closing curly bracket as a simple character.

Question Mark
Outside a character class, a question mark (?) matches zero or one character in the string. It is the same as using \{0,1\}.
For example: c(\[[ab]\]?r) matches car, cbr, and cr
Inside a character class, it matches a question mark: [? ] matches ? (question mark).

Asterisk
Outside a character class, an asterisk (*) matches any number of characters in the string. It is the same as using \{0,\}.
For example: c(\[[ab]\]*r) matches car, cbr, cr, cabr, and caaabbbr
Inside a character class, it matches an asterisk: [*] matches * (asterisk).

Plus
Outside a character class, a plus (+) matches one or more characters in the string. It is the same as using \{1,\}.
For example: c(\[[ab]\]+) matches character strings such as car, cbr, cabr, caaabbbr; but not cr
Inside a character class, it matches a plus: \[ + \] matches + (plus).

**Vertical Bar**

A vertical bar (|) is used to separate alternative patterns.

If the right side is empty, this symbol indicates the NULL string: a| matches a or empty string.

For example: a|b matches a or b

**Circumflex Anchor**

A circumflex anchor (^; also known as a caret) is used to match only the beginning of a buffer. The circumflex is treated as an anchor only when it is the first character in the pattern and can also be used to negate a character class, but only if it is the first character of the class.

A circumflex anchor that is used as literal must always be escaped with backslash, both inside and outside character class.

**Dollar Anchor**

A dollar anchor ($) is used as a metacharacter only if it is the last character of a pattern and only to match the end of a buffer.

A dollar anchor that is used as literal must be escaped with backslash when it is not inside a character class.

For example: ab$ matches a string that ends in ab

**Internal Options**

To configure for compilation options from within the pattern, enclose the option strings between curly brackets, with a colon at the end: { }:

To specify multiple option strings, use the semicolon (;) as a separator.

An internal option setting must appear at the beginning of the pattern, and are applied to the whole pattern.

For example: {case; literal}:*a matches the string "*a"

The option strings are described in the following table.

**Internal Option Strings**

<table>
<thead>
<tr>
<th>Option String</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>case</td>
<td>Treat all characters in the pattern as case-sensitive</td>
</tr>
<tr>
<td>caseless</td>
<td>Treat all characters in the pattern as case-insensitive</td>
</tr>
<tr>
<td>literal</td>
<td>Treat all characters in the pattern as literals (metacharacters are treated as regular characters)</td>
</tr>
<tr>
<td>LSS(string)</td>
<td>Force string to be the pattern's LSS</td>
</tr>
</tbody>
</table>

**Earlier Versions**

If you have gateways of earlier versions, and you create a regular expression for a protection enabled on such a gateway, IPS checks if the pattern is supported. If a pattern does not support both earlier versions and the new version of Check Point regular expressions, you are notified.

If you have earlier gateways as well as newer ones, and you want to configure a protection against a pattern, you can do one of the following:
• Change the pattern to use metacharacters that are supported by both the newer version of Check Point software and the earlier versions.
• Configure GUIDBedit for both patterns.

**Support for Internal Option Settings**
Internal compilation options are not supported in earlier versions.

**Support for Backslash**
• **Escaping symbols:** In earlier versions, the backslash to escape metacharacters applies only outside character classes. **For example:** `\*` matches `*`; but `[\*]` matches `"*"`.
• **Specifying character types:** In earlier versions, this usage of backslash is not supported.
• **Encoding non-printable characters:** In earlier versions, this usage of backslash is not supported.

**Support for Square Brackets**
To make a closing square bracket be part of a character class (to match `]` as a character in a string):
• In earlier versions: use the closing bracket as the first character in the class; or, if using the circumflex anchor, it may come after the circumflex anchor. `[[]` or `[^]`
• In R70 and above: escape the closing bracket with a backslash. `\[\]`

**Support for Quantifiers**
In earlier versions, only `*` (zero or any number), `+` (one or more), and `?` (zero or more) are supported. The minimum/maximum quantifiers (using curly brackets) are not supported in earlier versions.

**Support for Circumflex and Dollar Anchors**
If the protection against the pattern is for earlier gateways as well as for newer ones, do not write a circumflex or dollar in the middle of the pattern.

If you want to specify a literal circumflex or dollar outside square brackets, always add a preceding backslash.
• In earlier versions, the circumflex or dollar anchor is always a metacharacter (unless preceded by backslash or inside a character class).
• In R70 and above, the circumflex anchor is a metacharacter only if it is the first character of a pattern; the dollar anchor is a metacharacter only if it is the last character of a pattern.

**Support for Hyphen**
A hyphen (`-`) is used to specify a range of characters in a character class. For example, `[a-z]` matches the lower-case alphabet.
• In earlier versions, if a hyphen is required as a character without special meaning, it must be the first or last character in a character class.
• In R70 and above, if a hyphen is required as a regular character, it must be escaped with a backslash.
Index

A
Action • 68
Activating New Protections • 51
Activating Protections • 20
Activating Protections for a Specific Profile • 23
Activating Protections for All Profiles • 23
Activation Settings • 9
Adding a New Host Site • 68
Adding a Server Certificate • 66
Adding IPS Software Blade Gateways • 16
Adding IPS-1 Sensors • 17
Adding Trusted CAs for Outbound HTTPS Inspection • 70
Adjusting Allowed Concurrent HTTP Connections • 48
Advanced IPS Protection • 13
Advanced Sorting • 29
Aggressive Aging Configurations • 36
Allowing Traffic using Network Exceptions • 56
Anti Spoofing Configuration Status • 36
Application Layer • 45
Assigning Profiles to Gateways • 24
Asterisk • 88
Attaching a Packet Capture to Every Log • 55
Authenticity is Assured • 40
Automatically Activating Protections • 20
Automatically Marking New Protections for Follow Up • 60
Automatically Updating the Trusted CAs List • 70

B
Backslash • 86
Basic IPS Protection • 12
Blade • 69
Blade Queries • 75
Blocking IP Fragments • 39
Bypass Under Load • 14, 78
Bypassing HTTPS Inspection to Software Update Services • 69

C
Certificate • 69
Certificate Blacklisting • 72
Changing the Assigned Profile • 13
Choosing the Level of Protection • 12
Circumflex Anchor • 89
Citrix ICA • 43
CLI Commands • 18
Cluster Failover Management • 79
Confidence Level • 32
Configuring Aggressive Timeouts • 36
Configuring Application Intelligence • 40
Configuring Geo Protections • 48
Configuring Implied IPS Exceptions • 51
Configuring Inbound HTTPS Inspection • 65
Configuring IP Fragments Thresholds • 39
Configuring IPS Pattern Granularity • 51
Configuring Network Exceptions • 57
Configuring Network Security Settings • 35
Configuring Outbound HTTPS Inspection • 63
Configuring Specific Protections • 35
Configuring Thresholds • 37
Configuring Update Options • 83
Configuring Web Intelligence • 44
Configuring Web Intelligence Protections • 44
Connectivity/Performance Versus Security • 47
Controlling Traffic by Country • 49
CoreXL • 81
Creating an Outbound CA Certificate • 63
Creating Profiles • 19
Curly Brackets • 88
Customizable Error Page • 46
Customizing Profiles for IPS-1 Sensors • 26
Customizing the Protections Browser View • 27

D
Default Protection • 12
Defining Allowed Applications • 43
Defining Commands and Distinguished Names • 45
Defining DNS Servers • 33
Defining HTTP Worm Patterns • 45
Defining Mail Servers • 34
Defining Peer to Peer HTTP Headers • 42
Defining Web Servers • 33
Deleting Profiles • 25
Deploying Certificates by Using Group Policy • 65
Destination • 67
DNS Servers • 33
Dollar Anchor • 89
Dot • 87
DShield Storm Center • 39

E
Earlier Versions • 89
Editing DNS Servers • 33
Editing Mail Servers • 34
Editing Web Servers • 34
Enabling HTTPS Inspection • 63
Encoding Non-Printable Characters • 86
Enforcing Gateways • 8
Enhancing System Performance • 81
Escaping Symbols • 86
Event Analysis in SmartEvent • 75
Exporting a Certificate from the Security Management Server • 64
Exporting and Deploying the Generated CA • 64
Exporting Protections List • 30

F
Filtering Protections • 28
Finding Protections • 28
Focus on High Confidence Level Protections • 80
Focus on High Severity Protections • 80
Focus on Low Performance Impact Protections • 81
FTP • 41
Functions for Monitoring • 9
Scheduling IPS Updates • 83
Security Center • 11
Security Status • 10
Separate Profiles by Gateway Version • 80
Separate Profiles by Segment • 80
Server Certificates • 65
Server Validation • 71
Services • 67
Setting POP3/IMAP Scope • 40
Severity • 32
Site Category • 67
SNMP • 43
Sorting Protections • 29
Source • 67
Specifying Character Types • 87
Square Brackets • 87
Streaming Engine Settings • 36
Support for Backslash • 90
Support for Circumflex and Dollar Anchors • 90
Support for Hyphen • 90
Support for Internal Option Settings • 90
Support for Quantifiers • 90
Support for Square Brackets • 90

T
The Check Point IPS Solution • 7
The HTTPS Inspection Policy • 66
The IP Address to Country Database • 49
Tour of IPS • 8
Track • 68
Tracking Protections using Follow Up • 58
Troubleshooting • 13, 73
Troubleshooting Profiles • 26
Tuning Protections • 80
Type • 30
Types of Protections • 9

U
Unmarking Protections for Follow Up • 60
Unmarking Protections from Follow Up Page • 61
Unmarking Protections from Protection Details • 61
Updating IPS Manually • 83
Updating IPS Protections • 82
Updating Protections • 82

V
Vertical Bar • 89
View Protected Gateways by Profile • 24
Viewing Information in SmartEvent • 76
Viewing IPS Event Details • 54
Viewing IPS Events • 53
Viewing Network Exceptions • 57
Viewing Packet Capture Data in SmartView Tracker • 55
Viewing Profile Modification Data • 24
VoIP • 43
VPN Protocols • 43

W
Web Protection Scope • 78
Web Servers • 33
Working with Packet Information • 55