CHECK POINT IPS
R75.X, R76 AND R77.X
Best Practices
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 Version of this Document**

Download the latest version of this document

To learn more, visit the Check Point Support Center

**Feedback**

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

Please help us by sending your comments
cp_techpub_feedback@checkpoint.com?subject=Feedback on Check Point IPS R75.x, R76 and R77.x Best Practices.

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 October 2018</td>
<td>Updated: Section Overview [on page 21] (in the Chapter <em>Performance Tuning</em>)</td>
</tr>
</tbody>
</table>
| 02 November 2016       | Updated: Configuring the Security Gateway Performance Settings [on page 10] - changed High setting to 80%.
|                       | Updated: Analyzing the Initial Logs [on page 13] - added procedure to determine the applicable mode for each IPS protection.               |
|                       | General updates                                                                                                                              |
| 29 June 2016          | Updated: Section Overview [on page 21] (in the Chapter *Performance Tuning*)                                                                     |
|                       | Improved formatting                                                                                                                          |
| 06 January 2015       | Added: Overview of the Tuning Process [on page 6]                                                                                             |
|                       | General updates                                                                                                                              |
| 17 September 2014     | First release of this document                                                                                                               |
Introduction

In This Section:

Choosing IPS Protections........................................................................................................5
Overview of the Tuning Process.................................................................................................6

IPS is not a “set and forget” solution. To maximize your network’s security and performance, configure it to best fit the unique traffic of each organization. The world of cyber-threats and your network are dynamic. Therefore, it is necessary to consistently tune and maintain IPS. Check Point recommends you update to the latest IPS update. The update process can be scheduled for a specific date and time.

The goal of this guide is to assist you in the initial and ongoing tuning of your IPS Software Blade.

Choosing IPS Protections

The IPS tuning best practices are based on knowledge from Check Point’s ThreatCloud Managed Security Service that continuously monitors and manages of hundreds of IPS gateways for Check Point customers.

When you tune IPS, you must decide which protections to enable. For each enabled protection, you must select Prevent or Detect mode. In addition, network environments and the threat landscape are very dynamic. To ensure maximum protection, the IPS security policy must adapt accordingly. IPS tuning must be a continual process to address the changing threat landscape, changing network configuration, newly released and updated protections, new gateway capabilities, and more. The bottom line is that IPS tuning is a continuous task that needs to be managed professionally at all times.

This guide explains the best practice guidelines to help you manage the Check Point IPS Software Blade. One of the key elements to maintain an effective IPS policy is to monitor IPS events in real-time:

• Understand how IPS protections process traffic and protocols across the network.
• Identify where it is necessary to tune IPS and exclude unique traffic protocols.

This guide does not explain how to mitigate malware attacks.

When you tune the IPS policy, consider these areas:

• Coverage – Does the IPS policy cover all critical network assets and services, vulnerabilities, and threats?
• Accuracy – Do all the protections in the IPS policy alert only for real threats, and not for legitimate traffic?
• Performance – Is there enough CPU and memory to run the new IPS policy?

IPS tuning is the science (and art) of balancing the trade-offs between these three areas with corporate security, compliance and operational requirements.

Most of this guide focuses on how you can optimize security coverage and accuracy. Performance Tuning [on page 21] is discussed in a separate section.
Overview of the Tuning Process

It takes approximately one to two weeks to tune your IPS policy. We recommend that you follow this checklist during the tuning process, and refer to additional information and instructions ("Implementing IPS" on page 8) as necessary for each step.

Getting started:
1. Update the IPS package. Make sure that the Security Gateway is up-to-date with the most recent protection signatures.
2. Set the default IPS action to Prevent. This action gives maximum network protection.
3. Set the default IPS action for newly downloaded protections to Prevent.
4. Clone the Recommended Profile. Create a backup copy and make sure that all changes are only on the cloned profile.

The security requirements for the different segments in your network often depend on the specified traffic types and network objects for each segment. For deployments with a Multi-Domain Server or several gateways, consider creating separate IPS policies and perform these steps for each segment.
5. Enable Troubleshooting mode.

During the initial tuning process, the IPS Software Blade inspects the network’s unique traffic, but does not block it. When you use Troubleshooting mode, even though all protections are set to Prevent, the gateway only detects possible threats and generates logs for the traffic.
6. Click Follow Up. Select Mark newly downloaded protections for Follow Up to help the analysis and tuning of new protections.
7. Configure the gateway. Assign the active profile to the relevant gateways.

To make sure that IPS analysis does not have a negative impact on network traffic, enable Bypass IPS inspection when gateway is under heavy load is a consideration.
8. Install the policy on the gateways. New IPS updates and changes in the active profile are not automatically deployed. You must install the policy and push it to the gateways.
9. Collect the logs. After you install the policy, IPS starts to inspect the traffic and generate logs. We recommend that you collect logs for at least a week, and ideally for two weeks.

Note - The IPS Software Blade does not block malicious traffic when Troubleshooting mode is enabled.

Initial IPS tuning:
1. Review the logs. Decide which protections to run in Protect or Detect mode, and which ones require more fine-tuning and analysis.
2. Disable Troubleshooting mode.

The IPS Software Blade now protects the network.
3. Change the settings for Updates policy. Configure updates to Newly downloaded protections will be set to Detect.

When new IPS protections are deployed, they are set to Detect mode.
4. Clear the Follow up or Newly downloaded flags for all protections reviewed during the tuning process.
**Ongoing maintenance and tuning:**
We recommend that twice a month you tune the new IPS protections, and look for changes in the behavior of the ones that you already tuned.

**Performance tuning:**
Monitor the gateway performance and configure the applicable settings to give the best network security and performance.
Implementing IPS

In This Section:

Initial Installation ............................................................................................................8
Collecting IPS Logs ....................................................................................................... 12
Analyzing the Initial Logs ............................................................................................. 13
Configuring IPS to Protect the Network ....................................................................... 14

Initial Installation

The Check Point IPS Software Blade uses thousands of protections to keep your network safe. When you set up IPS for the first time, it is impossible to run a signature analysis for each protection. While you implement IPS, you can use a mirror port or TAP server or appliance to run an analysis on the traffic. We recommend you deploy IPS in-line when you enable Protect mode.

The Recommended Profile is defined to give excellent security with good gateway performance. This profile enables all protections to:

- Protect against important threats
- Have an attack confidence level of at least good
- Do not have a critical effect on performance

Updating Protections

The IPS Software Blade includes the protections available when the software was first released. The first time that you enable IPS, it is important to update and download the most recent protections.

To update the IPS protections:

Note - We recommend that you select the checkbox to enable revision control before you download a new IPS update.

1. Log in to SmartDashboard.
2. From the navigation tree in the IPS tab, click Download Updates.
   The Download Updates window opens.
3. Click Update Now.
4. If necessary, enter the User Center credentials.
Cloning the Profile

Make a copy of the Recommended Profile before you start the initial IPS tuning. Make sure that all changes are only on the cloned profile. For a Multi-Domain Server deployment, we recommend that you create a separate IPS policy and perform these steps for each segment.

To clone the Recommended Profile:
1. From the navigation tree in the **IPS** tab, click **Profiles**.
   The **Profiles** window opens.
2. Right-click the **Recommended_Profile** and select **Clone selected profile**.
   The new profile is added to the list of profiles.

Configuring the Profile

For the initial analysis of the IPS inspection, configure the profile settings with **Troubleshooting** mode enabled.

The default action for the protections is **Prevent**. However, when **Troubleshooting** mode is enabled, the protections run in **Detect**. During this initial analysis, you detect security events and generate logs. IPS blocks malicious traffic only after the initial analysis and tuning is complete.

When you configure the profile:
- Set the default action of the profile to **Prevent**. The majority of the protections are finally deployed in **Prevent** mode.
- When you initially implement IPS, configure the blade to run in **Troubleshooting Detect-only** mode.
- Configure new protections that are added to the profile to run in **Prevent** mode. During the initial analysis, these protections are set to **Detect**.

To configure the profile:
1. From the navigation tree in the **IPS** tab, click **Profiles**.
   The **Profiles** window opens.
2. Double-click the profile.
   The **General** page of the **Profile Properties** window opens.
3. In the **IPS Mode** section, select **Prevent**.
4. From the navigation tree, click **IPS Policy > Updates Policy**.
5. For **Newly downloaded protections will be set to**, select **Prevent**.
6. From the navigation tree, click **Troubleshooting**.
7. Click **Detect-only**.
   The window shows this message: **Detect-Only for Troubleshooting is enabled**.
8. Click **OK**.

Some protections require further configuration. For example, email protections require you to configure a mail server. See Email Protections (on page 18).
Scheduling IPS Updates

You can schedule periodic updates of the IPS protections based on your organization’s needs and policies.

Configure the regular IPS updates for the profile. We recommend that you use all of these settings:

- Daily updates of IPS protections
- Enable **Apply Revision Control** to revert to earlier versions if necessary
- Configure IPS to update the protections each time you open SmartDashboard

To schedule IPS updates:

1. From the navigation tree in the **IPS** tab, click **Download Updates**.
   The **Download Updates** window opens.
2. Click **Apply Revision Control**.
3. Click **Check for new updates while SmartDashboard is active**.
4. Click **Scheduled Update**.
   The **Scheduled Update** window opens.
5. Click **Enable IPS scheduled update**.
6. Click **Edit Schedule**
7. Configure a daily IPS update.
8. Click **OK**.
9. If necessary, click **User Center credentials**, and enter the User Center username and password.
10. Click **OK**.

Configuring the Security Gateway Performance Settings

When the IPS Software Blade is enabled on a Security Gateway, it can affect the network performance. We recommend that you configure the gateway to bypass IPS inspection when there is a heavy load on the server or appliance.

To configure bypass under load on the gateway:

1. From the navigation tree in the **IPS** tab, click **Enforcing Gateways**.
   The **Enforcing Gateways** window opens.
2. Double-click the gateway that runs IPS analysis on the traffic.
   The **IPS** page of the gateway window opens.
3. In the **Bypass Under Load** section, click **Bypass IPS inspection when gateway is under heavy load**.
4. Click **Advanced**.
5. Change the settings for the **CPU** and **Memory Usage**:
   - **Low** - 50%
   - **High** - 80%
6. Click **OK**.
Installing the Policy

Install the policy to push the IPS profile to the gateway.
Collecting IPS Logs

Install the policy with the new profile and let it run IPS analysis and generate logs for at least a week. We recommend that you wait two weeks before you disable Troubleshooting mode and enable the Prevent protections.

**Note** - While you run IPS analysis, all protections run in Detect mode and the gateway cannot block IPS attacks.
Analyzing the Initial Logs

After you collect the IPS logs, analyze them to determine the mode for each IPS protection:

- **Prevent** - Blocks the traffic
- **Detect** - Allows the traffic and generates a log

For each IPS protection:

1. Look at the generated log and use the attached traffic capture to investigate it. A traffic capture can be enabled for each protection separately.
2. If a SOC department exists, logs should be further analyzed by a SOC engineer to negate a true positive case.
3. Low confidence and application control protections may generate many FP logs. To reduce the number of logs, you can disable protections for products that are not used in your network.

**Protections that run in Prevent mode**

You do not need to configure these protections. When you disable **Troubleshooting** mode, these protections automatically run in **Prevent** mode.

Protections that did not generate any events during the initial tuning remain in **Protect** mode. They maintain a high level of security and do not impact network performance.

Protections that generated events only for malicious traffic also remain in **Protect** mode. You can identify events as malicious based on:

- Country and reputation of the source IP address (for example, use ipvoid.com)
- URLs
- Packet capture analysis

**Protections to run in Detect mode**

We recommend that you configure protections that generate events for a wide range of legitimate traffic to run in **Detect** mode. In addition, report these protections to Check Point for additional analysis and classification.

**Protections that require more analysis**

Some protections generate events for both legitimate and malicious traffic. One possible reason is that legacy applications often use non-standard traffic and generate an IPS event. We recommend that you look for patterns in the events of the legitimate traffic and create IPS network exceptions. For example, there can be a small set of Source or Destination IP addresses, services, or ports.

If you can identify a pattern for the types of traffic:

1. Create network exceptions for each type of traffic.
2. Set the protection to **Prevent**.

If you cannot identify a pattern:

1. Set the protection to **Detect**
2. Report the protection to Check Point.
Configuring IPS to Protect the Network

When you complete the initial IPS tuning, disable Troubleshooting mode and configure the IPS Software Blade for regular operation. The profile is now configured to maximize performance and security for your network. It is necessary to continue to regularly run maintenance tuning ("Ongoing IPS Maintenance Tuning" on page 15) for the IPS protections.

To configure IPS to protect the network:

1. From the navigation tree in the IPS tab, click Profiles.
   The Profiles window opens.
2. Double-click the profile.
   The General page of the Profile Properties window opens.
3. From the navigation tree, click Troubleshooting.
4. Click Detect-only.
   The window shows this message: Detect-Only for Troubleshooting is disabled.
5. Click OK.
6. Install the policy.
   The IPS Software Blade now protects the network.
Overview

After you successfully configure the initial IPS installation, most protections are deployed in Prevent mode. A few remain in Detect mode for additional analysis. However, new threats continuously emerge and the internal network changes with new applications, services and protocols. It is necessary to regularly run an analysis on the IPS logs for maintenance tuning of the policy.

We recommend that you run an IPS analysis twice a month and review IPS updates (on page 16) for new attacks and other issues.

Analyzing New Protections

We recommend that you deploy new Protections in Detect mode ("Configuring the Profile" on page 9). As you did when you performed the initial installation, run an analysis on the new protections ("Analyzing the Initial Logs" on page 13) and determine if they can run in Prevent mode.

Running Maintenance on Existing Protections

Run an analysis on the logs that are generated by the IPS protections.

Protections in Prevent Mode

Make sure that most of the events are generated by malicious traffic. Analyze these events based on the source IP address, URLs, and packet capture.

If events are generated by legitimate traffic:

1. Try to identify the pattern and create an exception for the traffic.
2. If you cannot identify the pattern, configure the protection to Detect mode.

   Note - If this protection generates a small number of logs, we recommend that you continue to run it in Prevent mode.

Protections in Detect Mode

Make sure that events continue to be generated for legitimate traffic.

If legitimate traffic no longer generates events, change the protection to Prevent mode.
General Recommendations

This section contains general advice to help you manage the IPS Software Blade.

IPS Updates

Check Point releases new IPS protections packages as necessary, usually at least once a week.

It is important to review the published Check Point IPS update. The update shows new protections against zero-day vulnerabilities. If the protections are crucial for your network, immediately deploy them in **Prevent** mode.

There is a risk that a new protection might disrupt legitimate traffic. However, there is a greater benefit in preventing active malware attacks.

Software Upgrades

It is important to review the Release Notes for new software versions, and regularly install software updates.

Check Point IPS combines the features of the IPS engine and new protections that are continually added. The engine is the core code that parses and inspects the traffic. It is often improved as part of software upgrades for Security Gateways.

These upgrades give better IPS protection and performance. For example:

- R75.40 improved the Non-Compliant HTTP inspection protection.
- R76 improved the Non-Compliant DNS protection.

Separate Profiles

The initial performance tuning focuses on a single IPS profile that is recommended for many situations. However, it can be necessary to create different profiles for the specified gateways in an organization to improve security or performance.

Examples of separate profiles:

- Gateways on the perimeter often use a different profile than gateways that protect data centers.
- Gateways that use different versions of Check Point software can use different profiles.
IPS Management Tips

Enhancing the Recommended Profile

The initial tuning process uses only protections that are included in the **Recommended** IPS profile. We recommend that you add other protections to the active IPS profile. Make sure that you run the performance-tuning procedure ("Analyzing the Initial Logs" on page 13) before you enable **Prevent** mode for a protection.

These are some common additional protections for a profile:

- **Application Control** - These protections identify and can control specific applications and protocols such as VNC, BitTorrent, Google Talk, and TeamViewer.
  
  Review Application Control protections, and enable the ones that help protect the network. However, the optimal way to manage how applications are used is with the Check Point Application Control Software Blade.

- **DoS (Denial of Service)** - There are several protections that look for massive use of Web Server protocols (UDP, HTTP, SSL). They can detect and protect the network from DoS attacks.

Configuring Individual Protections

Some IPS protections require more in-depth customization to give a network the best security.

- **SQL Injection** - This protection runs a scan on traffic to a user-defined list of specified web servers. The protection is active only when the network objects for these servers are created correctly. Do not apply the protections for SQL injection to all HTTP traffic, as unnecessary false-positives can disrupt network traffic.

- **Geo Protection** - Control network traffic for specified countries. An IP-to-country database connects packet IP addresses to the countries. Configure one set of policies for each Profile to block or allow traffic for one or more countries. If your company has no business and network traffic with certain countries, you can use Geo Protection to block the traffic. When you block traffic, you increase overall security and are well protected against targeted and DDoS attacks. You can track traffic to or from other countries and after some time determine if you can also block the traffic.
  
  **Note** - If you track traffic for all countries, IPS generates too many logs.

- **General HTTP/CIFS Worm Catcher and Header Rejection** - These protections let you add and edit regular expressions so that the Firewall can block the specified HTTP requests. Check Point occasionally advises customers to add a pattern to these protections as an immediate pre-emptive action against a new threat. The IPS protections are updated when the new protections package is available from Check Point.

- **SNORT Conversion** - Gateways that are version R76 and higher can import and convert SNORT signatures to IPS protections. You can use public-domain and custom signatures to help protect the network. For more about how to use SNORT signatures for IPS, go to the *IPS Administration Guide* for your version.

Email Protections

Activate protections for the protocols that your environment uses for emails and add customized security to the mail servers.

**Setting POP3/IMAP Scope**

By default, when you configure the POP3/IMAP Security settings in Protections > By Protocol > IPS Software Blade > Application Intelligence > Mail, they apply to all hosts that are defined as mail servers based on the Action settings of each IPS profile. You can also limit the scope of this protection to only the specified mail servers.

To specify which hosts get the POP3/IMAP protection settings:

1. In the IPS tab, go to Protections > By Protocol > IPS Software Blade > Application Intelligence > Mail.
2. In the Look for field, enter POP3/IMAP Security.
3. In the search results that show, double-click POP3/IMAP Security.
   
4. Select the profile and click Edit.
5. In the Protection Scope area, click Apply to selected mail servers.
6. Click Customize.
   
   The Select Servers window opens, and all mail servers are selected by default.
7. Change selection of servers on which POP3 and IMAP protections should not be enforced:
   • To remove servers from the list - clear the servers
   • To add servers to this list - click Add, select the servers, and click OK
   • To edit server settings - select a server, click Edit, edit settings in the Host Node configuration window that opens, and click OK

8. Click OK.

The POP3/IMAP Security protection has a list of commands that IPS recognizes and inspects. The definitions of the POP3 commands apply to all IPS profiles. In the Protection Details - POP3/IMAP Security configuration window, you can edit the list of POP3 commands that apply to all profiles or edit the list of POP3 commands that apply to specific profiles.

To edit the list of POP3 commands that apply to all profiles:
1. In the Protection Details - POP3/IMAP Security configuration window, click Edit for the POP 3 Commands Definitions.
   The Add custom POP3 command window opens.
2. Edit the list as necessary:
   • To add a new command - click Add and enter the new command
   • To change an existing command - select the command, click Edit, and edit the command
   • To delete a command - select the command, click Remove, and in the window that opens, click Yes to confirm
3. Click OK.

To block or allow a POP3 command for a profile:
1. In the Protection Details - POP3/IMAP Security configuration window, select the profile for which you want to edit the settings.
2. Click Edit.
   The Protection Settings window opens.
3. In the list of Known POP3 commands, clear any command that you do not want blocked.

When you finish editing POP3/IMAP Security settings, click OK to save them and exit the Protection Details - POP3/IMAP Security configuration window.
Ongoing IPS Maintenance Tuning

Optimizing Web Security Protections

You can manage Web Intelligence to configure the Web server settings to maximize security and reduce the Security Gateway performance, or the opposite.

**Improving Connectivity by Setting Scope**

Some inspection settings that are too severe can have a negative impact on 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.

Applying these restrictions (activating these protections) is in general good practice, but they may 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 only to a defined set of Web servers, select **Apply to selected web servers**.
3. Click **Customize**.
   - To exclude a Web server from the protection, clear the server 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.
Performance Tuning

Overview

When a gateway CPU consistently runs at a high load, it is possible that the active profile is too heavy for the hardware. We recommend that you change the profile and IPS settings to optimize IPS for the network.

Use SNMP or SmartView Monitor to monitor CPU load and memory usage for a few days. Make sure that the gateway meets these hardware statistics to continue to deploy the active profile:

- CPU utilization - average utilization is lower than 30% across cores
- CPU Peaks - short interval peaks (1 - 2 minutes) lower than 50% utilization
- Free RAM - at least 20%

If the gateway does not meet the previous requirements:

- Upgrade to an appliance or server with more powerful hardware
- Run fewer IPS protections in the network

The following sections show different methods to reduce IPS protections and improve gateway performance.

Note - The performance impact of a protection is almost the same for Prevent and Detect modes. Prevent mode sometimes drops traffic and does not inspect it.
Changing IPS Protection Scope

You can configure IPS for a gateway to inspect the traffic from the external to internal network only. Change the IPS protection scope to protect only the internal network. IPS does not run scans on traffic from the internal to the external network.

To change the IPS Protection Scope:

1. From the navigation tree in the IPS tab, click **Enforcing Gateways**. The **Enforcing Gateways** window opens.
2. Double-click the gateway. The **IPS** page of the gateway window opens.
3. From the **Protection Scope** section, click **Protect internal hosts only**.
4. Click **OK**.
5. Install the policy on the gateway.
Excluding Protections

The IPS profile can include protections that are not necessary for the network. You can exclude unnecessary IPS protections for the application or service and improve network performance. For example, if an organization does not use VoIP services, exclude the IPS protections for VoIP traffic.

Exclude a Protection Category

IPS Protections are classified into categories of applications and protocols that they protect. If there are applications that are not used in the network, you can exclude the appropriate category of IPS protections.

To exclude an IPS category:

1. From the navigation tree in the IPS tab, click Profiles. The Profiles window opens.
2. Double-click the profile. The General page of the Profile Properties window opens.
3. From the navigation tree, click IPS Policy.
4. From the Protections to Deactivate section, click Do not activate protections categories.
5. Click Configure. The Non-Auto Activation window opens.
6. Click Add.
7. Select the category of IPS protections that you are excluding.
8. Click OK.
9. Install the policy.

Exclude a Specified Protection

Often it is not possible to exclude an entire category of IPS protections. However, you can still exclude individual protections for:

- An application or a feature that you do not use
- An application that is non-vulnerable because it is a fully patched version

To safely exclude protections, make sure that you have all the data about the applications and services that run in the network. It must be up-to-date, and include data about software versions and patches.

To exclude a specified IPS protection:

1. From the navigation tree in the IPS tab, click Network Exceptions. The Network Exceptions window opens.
2. Click New. The Add/Edit Exception Rule window opens.
3. From Profile, select the active profile.
5. Click Select. The Select Protection window opens.
6. Select the IPS protection that you are excluding.
7. Click OK.
8. From the Install On section, click Apply this exception.
9. From the drop-down menu, select the gateway.
10. Click OK.
11. Install the policy.
Gradually Activating Protections

The Recommended Profile does not include protections that have a critical impact on performance. However, it is possible that you must disable additional protections with a lower performance threshold to reduce the load on the gateway. If you do not have a detailed performance analysis of the IPS protections, we recommend that you disable high Performance Impact protections and then gradually activate them.

Sample Workflow

1. Disable all IPS protections with that are categorized as Critical or High Performance Impact.
2. Identify the protections that protect high-value assets.
   a) Enable one protection.
   b) Monitor the performance of the gateway.
   c) Make sure that the gateway handles the IPS load.
   d) Do the previous steps again for other High Performance Impact protections.
Tuning Performance Impact

Check Point categorizes the performance impact of protections based on the industry standard estimation of network traffic, and emphasizes protocols such as HTTP, DNS, and SMTP. In addition, you can measure the actual performance impact of the protections and then disable the ones that use too much CPU.

Use the applicable command in Expert mode to gather statistics about protections impact:

- For R77 and higher, run `get_ips_statistics.sh`
- For R76 and earlier, run `fw ctl sdstat`

Carefully review protections that use more than 1% load. If problems persist, send the `pm_stats` data to your Check Point resources (Technical Support, Professional Services or Managed Security Service) for additional analysis.

For more on monitoring performance impact, see sk43733
Optimizing the Rule Base

The Firewall Rule Base can have a big effect on gateway performance. We recommend that you make sure that the rules that are used the most are at the top of the Rule Base. For more about how to configure the Rule Base, see the *Firewall Administration Guide* for your version.

Monitoring Security Gateway Performance

sk33781 [http://supportcontent.checkpoint.com/solutions?id=sk33781](http://supportcontent.checkpoint.com/solutions?id=sk33781) explains how to monitor and troubleshoot gateway performance and includes these topics:

- Review the CPU load
- Review logs that are related to gateway performance
- Review memory load