Check Point
SOFTWARE TECHNOLOGIES LTD.

6 February 2018

CHECK POINT
IPS
R80.10

Best Practices

Check Point
SOFTWARE TECHNOLOGIES LTD
INFINITY

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 http://downloads.checkpoint.com/dc/download.htm?ID=59099.

To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

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 R80.10 Best Practices.

Revision History

Date	Description
06 February 2018	First release of this document

Contents

Introduction

In This Section:

R80.10 SmartConsole includes these default Threat Prevention profiles:

- Optimized Profile
- Basic Profile
- Strict Profile

Check Point recommends using the out of the box Optimized profile which provides the balance between excellent protection for common network products and protocols against recent or popular attacks and performance impact. However, your organization may have additional environments. Therefore, you may want to customize your profile to best fit your organization's network traffic. As the world of cyber-threats and your network needs are dynamic, you may need to tune and maintain IPS profiles and set protections to prevent/detect/ inactive or add exceptions.

One of the key elements to maintain an effective IPS policy is to monitor IPS events:

- Review IPS protections events as described in the guide.
- Identify where you need to tune IPS and exclude unique traffic protocols.

When reviewing the IPS policy, consider:

- **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 for real threats in your environment?
- **Performance** – The IPS blade uses deep inspections, and therefore additional gateway resources. Does the Security Gateway hardware (CPU and memory) fit the IPS blade policy?

The Optimized profile balances the trade-offs between these three measures and the corporate security, compliance and operational requirements.

Note - This guide does not explain how to mitigate malware attacks.

R80.10 Improvements

Check Point R80.10 IPS makes it easy to manage security for complex networks. Please review these new features in the *Check Point R80.10 Security Management Administration Guide:* http://downloads.checkpoint.com/dc/download.htm?ID=54842

- Separated Access Control and Threat Prevention Policy
- Multiple Threat Prevention profiles per gateway.
- IPS protections pre-defined tags.
- Automatically saves multiple IPS updates, allowing reverting to a previous IPS update without impacting other security configuration such as configuring profiles, rules, exceptions etc.

These new features help the administrator customize IPS profiles to fit the organization topology and create the Threat Prevention Rule Base accordingly.

Initial IPS Configuration Process

In This Section:

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 analyze each protection.

The Optimized Profile gives excellent security with good performance impact. This profile enables all protections that:

- Protect against relevant and important threats in commonly used products.
- Detect the attack in a reliable way.
- Have a moderate performance impact.

We recommend using the Optimized profile.

Updating Protections

When enabling IPS for the first time, the most recent IPS protections will be loaded. We recommend that you use a manual update the first time you update IPS and then automate the process.

To manually update the IPS protections:

1. In SmartConsole, click **Security Policies** > **Threat Prevention**.
2. In the **Threat Tools** section, click **Updates**.
3. In the IPS section, click **Update Now**.
4. Install the Threat Prevention policy.

Collecting and Analyzing the Initial IPS Events

We highly recommend that you use SmartEvent reports for a clear view of the protections that generate logs for ease of profile tuning. Please review the *Check Point R80.10 Logging and Monitoring Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=54830.

After the first IPS update, let it run for at least a week.

When IPS has generated logs, review the logs and use this guide to set the protection's mode to one of these:

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

Protections with high confidence can be set to Prevent as these protections were closely monitored and analyzed by Check Point.

Protections that generated events only for malicious traffic should be set to Prevent.

Use these indicators to identify events as malicious:

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

Protections that did not generate any events during the initial tuning can be set to Prevent mode.

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 IPS events. 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 the Check Point Support Center http://supportcenter.checkpoint.com.

Scheduling IPS Updates

After the initial IPS update, configure IPS to update automatically and on a regular basis:

To configure IPS scheduled updates:

1. In SmartConsole, go to the **Security Policies** page and select **Threat Prevention**.
2. In **Threat Prevention Policy** > **Threat Tools**, click **Updates**.
3. In the section for the applicable Software Blade, click **Schedule Update**.
   The **Scheduled Update** window opens.
4. Make sure **Enable IPS scheduled update** is selected.
5. Click **Configure**.
6. In the window that opens, set the **Update at tim**e and the **frequency** to best fit your business:
   - Daily
   - Every day
7. Click **OK**, and then click **OK** again.
8. Install the Threat Prevention policy.

Ongoing IPS Configuration Process

In This Section:

Collecting and Analyzing New Protections

After you successfully configure the initial IPS installation, most protections are deployed in Prevent mode. A few remain in Detect mode for an additional analysis.

However, new threats continuously emerge and the network traffic changes with new applications, services and protocols. We recommend that you run an IPS analysis periodically and review IPS events.

Newly downloaded protections will be in *staging mode*. Review these protections' events and change their mode from Staging to Detect.

Run an analysis on the new protections and determine if they can run in Prevent mode as performed earlier in Collecting and Analyzing the Initial IPS Events (on page 7).

IPS Software Blade Maintenance

In This Section:

IPS Updates

Check Point releases new IPS protections almost daily. Review the published Check Point IPS Security Update, which contains new and updated protections including protections against urgent and zero-day vulnerabilities. If the protections are crucial for your network, deploy them in Prevent mode. Consider the benefit of preventing active malware and attacks in the wild using Check Point IPS.

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 and it is often improved as part of software upgrades for Security Gateways. These upgrades give better IPS protections and performance.

User Communities

We encourage you to learn, share and inspire using our CheckMates platform:
http://community.checkpoint.com

Extending the IPS Configuration

In This Section:

Cloning the Profile

Make a copy of the Optimized Profile before you start the initial IPS tuning. 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 Optimized Profile:

1. Navigate to **Security policies** tab on the left panel, and then click **Threat Prevention Policy**.
2. Right-click the **Optimized Profile** and edit.
3. Click **OK**.
   A message appears and asks if you want to clone the profile.
4. Enter a new name for the cloned profile and click **OK**.

Configuring the Profile

Configure the setting of the profile to help the initial analysis of the IPS inspection with staging mode. The default action for the protections is Prevent, but staging mode protections run in Detect mode.

Configure new protections that are added to the profile to run in Prevent mode (during staging, these protections are set to Detect).

To configure the Profile:

1. Navigate to the **Security policies** tab on the left panel and click **Threat Prevention Policy**.
2. Right-click the profile and select the cloned profile you created.
3. Right-click the cloned profile and edit.
4. For **IPS Activation Mode**, select **Prevent**.
5. From the navigation tree, click **IPS** > **Updates**.
   The newly downloaded protections are set to **Active – According to profile settings**.
6. Set activation as **staging mode (Detect)**.
7. Click **OK**.

Configuring Inspection Settings Protections

Some Firewall Inspection Settings can be configured to help protect the network. For ease of use, we included their configuration in this document.

Email Inspection Settings

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 setting in **Security policies** > **Inspection settings** > **POP3/IMAP Security**, they apply to all hosts that are defined as mail servers according to 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. Navigate to **Security policies** > **Inspection settings**.
2. In the search 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. From the navigation tree, click **Advanced**.
6. In the **Protection Scope** area, click **Apply to selected mail servers**.
7. Click **View**.
   The **Select Servers** window opens and all mail servers are selected by default.
8. Change the 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**.
9. Click **OK**.

The POP3/IMAP Security inspection settings have a list of commands that IPS recognizes and inspects. The definitions of the POP3 commands apply to all IPS profiles. In the **Protections 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 applies to all profiles:

1. In the **Protection Details – POP3/IMAP Security configuration** window, click **Edit** for the POP3 Commands Definitions.
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 and click **Edit**.
   - 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 whose settings you want to edit.
2. Click **Edit**.
3. In the list of Known POP3 commands, clear any command that you do not want blocked.
4. When you finish editing the POP3/IMAP Security settings, click **OK** to save them and exit the **Protection Details – POP3/IMAP Security configuration** window.

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.
- 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 or unnecessary false-positives will disrupt network traffic.
- 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 advises customers to add a pattern to these protections as an immediate pre-emptive action against a new threat.

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. Navigate to **Security policies** > **Inspection settings** to see the protections area.
2. To apply the protection only to a defined set of Web servers, select **Apply to selected web servers**.
3. Click **Customize**.
4. To exclude a Web server from the protection, clear the server checkbox.
5. 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**.

6. To edit a Web server, select the Web server in the list and click **Edit**.

   TheCheck 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 protection's window, but enforcement of these configurations always depends on whether they are activated by the Web server's IPS profile.

Excluding Protections

The IPS profile may include protections that are not necessary for your network. You can exclude these IPS protections and improve network performance. For example, if an organization does not use VoIP services, exclude the IPS protection for VoIP traffic.

Exclude Protections by Tags

Each IPS protection is classified using tags such as:

- Type
- Vendor
- Product
- Threat year
- Protection type
- Vulnerability effect
- File type
- Protection protocol

You can exclude a group of protections using the relevant tags. You can do that either as part of the profile definition or directly from the IPS Protections view.

To exclude protection by tag using IPS Protections view:

1. On the left panel, navigate to **Security policies** and click **Threat Prevention Policy**.
2. Click **IPS Protections**.
3. From the filters on the right, select the tags whose protections you want to exclude.
4. Select the protections on the left and deactivate the protections.
5. Install the policy.

To exclude protection by tag using Threat Prevention profile definitions:

1. Extend the **IPS** TAB.
2. Select **Additional Activation**.
3. Select the tags whose protections you want to activate.
4. Select the tags whose protections you want to deactivate.
5. Install the policy.

Separate Profiles

The initial performance tuning focuses on a single IPS profile that is optimized for many situations. However, we recommend you create a different policy per network segment and gateway according to the protected assets and assign different profiles to each rule in the policy.

Examples of separate profiles:

- Gateways on the perimeter frequently use a different profile than gateways that protect data centers
- Different network segments protect different types of protocols, client/server, applications etc.

Performance Tuning

In This Section:

Overview

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

Monitoring Performance Impact

The performance impact is derived from the complexity of the protection and the amount of traffic inspected due to the nature of the traffic blend. In addition, you can measure the actual performance impact of protections as follows:

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

Run: `get_ips_statistics.sh`

Use the IPS Analyzer tool and collect information about the IPS Protections:

- For information on how to measure CPU time consumed by IPS protections, see sk43733 http://supportcontent.checkpoint.com/solutions?id=sk43733.
- For information on the IPS Analyzer tool, see sk110737 http://supportcontent.checkpoint.com/solutions?id=sk110737.

The Analyzer tool processes the statistic output and produces a clear HTML report based on that output. The report indicates which IPS protections are causing critical, high or medium load on the gateway. We recommend that you deactivate the critical performance protections or add exceptions as needed. You may contact the Check Point Support Center (https://supportcenter.checkpoint.com) to report these protections.

Configuring the Security Gateway Performance Settings

When the IPS Software Blade is enabled on a Security Gateway, it might affect network performance due to the need for deep packet inspection on the traffic.

The effect on network performance can be mitigated by correct appliance sizing. Customers who wish to make sure connections are not dropped due to high utilization but rather to exclude them from inspection, can configure the gateway to bypass IPS inspection when there is a heavy load on the server or appliance.

Note - Enabling this mode will impact security effectiveness on the system and is by no means recommended from a security perspective. Correct appliance size should be used to ensure high security effectiveness of the Check Point Threat Prevention solution.

To configure bypass under load on the gateway:

1. Navigate to **Gateways & Servers** and double-click the Security Gateway.
2. From the navigation tree, click **IPS**.
3. Select **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 – 75%
6. Click **OK**.
7. Install the Threat Prevention policy.