28 June 2017

IPS

Self Help Guide

R80.10

Check Point
SOFTWARE TECHNOLOGIES LTD.

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=54164.

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 IPS Self Help Guide.

Revision History

Date	Description
28 June 2017	First release of this document

Contents

Introduction

This document helps IPS users answer the most common questions that arise when dealing with IPS issues.

Customer Assistance

Check Point Support has a broad range of various services. Contact Check Point Support Center http://supportcenter.checkpoint.com and select the services that best suit your needs.

Requesting New Protections

IPS protections are developed based on the availability of technical information, severity and popularity of the affected product, and customer requests.

To cover a specific CVE, Check Point uses reliable and comprehensive information available internally and externally.

Every customer's request is addressed, and if possible, a new protection is released and published in the IPS package.

To request a new protection, please refer to Customer Assistance (on page 5) and provide detailed information.

False Positive

There are three scenarios in which a protection can be suspected as creating false positive (FP) logs:

- A protection blocks unsuspicious traffic, such as browsing a legitimate website or downloading a benign file.
- A protection creates an unusual amount of logs.
- A log in SmartConsole with a clear difference between the log and protection's description. For example, an Excel protection that blocks while browsing the internet without downloading any file.

If false positive logs were created:

1. Activate the relevant protection's capture traffic (packet capture) and configure the protection to Detect mode.

   If you suspect the traffic is legitimate, export the profile and refer to Customer Assistance (on page 5).
2. If a protection's confidence is high, the protection is reliable and most likely this is not an FP.

   If you believe it is an FP, please open a ticket to Support.

Update Failure

If you experience an update failure:

1. Make sure you followed the "Check Point update and online services migration to SHA-256 based certificates" procedure in sk103839 http://supportcontent.checkpoint.com/solutions?id=sk103839.
2. Make sure the client has internet connectivity and DNS is configured. For more information on IPS contracts, see sk44175 http://supportcontent.checkpoint.com/solutions?id=sk44175.
3. Verify license is valid:

   a) If the license expired, you need to contact account services.

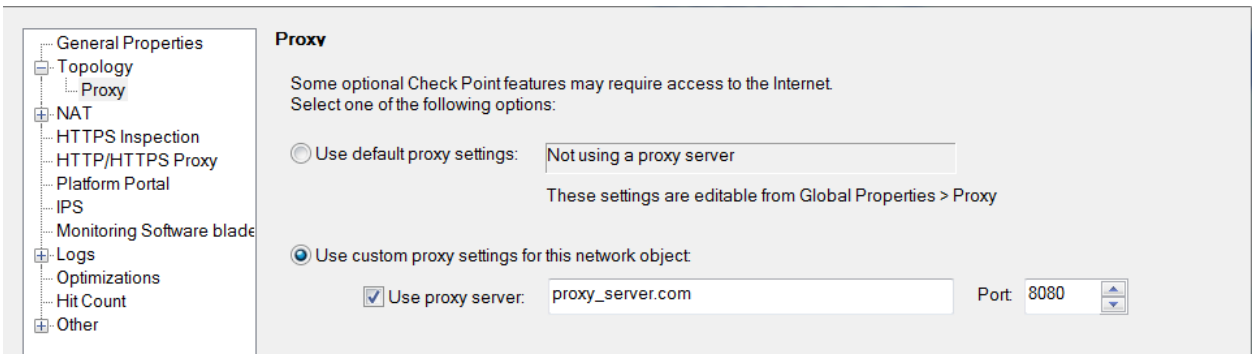
   b) If the license is valid but the firewall claims it is not, you need to contact account services to make sure there is no issue with the license.

   c) Clear the license cache.

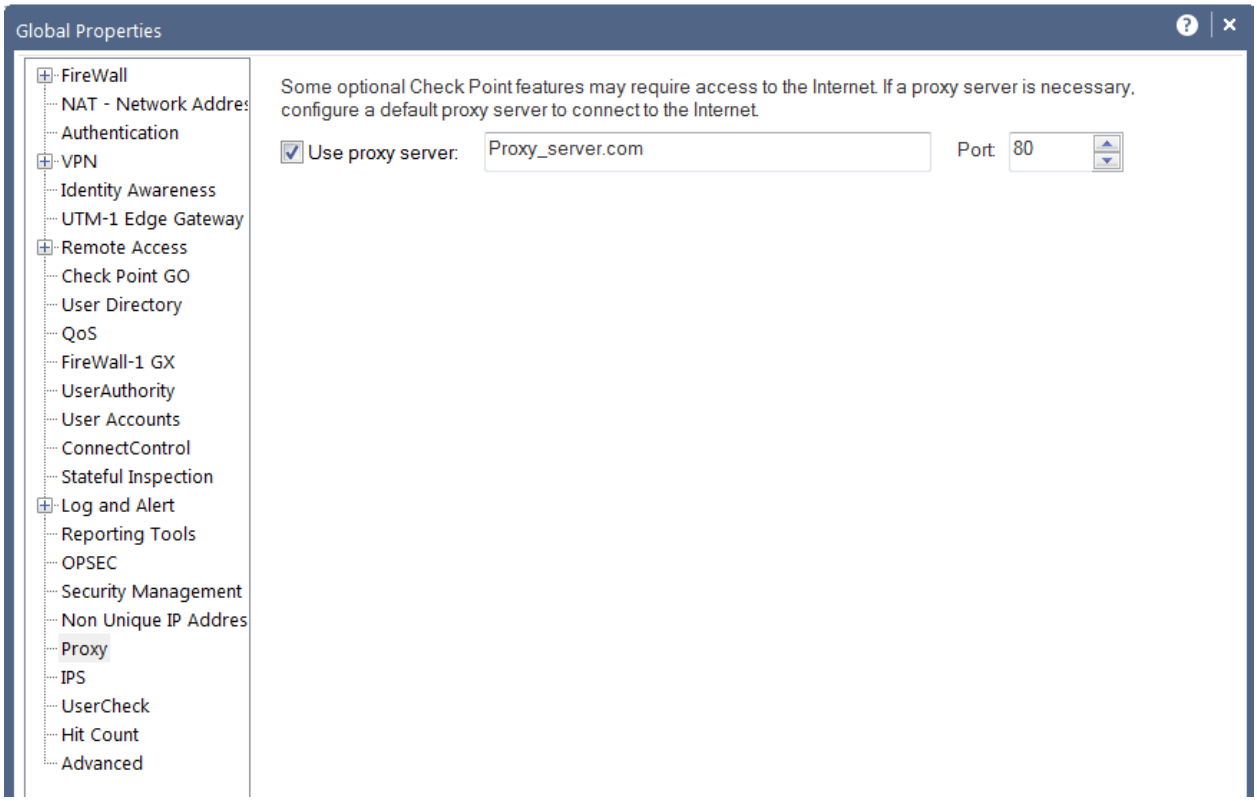
   - If you see "Contract entitlement check failed", refer to sk105757 http://supportcontent.checkpoint.com/solutions?id=sk105757.
   - For VSX Gateway, refer to sk105711 http://supportcontent.checkpoint.com/solutions?id=sk105711
   - For gateways where "Contract expired message" is shown twice, refer to sk102146 http://supportcontent.checkpoint.com/solutions?id=sk102146

4. Check if there is a proxy:

a) If there is a proxy in your environment and the firewall passes it to access the internet, configure it in SmartConsole > **Gateway object** > **Topology** > **Proxy (Gateway side)**:



b) If there is a proxy and the security management server passes it to access the internet, configure it in SmartConsole > **Global properties** > **Proxy (Management side)**:



c) If the proxy requires credentials, please follow the "How to enable Proxy Server credentials in SmartDashboard for supporting IPS and Application Control scheduled updates" procedure in sk89920 http://supportcontent.checkpoint.com/solutions?id=sk89920.

d) See sk112635 http://supportcontent.checkpoint.com/solutions?id=sk112635.

If the issue was not resolved, revert your machine to the last stable package and open a support ticket for further assistance.

No IPS Logs on SmartConsole

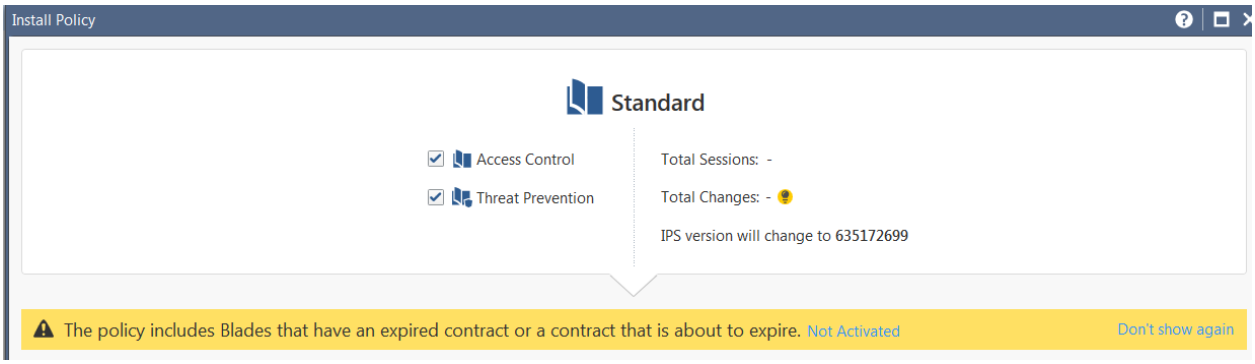
If there are no IPS logs on SmartConsole or you can only see very old protections logs:

1. Check connectivity issues.
2. Verify contract is valid:
   - Check your contract expiration date using Gaia CLISH command `cplic print -x`

     For more information, see sk44175 http://supportcontent.checkpoint.com/solutions?id=sk44175.
3. If your contract expired, contact your Check Point sales representative to renew.

Best Practice - Periodically check your contract validity and the expiration date.

Please notice expiration announcements during install policy:



Highly Loaded Gateway

Performance issues can have a number of causes. Review the Best Practices - Security Gateway Performance guidelines in sk98348 http://supportcontent.checkpoint.com/solutions?id=sk98348.
For an overview of the system load, use CPVIEW sk101878 http://supportcontent.checkpoint.com/solutions?id=sk101878.

If a gateway consistently runs at a high load, check the IPS profile:

1. We recommend that you use the **Optimized** profile. This profile does not include protections that have a critical impact on performance.
2. Disable all protections that are not relevant for your network traffic using tags functionality:
   - Products that are not used in your network.
   - Products that are used, but are already patched against specific vulnerabilities.

   To disable protections using tags functionality:
   i. Go to the Threat Prevention Profiles page.
   ii. In SmartConsole click on Security Policies -> Threat Prevention -> Policy.
   At the bottom, under Threat Tools, click on "Profiles".
   iii. Edit your Threat Prevention profile. In the profile editor, go to IPS->Additional Activation.
   iv. Select tags inside "protections to deactivate".
3. Edit your IPS profile and disable critical performance.
4. 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 CPU and which protections are causing a critical load on the gateway. We recommend that you deactivate the critical performance protections and refer to Customer Assistance (on page 5).

     The IPS Analyzer tool is supported on versions R77 and higher.

Protections Severity, Performance, and Confidence Levels

The following documents the severity level assigned by Check Point to the IPS protections:

Critical:

- Vulnerability may lead to remote code execution or administrative level compromise and may affect network infrastructure.
- The vulnerable software is from a major enterprise vendor. An exploit for the vulnerability exists.
- The vulnerability is unpatched at the time the protection is released.
- The vulnerable application or protocol is very common in corporate environments.

High:

- Vulnerability may lead to non-privileged remote code execution.
- Vulnerability may affect important company assets.
- Vulnerability can be easily exploited.
- The vulnerable software is significantly deployed in corporate environments.

Medium:

- Vulnerability may lead to denial of service.
- Vulnerability exists in general availability release of the product.
- Vulnerability exists in the default configuration of the product.
- The vulnerable software is partially deployed in some enterprises.

Low:

- Vulnerability may lead to information disclosure.
- Vulnerability effect can be easily contained or mitigated.
- Vulnerability exists only in customized configurations of the product.
- Exploit code and vulnerability details are not widely available.
- The vulnerability is already patched when the protection is released.
- There is no apparent way to create an effective exploit.
- The vulnerable software is only moderately deployed.

In addition, a protection severity level can be raised to fit one or more of the following parameters:

- Severity of the exploit according to its CVSS score.
- Severity rating of the vulnerability according to the vendor.
- Severity rating of the vulnerability according to the entity that discovered it.

Performance of Protections

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. For example, HTTP is a complex application requiring security analysis in comparison to TELENT which is a much more simple applications.

Very Low:

- All protections which do not cause any performance degradation.
- New protections are not added to this category without performance tests.

Low:

- All simple signatures over any protocol which have very unique traffic patterns.

Medium:

- ALL HTTP Client protections which use complex detection logic.
- All protocol parsers which perform protocol anomaly over PSL.
- All signatures executed on HTTP responses.

High:

- Protections which are executed on all ports.
- Performs extremely heavy and complex detection logic. For example, decoding of RC4 encryption.

Critical:

- Requires deep inspection of a significant portion of the traffic

Confidence of Protections

Confidence levels are the same across all Threat Prevention blades.

Low	Medium	High
Protections which can produce false positive events in **high** probability.	Protections which produce false positive events in **low** probability.	Protections which are reliable in detecting attacks and do not produce any false positives.