LICENSE

The MITRE Corporation (MITRE) hereby grants you a non-exclusive, royalty-free license to use Structured Threat Information Expression (STIX™) for research, development, and commercial purposes. Any copy you make for such purposes is authorized provided that you reproduce MITRE’s copyright designation and this license in any such copy.
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.

**Certifications**
For third party independent certification of Check Point products, see the Check Point Certifications page

**Check Point R80.20**
For more about this release, see the R80.20 home page

**Latest Version of this Document**
Open the latest version of this document in a Web browser

Download the latest version of this document in PDF format

**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 Threat Prevention R80.20 Administration Guide.

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 September 2021</td>
<td>Updated: Creating SNORT Rule Files (on page 114)</td>
</tr>
<tr>
<td></td>
<td>Unsupported SNORT Syntax (on page 116)</td>
</tr>
<tr>
<td>12 August 2021</td>
<td>General updates</td>
</tr>
<tr>
<td>06 June 2021</td>
<td>Updated Configuring the Security Gateway for UserCheck (on page 89)</td>
</tr>
<tr>
<td>02 April 2020</td>
<td>Updated: mgmt_cli install-policy (on page 126)</td>
</tr>
<tr>
<td>17 June 2019</td>
<td>Re-written: “SNORT Signature Support” chapter</td>
</tr>
<tr>
<td>13 May 2019</td>
<td>Removed: ips_export_import</td>
</tr>
<tr>
<td>26 February 2019</td>
<td>Updated: Anti-Virus (on page 16), Threat Emulation (on page 17), Threat Extraction (on page 18)</td>
</tr>
<tr>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>13 December 2018</td>
<td>Updated: Threat Emulation (on page 17)</td>
</tr>
<tr>
<td></td>
<td>Updated: Threat Prevention Policy Layers (on page 30)</td>
</tr>
<tr>
<td></td>
<td>Updated: Creating a New Policy Layer (on page 31)</td>
</tr>
<tr>
<td></td>
<td>Updated: IPS Updates (on page 45)</td>
</tr>
<tr>
<td></td>
<td>Updated: Exception Rules (on page 57)</td>
</tr>
<tr>
<td></td>
<td>Updated: Enabling MTA on the Security Gateway (on page 70)</td>
</tr>
<tr>
<td></td>
<td>Updated: ICAP Server (on page 76)</td>
</tr>
<tr>
<td></td>
<td>Updated: SNORT Signature Support (on page 107)</td>
</tr>
<tr>
<td>04 October 2018</td>
<td>Improved formatting and document layout for the HTML guide</td>
</tr>
<tr>
<td>26 September 2018</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>4</td>
</tr>
<tr>
<td>Terms</td>
<td>12</td>
</tr>
<tr>
<td>The Check Point Threat Prevention Solution</td>
<td>14</td>
</tr>
<tr>
<td>Threat Prevention Components</td>
<td>14</td>
</tr>
<tr>
<td>IPS</td>
<td>15</td>
</tr>
<tr>
<td>Anti-Bot</td>
<td>16</td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>16</td>
</tr>
<tr>
<td>SandBlast</td>
<td>17</td>
</tr>
<tr>
<td>Assigning Administrators for Threat Prevention</td>
<td>19</td>
</tr>
<tr>
<td>Analyzing Threats</td>
<td>19</td>
</tr>
<tr>
<td>The Threat Emulation Solution</td>
<td>20</td>
</tr>
<tr>
<td>ThreatCloud Emulation</td>
<td>20</td>
</tr>
<tr>
<td>Threat Emulation Analysis Locations</td>
<td>21</td>
</tr>
<tr>
<td>Local or Remote Emulation</td>
<td>21</td>
</tr>
<tr>
<td>Preparing for Local or Remote Emulation</td>
<td>22</td>
</tr>
<tr>
<td>Optimizing File Emulation</td>
<td>22</td>
</tr>
<tr>
<td>Selecting the Threat Emulation Deployment</td>
<td>23</td>
</tr>
<tr>
<td>Inline Deployments (Prevent and Ask)</td>
<td>23</td>
</tr>
<tr>
<td>Monitor Deployments</td>
<td>23</td>
</tr>
<tr>
<td>Threat Emulation Deployments with a Mail Transfer Agent</td>
<td>24</td>
</tr>
<tr>
<td>Out-of-the-Box Protection from Threats</td>
<td>25</td>
</tr>
<tr>
<td>Getting Quickly Up and Running with the Threat Prevention Policy</td>
<td>25</td>
</tr>
<tr>
<td>Enabling the Threat Prevention Software Blades</td>
<td>25</td>
</tr>
<tr>
<td>Enabling the IPS Software Blade</td>
<td>25</td>
</tr>
<tr>
<td>Enabling the Anti-Bot Software Blade</td>
<td>26</td>
</tr>
<tr>
<td>Enabling the Anti-Virus Software Blade</td>
<td>26</td>
</tr>
<tr>
<td>Enabling SandBlast Threat Emulation Software Blade</td>
<td>26</td>
</tr>
<tr>
<td>Enabling the SandBlast Threat Extraction Blade</td>
<td>27</td>
</tr>
<tr>
<td>Installing the Threat Prevention Policy</td>
<td>27</td>
</tr>
<tr>
<td>Predefined Rule</td>
<td>28</td>
</tr>
<tr>
<td>The Threat Prevention Policy</td>
<td>29</td>
</tr>
<tr>
<td>Workflow for Creating a Threat Prevention Policy</td>
<td>29</td>
</tr>
<tr>
<td>To Learn More about Policy Packages</td>
<td>29</td>
</tr>
<tr>
<td>Threat Prevention Policy Layers</td>
<td>30</td>
</tr>
<tr>
<td>Action Enforcement in Multiple-Layered Security Policies</td>
<td>30</td>
</tr>
<tr>
<td>Creating a New Policy Layer</td>
<td>31</td>
</tr>
<tr>
<td>To Learn More about Permission Profiles</td>
<td>32</td>
</tr>
<tr>
<td>Threat Prevention Layers in Pre-R80 Gateways</td>
<td>32</td>
</tr>
<tr>
<td>Threat Prevention Rule Base</td>
<td>32</td>
</tr>
<tr>
<td>Parts of the Rules</td>
<td>32</td>
</tr>
<tr>
<td>Number (No.)</td>
<td>33</td>
</tr>
<tr>
<td>Name</td>
<td>33</td>
</tr>
<tr>
<td>Protected Scope</td>
<td>33</td>
</tr>
<tr>
<td>Protection</td>
<td>34</td>
</tr>
<tr>
<td>Action</td>
<td>35</td>
</tr>
<tr>
<td>Threat Prevention Track Options</td>
<td>35</td>
</tr>
<tr>
<td>Install On</td>
<td>35</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Threat Prevention Profiles</td>
<td>36</td>
</tr>
<tr>
<td>Introducing Profiles</td>
<td>36</td>
</tr>
<tr>
<td>Optimized Protection Profile Settings</td>
<td>37</td>
</tr>
<tr>
<td>Profiles Pane</td>
<td>37</td>
</tr>
<tr>
<td>Creating Profiles</td>
<td>38</td>
</tr>
<tr>
<td>Cloning Profiles</td>
<td>39</td>
</tr>
<tr>
<td>Editing Profiles</td>
<td>39</td>
</tr>
<tr>
<td>Deleting Threat Prevention Profiles</td>
<td>39</td>
</tr>
<tr>
<td>Showing Changes to a Threat Prevention Profile</td>
<td>40</td>
</tr>
<tr>
<td>Creating Threat Prevention Rules</td>
<td>41</td>
</tr>
<tr>
<td>Configuring Mail Settings</td>
<td>41</td>
</tr>
<tr>
<td>General</td>
<td>41</td>
</tr>
<tr>
<td>Use Case</td>
<td>42</td>
</tr>
<tr>
<td>Exceptions</td>
<td>43</td>
</tr>
<tr>
<td>MIME Nesting</td>
<td>44</td>
</tr>
<tr>
<td>Configuring Inspection of Links Inside Mail</td>
<td>44</td>
</tr>
<tr>
<td>Configuring IPS Profile Settings</td>
<td>45</td>
</tr>
<tr>
<td>Additional Activation Fields</td>
<td>45</td>
</tr>
<tr>
<td>Updates</td>
<td>45</td>
</tr>
<tr>
<td>Pre-R80 Settings</td>
<td>46</td>
</tr>
<tr>
<td>Configuring Anti-Bot Settings</td>
<td>46</td>
</tr>
<tr>
<td>Blocking Bots</td>
<td>47</td>
</tr>
<tr>
<td>Monitoring Bot Activity</td>
<td>47</td>
</tr>
<tr>
<td>Configuring Anti-Virus Settings</td>
<td>48</td>
</tr>
<tr>
<td>Enabling Archive Scanning</td>
<td>49</td>
</tr>
<tr>
<td>Blocking Viruses</td>
<td>50</td>
</tr>
<tr>
<td>Configuring Threat Emulation Settings</td>
<td>50</td>
</tr>
<tr>
<td>Threat Emulation General Settings</td>
<td>51</td>
</tr>
<tr>
<td>Emulation Environment</td>
<td>52</td>
</tr>
<tr>
<td>Advanced Threat Emulation Settings</td>
<td>52</td>
</tr>
<tr>
<td>Configuring Threat Extraction Settings</td>
<td>53</td>
</tr>
<tr>
<td>Threat Extraction General Settings</td>
<td>53</td>
</tr>
<tr>
<td>Threat Extraction Advanced Settings</td>
<td>55</td>
</tr>
<tr>
<td>Configuring a Malware DNS Trap</td>
<td>55</td>
</tr>
<tr>
<td>SandBlast Use Cases</td>
<td>56</td>
</tr>
<tr>
<td>Exception Rules</td>
<td>57</td>
</tr>
<tr>
<td>Disabling a Protection on One Server</td>
<td>58</td>
</tr>
<tr>
<td>Blade Exceptions</td>
<td>59</td>
</tr>
<tr>
<td>Creating Exceptions from IPS Protections</td>
<td>59</td>
</tr>
<tr>
<td>Exception Groups</td>
<td>59</td>
</tr>
<tr>
<td>Creating Exception Groups</td>
<td>60</td>
</tr>
<tr>
<td>Adding Exceptions to Exception Groups</td>
<td>60</td>
</tr>
<tr>
<td>Adding Exception Groups to the Rule Base</td>
<td>60</td>
</tr>
<tr>
<td>Creating Exceptions from Logs or Events</td>
<td>61</td>
</tr>
<tr>
<td>Configuring Threat Emulation on the Gateway</td>
<td>62</td>
</tr>
<tr>
<td>Using Local or Remote Emulation</td>
<td>62</td>
</tr>
<tr>
<td>Changing the Analysis Location</td>
<td>63</td>
</tr>
<tr>
<td>Setting the Activation Mode</td>
<td>64</td>
</tr>
<tr>
<td>Optimizing System Resources</td>
<td>64</td>
</tr>
<tr>
<td>Managing Images for Emulation</td>
<td>65</td>
</tr>
<tr>
<td>Configuring Threat Extraction on the Gateway</td>
<td>66</td>
</tr>
</tbody>
</table>
Monitoring Threat Prevention

Log Sessions
Using the Log View in SmartConsole
Viewing Threat Prevention Rule Logs
Predefined Queries
Creating Custom Queries
Selecting Criteria from Grid Columns
Manually Entering Query Criteria
Selecting Query Fields
Packet Capture
Advanced Forensics Details
Threat Analysis in the Logs & Monitor View
Views
Reports

Configuring Advanced Threat Prevention Settings
Threat Prevention Engine Settings
Fail Mode
Check Point Online Web Service
Connection Unification
Configuring Anti-Bot Whitelist
Selecting Emulation File Types
Configuring Advanced Engine Settings for Threat Extraction

SNORT Signature Support
Importing SNORT Protection Rules to the Security Management Server
Deleting SNORT Protection Rules from the Security Management Server
Importing SNORT Protection Rules to the Multi-Domain Server
Deleting SNORT Protection Rules from the Multi-Domain Server
Action on SNORT Protection Rules
Alternative Methods to add and delete SNORT Protection Rules
Creating SNORT Rule Files
Unsupported SNORT Syntax

Optimizing IPS
Managing Performance Impact
Tuning Protections
Enhancing System Performance

Using the Whitelist
Adding a File to the Whitelist

Threat Indicator Settings
Example of a CSV Indicator File
Example of a STIX 1.0 XML Indicator File
Configuring Indicators in SmartConsole

Using Anti-Bot and Anti-Virus with VSX
Using Threat Extraction with VSX
Threat Prevention CLI Commands
mgmt_cli install-policy
te_add_file
tecli
Managing IPS gateways - CLI

Configuring Advanced Threat Emulation Settings
Updating Threat Emulation
Updating Threat Emulation Images
Terms

**Action**
What a Software Blade does to traffic that matches a rule.

**Affinity**
The assignment of a specified CoreXL Firewall instance, VSX Virtual System, interface, user space process, or IRQ to one or more specified CPU cores.

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

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

**Ask**
UserCheck rule action that blocks traffic and files and shows a UserCheck message. The user can agree to allow the activity.

**Detect**
UserCheck rule action that allows traffic and files to enter the internal network and logs them.

**Event**
A record of a security or network incident that is based on one or more logs, and on a customizable set of rules that are defined in the Event Policy.

**Indicator**
Pattern of relevant observable malicious activity in an operational cyber domain, with relevant information on how to interpret it and how to handle it.

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

**Malware Database**
The Check Point database of commonly used signatures, URLs, and their related reputations, installed on a Security Gateway and used by the ThreatSpect engine.

**Observable**
An event or a stateful property that can be observed in an operational cyber domain.

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

**Prevent**
UserCheck rule action that blocks traffic and files and can show a UserCheck message.

**Rule**
A set of traffic parameters and other conditions that cause specified actions to be taken for a communication session.

**Security Gateway**
A computer that runs Check Point software to inspect traffic and enforces Security Policies for connected network resources.

**Security Management Server**
A computer that runs Check Point software to manage the objects and policies in Check Point environment.

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

**SmartConsole**
A Check Point GUI application used to manage Security Policies, monitor products and events, install updates, provision new devices and appliances, and manage a multi-domain environment and each domain.
STIX
Structured Threat Information eXpression. A language that describes cyber threat information in a standardized and structured way.

Threat Emulation
Protects against new malware. Virtual computers open files and are monitored for unusual and malicious behavior.

Threat Emulation Private Cloud Appliance
A Check Point appliance that is certified to support the Threat Emulation Software Blade.

ThreatCloud IntelliStore
Threat intelligence marketplace where you can select intelligence feeds (in addition to ThreatCloud feeds) from a range of security vendors that specialize in cyber intelligence. ThreatCloud translates these feeds into protections which run on Security Gateways.

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

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

Traffic
The flow of data between network devices.

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

In This Section:
Threat Prevention Components..................................................................................................................14
Assigning Administrators for Threat Prevention......................................................................................19
Analyzing Threats .......................................................................................................................................19

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

- IPS - A complete IPS cyber security solution, for comprehensive protection against malicious and unwanted network traffic, which focuses on application and server vulnerabilities, as well as in-the-wild attacks by exploit kits and malicious attackers.

- Anti-Bot - Post-infection detection of bots on hosts. Prevents bot damages by blocking bot C&C (Command and Control) communications. The Anti-Bot Software Blade is continuously updated from ThreatCloud, a collaborative network to fight cybercrime. Anti-Bot discovers infections by correlating multiple detection methods.

- Anti-Virus - Pre-infection detection and blocking of malware at the gateway. The Anti-Virus Software Blade is continuously updated from ThreatCloud. It detects and blocks malware by correlating multiple detection engines before users are affected.

- SandBlast - Protection against infections from undiscovered exploits, zero-day and targeted attacks:
  - Threat Emulation - This innovative solution quickly inspects files and runs them in a virtual sandbox to discover malicious behavior. Discovered malware is prevented from entering the network. The ThreatCloud Emulation service reports to the ThreatCloud and automatically shares the newly identified threat information with other Check Point customers.
  - Threat Extraction - Protection against incoming malicious content. The Threat Extraction capability removes exploitable content, including active content and embedded objects, reconstructs files to eliminate potential threats, and promptly delivers sanitized content to users to maintain business flow. To remove possible threats, the Threat Extraction blade creates a safe copy of the file, while the Threat Emulation Software Blade inspects the original file for potential threats.

Each Software Blade gives unique network protections. When combined, they supply a strong Threat Prevention solution. Data from malicious attacks are shared between the Threat Prevention Software Blades and help to keep your network safe. For example, the signatures from threats that Threat Emulation identifies are added to the ThreatCloud for use by the other Threat Prevention blades.
IPS

The IPS Software Blade delivers complete and proactive intrusion prevention. It delivers 1,000s of signatures, behavioral and preemptive protections. It gives another layer of security on top of Check Point firewall technology. IPS protects both clients and servers, and lets you control the network usage of certain applications. The 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.

Elements of Protection

IPS protection includes:

- 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.

Check Point constantly updates the library of protections to stay ahead of emerging 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
- Integrated management with SmartConsole.
- Easy navigation from business-level overview to a packet capture for a single attack.
- #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 in SmartConsole, to let you take immediate action based on IPS information.

For example, some malware can be downloaded by a user unknowingly when he browses to a legitimate web site, also known as a drive-by-download. This malware can exploit a browser vulnerability to create 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.
Anti-Bot

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

When a bot infects a computer, it:

- Takes control of the computer and neutralizes its Anti-Virus defenses. It is not easy to find bots on your computer; they hide and change how they look to Anti-Virus software.
- Connects to a C&C (Command and Control center) for instructions from cyber criminals. The cyber criminals, or bot herders, can remotely control it and instruct it to do illegal activities without your knowledge. Your computer can do one or more of these activities:
  - Steal data (personal, financial, intellectual property, organizational)
  - Send spam
  - Attack resources (Denial of Service Attacks)
  - Consume network bandwidth and reduce productivity

One bot can often create multiple threats. Bots are frequently used as part of Advanced Persistent Threats (APTs) where cyber criminals try to damage individuals or organizations.

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

The Anti-Bot Software Blade uses these procedures to identify bot infected computers:

- **Identify the C&C addresses used by criminals to control bots**
  These web sites are constantly changing and new sites are added on an hourly basis. Bots can attempt to connect to thousands of potentially dangerous sites. It is a challenge to know which sites are legitimate and which are not.

- **Identify the communication patterns used by each botnet family**
  These communication fingerprints are different for each family and can be used to identify a botnet family. Research is done for each botnet family to identify the unique language that it uses. There are thousands of existing different botnet families and new ones are constantly emerging.

- **Identify bot behavior**
  Identify specified actions for a bot such as, when the computer sends spam or participates in DoS attacks.

After the discovery of bot infected machines, the Anti-Bot Software Blade blocks outbound communication to C&C sites based on the Rule Base. This neutralizes the threat and makes sure that no sensitive information is sent out.

Anti-Virus

Malware is a major threat to network operations that has become increasingly dangerous and sophisticated. Examples include worms, blended threats [combinations of malicious code and vulnerabilities for infection and dissemination] and trojans.

The Anti-Virus Software Blade scans incoming and outgoing files to detect and prevent these threats, and provides pre-infection protection from malware contained in these files. The Anti-Virus blade is also supported by the Threat Prevention API (on page 136).
The Anti-Virus Software Blade:

- Identifies malware in the organization using the ThreatSpect engine and ThreatCloud repository:
  - Prevents malware infections from incoming malicious files types (Word, Excel, PowerPoint, PDF, etc.) in real-time. Incoming files are classified on the gateway and the result is then sent to the ThreatCloud repository for comparison against known malicious files, with almost no impact on performance.
  - Prevents malware download from the internet by preventing access to sites that are known to be connected to malware. Accessed URLs are checked by the gateway caching mechanisms or sent to the ThreatCloud repository to determine if they are permissible or not. If not, the attempt is stopped before any damage can take place.
  - Uses the ThreatCloud repository to receive binary signature updates and query the repository for URL reputation and Anti-Virus classification.

SandBlast

Cyber-threats continue to multiply and now it is easier than ever for criminals to create new malware that can easily bypass existing protections. On a daily basis, these criminals can change the malware signature and make it virtually impossible for signature-based products to protect networks against infection. To get ahead, enterprises need a multi-faceted prevention strategy that combines proactive protection that eliminates threats before they reach users. With Check Point’s Threat Emulation and Threat Extraction technologies, SandBlast provides zero-day protection against unknown threats that cannot be identified by signature-based technologies.

Threat Emulation

Threat Emulation gives networks the necessary protection against unknown threats in web downloads and e-mail attachments. The Threat Emulation engine picks up malware at the exploit phase, before it enters the network. It quickly quarantines and runs the files in a virtual sandbox, which imitates a standard operating system, to discover malicious behavior before hackers can apply evasion techniques to bypass the sandbox.

Threat Emulation receives files through these methods of delivery:

- E-mail attachments transferred using the SMTP or SMTPS protocols.
- Web downloads.
- Files sent to Threat Extraction through the Threat Prevention API (on page 136).

When emulation is done on a file:

- The file is opened on more than one virtual computer with different operating system environments.
- The virtual computers are closely monitored for unusual and malicious behavior, such as an attempt to change registry keys or run an unauthorized process.
- Any malicious behavior is immediately logged and you can use Prevent mode to block the file from the internal network.
- The cryptographic hash of a new malicious file is saved to a database and the internal network is protected from that malware.
- After the threat is caught, a signature is created for the new (previously unknown) malware which turns it into a known and documented malware. The new attack information is
automatically shared with Check Point ThreatCloud to block future occurrences of similar threats at the gateway.

If the file is found not to be malicious, you can download the file after the emulation is complete.

Learn more about Threat Emulation [on page 20].

**Threat Extraction**

Threat Extraction is supported on R77.30 and higher.

The Threat Extraction blade extracts potentially malicious content from files before they enter the corporate network. To remove possible threats, the Threat Extraction does one of these two actions:

- Creates a safe copy of the file by converting it to PDF, or
- Extracts exploitable content out of the file.

Threat Extraction receives files through these methods of delivery:

- E-mail attachments received through the Mail transfer Agent [on page 53].
- Files sent to Threat Extraction through the Threat Prevention API [on page 136].

Threat Extraction delivers the reconstructed file to users and blocks access to the original suspicious version, while Threat Emulation analyzes the file in the background. This way, users have immediate access to content, and can be confident they are protected from the most advanced malware and zero-day threats.

Threat Emulation runs in parallel to Threat Extraction for version R80.10 and higher.

Here are examples for exploitable content in Microsoft Office Suite Applications and PDF files:

- Queries to databases where the query contains a password in the clear
- Embedded objects
- Macros and JavaScript code that can be exploited to propagate viruses
- Hyperlinks to sensitive information
- Custom properties with sensitive information
- Automatic saves that keep archives of deleted data
- Sensitive document statistics such as owner, creation and modification dates
- Summary properties
- PDF documents with:
  - Actions such as launch, sound, or movie URIs
  - JavaScript actions that run code in the reader’s Java interpreter
  - Submit actions that transmit the values of selected fields in a form to a specified URL
  - Incremental updates that keep earlier versions of the document
  - Document statistics that show creation and modification dates and changes to hyperlinks
  - Summarized lists of properties

Before you enable the Threat Extraction blade, you must deploy the gateway as a Mail Transfer Agent [on page 70].
Assigning Administrators for Threat Prevention

You can control the administrator Threat Prevention permissions with a customized Permission Profile. The customized profile can have different Read/Write permissions for Threat Prevention policy, settings, profiles and protections.

Analyzing Threats

Networks today are more exposed to cyber-threats than ever. This creates a challenge for organizations in understanding the security threats and assessing damage.

SmartConsole helps the security administrator find the cause of cyber-threats, and remediate the network.

The Logs & Monitor > Logs view presents the threats as logs.

The other views in the Logs & Monitor view combine logs into meaningful security events. For example, malicious activity that occurred on a host in the network in a selected time interval (the last hour, day, week or month). They also show pre- and post-infections statistics.

You can create rich and customizable views and reports for log and event monitoring, which inform key stakeholders about security activities. For each log or event, you can see a lot of useful information from the ThreatWiki and IPS Advisories about the malware, the virus or the attack.
The Threat Emulation Solution

In This Section:

- ThreatCloud Emulation..........................................................................................................................20
- Threat Emulation Analysis Locations.....................................................................................................21
- Optimizing File Emulation......................................................................................................................22
- Selecting the Threat Emulation Deployment...........................................................................................23

ThreatCloud Emulation

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

Sample ThreatCloud Emulation Workflow

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

Sample ThreatCloud Deployment

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internet and external networks</td>
</tr>
<tr>
<td>2</td>
<td>Perimeter Security Gateway</td>
</tr>
<tr>
<td>3</td>
<td>Check Point ThreatCloud servers</td>
</tr>
<tr>
<td>4</td>
<td>Computers and servers in the internal network</td>
</tr>
</tbody>
</table>
Threat Emulation Analysis Locations

You can choose a location for the emulation analysis that best meets the requirements of your company.

- **ThreatCloud** - You can send all files to the Check Point ThreatCloud for emulation. Network bandwidth is used to send the files and there is a minimal performance impact on the Security Gateway.
- **Threat Emulation Private Cloud Appliance (Emulation appliance) in the Internal network** - You can use an Emulation appliance to run emulation on the files.

Local or Remote Emulation

You can install an Emulation appliance in the internal network.

**Sample Workflow for Emulation Appliance in a Local Deployment**

1. The Emulation appliance receives the traffic, and aggregates the files.
2. The Emulation appliance compares the cryptographic hash of the file with the database.
   - The file is already in the database, no more emulation is necessary.
   - If the file is not in the database, the virtual computers in the Emulation appliance run full emulation on the file.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internet and external networks</td>
</tr>
<tr>
<td>2</td>
<td>Perimeter Security Gateway</td>
</tr>
<tr>
<td>3</td>
<td>Threat Emulation Private Cloud Appliance</td>
</tr>
<tr>
<td>4</td>
<td>Computers and servers in the internal network</td>
</tr>
</tbody>
</table>

**Sample Workflow for Emulation Appliance in a Remote Deployment**

1. The Security Gateway aggregates the files, and the files are sent to the Emulation appliance.
2. The Emulation appliance compares the cryptographic hash of the file with the database.
   - The file is already in the database, no more emulation is necessary.
- If the file is not in the database, the virtual computers in the Emulation appliance run full emulation on the file.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internet and external networks</td>
</tr>
<tr>
<td>2</td>
<td>Perimeter Security Gateway</td>
</tr>
<tr>
<td>3</td>
<td>Threat Emulation Private Cloud Appliance</td>
</tr>
<tr>
<td>4</td>
<td>Computers and servers in the internal network</td>
</tr>
</tbody>
</table>

**Preparing for Local or Remote Emulation**

Prepare the network and Emulation appliance for a Local or Remote deployment in the internal network.

1. Open SmartConsole.
2. Create the network object for the Emulation appliance.
3. If you are running emulation on HTTPS traffic, configure the settings for HTTPS Inspection (on page 144).
4. Make sure that the traffic is sent to the appliance according to the deployment:
   - Local Emulation - The Emulation appliance receives the traffic. The appliance can be configured for traffic the same as a Security Gateway.
   - Remote Emulation - The traffic is routed to the Emulation appliance.

**Optimizing File Emulation**

Files have unique cryptographic hashes, these file hashes are stored in a database after emulation is complete. Before emulation is run on a file, the appliance compares the file hash to the database:

- If the hash is not in the database, the file is sent for full emulation
- If the hash is in the database, then it is not necessary to run additional emulation on the file

This database helps to optimize emulation and give better network performance.
Selecting the Threat Emulation Deployment

What are my options to send traffic for emulation?

- **Inline** - Traffic is sent for emulation before it is allowed to enter the internal network. You can use the Threat Prevention policy to block malware.
- **SPAN/TAP** - You can use a mirror or TAP port to duplicate network traffic. Files are sent to the computer in the internal network. If Threat Emulation discovers that a file contains malware, the appropriate log action is done.
- **MTA (Mail Transfer Agent) [on page 70]** - SMTP traffic goes to the Security Gateway, and is sent for emulation. The MTA acts as a mail proxy, and manages the SMTP connection with the source. The MTA sends email files to emulation after it closes the SMTP connection. When the file emulation is completed, the emails are sent to the mail server in the internal network.

I want to use the Prevent action and be able to block malicious files, what are my deployment options?

- **ThreatCloud** - Files are sent to the ThreatCloud for emulation. When the emulation is complete, ThreatCloud sends a notification to the Security Gateway that the files are safe. Then they go to computers in the internal network.
- **Threat Emulation Private Cloud Appliance with inline deployment** - The files are kept in the Emulation appliance and after emulation, safe files go to the computer in the internal network.

This table summarizes how Threat Emulation sends traffic for emulation:

<table>
<thead>
<tr>
<th></th>
<th>Block Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inline</td>
<td>Yes</td>
</tr>
<tr>
<td>SPAN/TAP</td>
<td>No</td>
</tr>
<tr>
<td>MTA</td>
<td>Recommended with Prevent action for emails</td>
</tr>
</tbody>
</table>

**Inline Deployments (Prevent and Ask)**

Use the Prevent or Ask UserCheck action to quarantine a malicious file [on page 88].

**Sample Inline Emulation Workflow (Prevent Action)**

1. The ThreatCloud or Emulation appliance gets a file from the Security Gateway.
2. Emulation is run on the file.
   - The file is safe, and it is sent to the computer in the internal network.
   - If the file contains malware, it is quarantined and logged.

**Monitor Deployments**

**Sample Monitor Emulation Workflow**

1. The ThreatCloud or Emulation appliance gets a copy of a file from the Security Gateway. The original file goes to the computer in the internal network.
2. Emulation is run on the file.
   - The file is safe, no other action is done
If the file is identified as malware, it is logged according to the Track action of the Threat Prevention rule.

**Threat Emulation Deployments with a Mail Transfer Agent**

SMTP traffic goes to the Security Gateway, and is sent for emulation. The MTA acts as a mail proxy, and manages the SMTP connection with the source. The MTA sends email files to emulation after it closes the SMTP connection. When the file emulation is completed, the emails are sent to the mail server in the internal network.

For more information on how to work with the Mail Transfer Agent, see Mail Transfer Agent [on page 70].
Out-of-the-Box Protection from Threats

In This Section:
- Getting Quickly Up and Running with the Threat Prevention Policy..........................25
- Enabling the Threat Prevention Software Blades......................................................25
- Installing the Threat Prevention Policy......................................................................27
- Predefined Rule............................................................................................................28

Getting Quickly Up and Running with the Threat Prevention Policy

You can configure Threat Prevention to give the exact level of protection that you need, but you can also configure it to provide protection right out of the box.

To get quickly up and running with Threat Prevention:
1. Enable the Threat Prevention blades on the gateway.
2. Install Policy.

After you enable the blades and install the policy, this rule is generated:

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

Notes:
- The Optimized (on page 37) profile is installed by default.
- The Protection/Site (on page 34) column is used only for protection exceptions.

Enabling the Threat Prevention Software Blades

Enabling the IPS Software Blade

Enable the IPS Software Blade on the Security Gateway.

To enable the IPS Software Blade:
1. In the Gateways & Servers view, double-click the gateway object. The General Properties window opens.
2. In the General Properties > Network Security tab, click IPS.
3. Follow the steps in the wizard that opens.
4. Click OK.
5. Click OK in the General Properties window.
6. **Install Policy** [on page 27].

## Enabling the Anti-Bot Software Blade

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

1. In the **Gateways & Servers** view, double-click the gateway object.  
   The **General Properties** window of the gateway opens.
2. From the **Network Security** tab, select **Anti-Bot**.  
   The **Anti-Bot and Anti-Virus First Time Activation** window opens.
3. Select an activation mode option:
   - **According to the Anti-Bot and Anti-Virus policy** - Enable the Anti-Bot Software Blade and use the Anti-Bot settings of the Threat Prevention profile in the Threat Prevention policy.
   - **Detect only** - Packets are allowed, but the traffic is logged according to the settings in the Threat Prevention Rule Base.
4. Click **OK**.
5. **Install Policy** [on page 27].

## Enabling the Anti-Virus Software Blade

Enable the Anti-Virus Software Blade on a Security Gateway.

**To enable the Anti-Virus Software Blade:**

1. In the **Gateways & Servers** view, double-click the gateway object.  
   The **General Properties** window of the gateway opens.
2. From the **Network Security** tab, click **Anti-Bot**.  
   The **Anti-Bot and Anti-Virus First Time Activation** window opens.
3. Select one of the activation mode options:
   - **According to the Anti-Bot and Anti-Virus policy** - Enable the Anti-Virus Software Blade and use the Anti-Virus settings of the Threat Prevention profile in the Threat Prevention policy.
   - **Detect only** - Packets are allowed, but the traffic is logged according to the settings in the Threat Prevention Rule Base.
4. Click **OK**
5. **Install Policy** [on page 27].

## Enabling SandBlast Threat Emulation Software Blade

**To enable the Threat Emulation Blade:**

1. In the **Gateways & Servers** view, double-click the Security Gateway object.  
   The **Gateway Properties** window opens.
2. From the **Network Security** tab, select **SandBlast Threat Emulation**.  
   The **Threat Emulation First Time Configuration Wizard** opens and shows the **Emulation Location** page.
3. Select the **Emulation Location**.
4. Click **Next**.  
   The **Summary** page opens.
5. Click **Finish** to enable Threat Emulation and close the First Time Configuration Wizard.

6. Click **OK**.

   The **Gateway Properties** window closes.

7. Install Policy [on page 27].

---

**Using Cloud Emulation**

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

**Best Practice** - For ThreatCloud emulation, it is necessary that the Security Gateway connects to the Internet. Make sure that the DNS and proxy settings are configured correctly in **Global Properties**.

---

**Enabling the SandBlast Threat Extraction Blade**

**To enable the Threat Extraction Blade:**

1. In the **Gateways & Servers** view, double-click the gateway object.
   The **General Properties** window of the gateway opens.

2. Go to the **Network Security** tab, and select **Threat Extraction**.
   The **Threat Extraction First Time Activation Wizard** opens:
   
   a) Configure the **Domain** and **Next Hop**.
   
   b) Click **Next**.
   
   c) Click **Finish**.

3. Enable the gateway as a **Mail Transfer Agent (MTA)** [on page 70].
   **Note** - In a ClusterXL High Availability environment, do this once for the cluster object.

---

**Configuring LDAP**

If you use LDAP for user authentication, you must activate User Directory for Security Gateways.

**To activate User Directory:**

1. Open **SmartConsole > Global Properties**.


3. Click **OK**.

---

**Installing the Threat Prevention Policy**

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

1. From the Global toolbar, click Install Policy.
   The Install Policy window opens showing the installation targets (Security Gateways).

2. Select Threat Prevention.

3. Select Install Mode:
   - **Install on each selected gateway independently** - Install the policy on the selected Security Gateways without reference to the other targets. A failure to install on one Security Gateway does not affect policy installation on other gateways.
     
     If the gateway is a member of a cluster, install the policy on all the members. The Security Management Server makes sure that it can install the policy on all the members before it installs the policy on one of them. If the policy cannot be installed on one of the members, policy installation fails for all of them.
   
   - **Install on all selected gateways, if it fails do not install on gateways of the same version** - Install the policy on all installation targets. If the policy fails to install on one of the Security Gateways, the policy is not installed on other targets of the same version.

4. Click OK.

**Predefined Rule**

When you enable one of the Threat Prevention Software Blades, a predefined rule is added to the Rule Base. The rule defines that all traffic for all network objects, regardless of who opened the connection, (the protected scope [on page 33] value equals any) is inspected for all protections according to the Optimized profile [on page 37]. By default, logs are generated and the rule is installed on all Security Gateways that use a Threat Prevention Software Blade.

The result of this rule (according to the Optimized profile) is that:

- When an attack meets the below criteria, the protections are set to Prevent mode:
  - **Confidence Level** - Medium or above
  - **Performance Impact** - Medium or above
  - **Severity** - Medium or above

- When an attack meets the below criteria, the protections are set to Detect mode:
  - **Confidence Level** - Low
  - **Performance Impact** - Medium or above
  - **Severity** - Medium or above

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

You can add more exceptions that prevent or detect specified protections or have different tracking settings.
The Threat Prevention Policy

In This Section:

Workflow for Creating a Threat Prevention Policy ..........................................................29
To Learn More about Policy Packages ..............................................................................29
Threat Prevention Policy Layers .........................................................................................30
Threat Prevention Layers in Pre-R80 Gateways ..............................................................32
Threat Prevention Rule Base ..............................................................................................32
Parts of the Rules ...............................................................................................................32

Workflow for Creating a Threat Prevention Policy

Threat Prevention lets you customize profiles that meet the needs of your organization.

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

When you define a new Threat Prevention profile, you can create a Threat Prevention Policy which activates only the protections that you need and prevents only the attacks that most threaten your network.

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

2. Update the IPS database and Malware database with the latest protections.
3. Optional: Create Policy Packages.
   Note - For each Policy Layer, configure a Threat Prevention Rule Base with the Threat Prevention profile as the Action of the rule.
5. Install the Threat Prevention policy.

To Learn More about Policy Packages

To learn more about Policy Packages, see the R80.20 Security Management Administration Guide
Threat Prevention Policy Layers

You can create a Threat Prevention Rule Base with multiple Policy Layers. Policy Layers help you organize your Rule Base to best suit your organizational needs. You can divide the Policy Layers by Software Blades, services or networks. Each Policy Layer calculates its action separately from the other Layers. In case of one Layer in the policy package, the rule enforced is the first rule matched. In case of multiple Layers:

- If a connection matches a rule in only one Layer, then the action enforced is the action in that rule.
- When a connection matches rules in more than one Layer, the gateway enforces the strictest action and settings.

**Important** - When Threat Emulation and Threat Extraction run in MTA mode, the gateway enforces the action of the first rule matched. It does not necessarily enforce the strictest rule.

Action Enforcement in Multiple-Layered Security Policies

These examples show which action the gateway enforces when a connection matches rules in more than one Policy Layers.

**Example 1**

<table>
<thead>
<tr>
<th></th>
<th>Data Center Layer</th>
<th>Corporate LAN Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule matched</td>
<td>Rule 3</td>
<td>Rule 1</td>
</tr>
<tr>
<td>Profile action</td>
<td>Prevent</td>
<td>Detect</td>
</tr>
</tbody>
</table>

**Enforced action:** Prevent

**Example 2**

<table>
<thead>
<tr>
<th></th>
<th>Data Center Layer</th>
<th>Corporate LAN Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule matched</td>
<td>Rule 3</td>
<td>Rule 1</td>
</tr>
<tr>
<td>Profile action</td>
<td>Prevent</td>
<td>Detect</td>
</tr>
<tr>
<td>Exception for protection X</td>
<td>Inactive</td>
<td>-</td>
</tr>
</tbody>
</table>

**Enforced action for protection X:** Detect

**Example 3**

<table>
<thead>
<tr>
<th></th>
<th>Data Center Layer</th>
<th>Corporate LAN Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule matched</td>
<td>Rule 3</td>
<td>Rule 1</td>
</tr>
<tr>
<td>Profile action</td>
<td>Prevent</td>
<td>Detect</td>
</tr>
<tr>
<td>Override for protection X</td>
<td>Detect</td>
<td>-</td>
</tr>
<tr>
<td>Exception for protection X</td>
<td>Inactive</td>
<td>-</td>
</tr>
</tbody>
</table>

Exception is prior to override and profile action. Therefore, the action for the Data Center Layer is Inactive.

The action for the Corporate LAN Layer is Detect.
**Enforced action for protection X:** Detect.

### Example 4

<table>
<thead>
<tr>
<th></th>
<th>Data Center Layer</th>
<th>Corporate LAN Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule matched</td>
<td>Rule 3</td>
<td>Rule 1</td>
</tr>
<tr>
<td>Profile action</td>
<td>Deep Scan all files</td>
<td>Process specific file type families: Inspect doc files and Drop rtf files.</td>
</tr>
</tbody>
</table>

**Enforced action:** Deep Scan doc files and Drop rtf files.

### Example 5

MIME nesting level and Maximum archive scanning time

**The strictest action is:**

Block combined with the minimum nesting level/scanning time, or Allow combined with the maximum nesting level/scanning time, or If both Block and Allow are matched, the enforced action is Block.

### Example 6

UserCheck

<table>
<thead>
<tr>
<th></th>
<th>HR Layer</th>
<th>Finance Layer</th>
<th>Data Center Layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule matched</td>
<td>Rule 3</td>
<td>Rule 1</td>
<td>Rule 4</td>
</tr>
<tr>
<td>Profile action</td>
<td>Detect</td>
<td>Prevent</td>
<td>Prevent</td>
</tr>
<tr>
<td>Configured page</td>
<td>Page A</td>
<td>Page B</td>
<td>Page C</td>
</tr>
</tbody>
</table>

The first Layer with the strictest action is enforced.

**Enforced Action:** Prevent with UserCheck Page B.

### Creating a New Policy Layer

This section explains how to create a new Threat Prevention Policy Layer. You can configure reuse of Threat Prevention Policy Layers in different Policy Packages, and set different administrator permissions per Threat Prevention Layer.

**To create a new Threat Prevention Layer:**

1. In SmartConsole, go to **Threat Prevention**.
2. Right-click **Policy** and select **Edit Policy**.
3. In the **General** tab, go to **Threat Prevention** and click the + sign.
4. Select **New Layer**.
   
   The **New Threat Prevention Layer** window opens
5. Enter the Layer Name.
6. Optional: In the **General** tab, in the **Sharing** area, you can configure reuse of the layer in different policy packages. Select **Multiple policies and rules can use this layer**.
Note - you cannot share the first Threat Prevention layer because it contains the MTA and ICAP rules. If this layer is shared with other policy packages then there can be conflicting MTA and ICAP rules in the same policy package.

7. In the Permissions tab, select the permission profiles that can edit this layer.

   Note - There is no need to add permission profiles that are configured to edit all layers.

8. Click OK.

To Learn More about Permission Profiles

To learn more about configuration of permission profiles, see the R80.20 Security Management Administration Guide

Threat Prevention Layers in Pre-R80 Gateways

In pre-R80 versions, the IPS Software Blade was not part of the Threat Prevention Policy, and was managed separately. In R80.xx versions, the IPS Software Blade is integrated into the Threat Prevention Policy.

When you upgrade SmartConsole to R80.xx from earlier versions, with some Security Gateways upgraded to R80.xx, and other Security Gateways remaining in previous versions:

- For pre-R80 gateways with IPS and Threat Prevention Software Blades enabled, the policy is split into two parallel layers: IPS and Threat Prevention.
  To see which Security Gateway enforces which IPS profile, look at the Install On column in the IPS Layer.

- R80.xx gateways are managed separately, based on the R80 or higher Policy Layers.

   Best Practice - For better performance, we recommend that you use the Optimized profile when you upgrade to R80 or higher from earlier versions.

Threat Prevention Rule Base

Each Threat Prevention Layer contains a Rule Base. The Rule Base determines how the system inspects connections for malware.

The Threat Prevention rules use the Malware database and network objects. Security Gateways that have Identity Awareness enabled can also use Access Role objects as the Protected Scope in a rule. The Access Role objects let you easily make rules for individuals or different groups of users.

There are no implied rules in this Rule Base, traffic is allowed or not allowed based on how you configure the Rule Base. For example, A rule that is set to the Prevent action, blocks activity and communication for that malware.

Parts of the Rules

The columns of a rule define the traffic that it matches and what is done to that traffic.
**Number (No.)**

The sequence of rules is important because the first rule that matches traffic according to a protected scope (on page 33) and profile is applied.

For example, if rules 1 and 2 share the same protected scope and a profile in rule 1 is set to detect protections with a medium confidence level and the profile in rule 2 is set to prevent protections with a medium confidence level, then protections with a medium confidence level will be detected based on rule 1.

**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 and click OK.

**Protected Scope**

Threat Prevention rules include a Protected Scope parameter. Threat Prevention inspects traffic to and/or from all objects specified in the Protected Scope, even when the specified object did not open the connection. This is an important difference from the Source object in Firewall rules, which defines the object that opens a connection.

For example, the Protected Scope includes a Network Object named MyWebServer. Threat Prevention inspects all files sent to MyWebServer for malware threats, even if MyWebServer did not open the connection.

Protected Scope objects can be:

- Network objects, such as Security Gateways, clusters, servers, networks, IP ranges, and so on
- Network object groups
- IP address ranges
- Roles
- Zones

You can set the Protected Scope parameter to Any. This option lets Threat Prevention inspect traffic based on the direction and interface type as defined by the Profile assigned to the applicable rule. By default, the predefined Optimized Rule sets the Protection Scope to Any.

**Traffic Direction and Interface Type Settings**

You can configure the traffic direction and Security Gateway interface types that send files to Threat Prevention for inspection. You do this in the Protected Scope section of the Anti-Virus or Threat Emulation Settings window. The options are:

- **Inspect incoming files from:**
  - Sends only incoming files from the specified interface type for inspection. Outgoing files are not inspected. Select an interface type from the list:
    - **External** - Inspect incoming files from external interfaces. Files from the DMZ and internal interfaces are not inspected.
    - **External and DMZ** - Inspect incoming files from external and DMZ interfaces. Files from internal interfaces are not inspected.
    - **All** - Inspect all incoming files from all interface types.
• **Inspect incoming and outgoing files** - Sends all incoming and outgoing files for inspection. When you select the **Any** option in the **Protected Scope** section of a rule, the traffic direction and interface type are defined by the **Profile** assigned to that rule. If you add objects to the Protected Scope in a rule, files that match these objects are inspected for all connections.

**Using Protected Scope with SPAN and TAP Configurations**

The default global parameter for SPAN and TAP configuration is set to **inspect all**. You can use these commands to configure the Security Gateway to use the Protected Scope settings for SPAN and TAP with Threat Emulation.

- `fw ctl set int` - Changes current **Protected Scope** settings for SPAN and TAP, does not survive reboot
- `Change $FWDIR/module/fwkern.conf` - This changes the settings after reboot.

Run these commands to set the SPAN port to use the Policy instead of the global default setting (**inspect all**):

```
# fw ctl set int te_handle_span_port_interfaces_according_to_topolgy 1
# echo “te_handle_span_port_interfaces_according_to_topolgy=1” >> $FWDIR/module/fwkern.conf
```

**Limitations and Troubleshooting**

- If no topology is defined for the Security Gateway interfaces, all traffic is inspected or sent for emulation.
- When you upgrade from R76 and earlier, the **Inspect incoming files** option is set to **All** by default.
- When the topology of the interfaces is defined and you are using SPAN or TAP modes, it is possible that some of the connections are not defined correctly.

**Protection**

The **Protection/Site** column shows the protections for the Threat Prevention policy.

- For **rules**, this field is always set to **n/a** and cannot be changed. Protections for Rule Base rules are defined in the configured profile [in the Action column].
- For **rule exceptions** and **exception groups**, this field can be set to one or more specified protections.

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

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the navigation tree, select a **Policy Layer**.
3. Right-click the rule and select **New Exception**.
   
   An exception sub-rule is added to the policy.
4. Right-click the **Protection/Site** cell and select **Add new items**.
5. From the list of Anti-Bot, Anti-Virus, or IPS protections, click the add button of protections to add to the exception.
   
   The protections are added to the exception sub-rule.
6. **Install Policy**.
To search for a malware in the Protection viewer:
1. Put your mouse in the Protection/Site column and click the plus sign to open the Protection viewer.
2. Select the protection category.
3. Enter the malware name in the search field.

Action
Action refers to how traffic is inspected.
- For rules, this is defined by the profile. The profile contains the configuration options for different confidence levels and performance impact (on page 37).
- For rule exceptions and exception groups, the action can be set to Prevent or Detect.

To select a profile for a rule:
1. Click in the Action column.
2. Select an existing profile from the list, create a new profile, or edit the existing profile.

Threat Prevention Track Options
- None - Do not generate an alert.
- Alert - Generate a log and run 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 the Menu > Global Properties > Log and Alert > Alerts.
- Packet Capture - Adds raw IPS, Anti-Virus, Anti-Bot, Threat Emulation and Threat Extraction packet data to the Threat Prevention logs. Only blocked packets are added.

Install On
Select the gateways on which to install the rule. The default is All [all gateways that have a Threat Prevention blade 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. If you right-click a column in the table, you can add more columns to the table from the list that shows.
Threat Prevention Profiles

In This Section:

- Introducing Profiles ................................................................. 36
- Optimized Protection Profile Settings ...................................... 37
- Profiles Pane ........................................................................... 37
- Creating Profiles .................................................................... 38
- Cloning Profiles ...................................................................... 39
- Editing Profiles ...................................................................... 39
- Deleting Threat Prevention Profiles ....................................... 39
- Showing Changes to a Threat Prevention Profile ................... 40

Introducing Profiles

Check Point Threat Prevention provides instant protection based on pre-defined Threat Prevention Profiles. You can also configure a custom Threat Prevention profile to give the exact level of protection that the organization needs.

When you install a Threat Prevention policy on the Security Gateways, they immediately begin to enforce IPS protection on network traffic.

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

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

A Threat Prevention profile applies to one or more of the Threat Prevention Software Blades: IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction.

A profile is a set of configurations based on:

- Activation settings (prevent, detect, or inactive) for each confidence level of protections that the ThreatSpect engine analyzes
- IPS Settings
- Anti-Bot Settings
- Anti-Virus Settings
- Threat Emulation Settings
- Threat Extraction Settings
- Indicator configuration
- Malware DNS Trap configuration
- Links inside mail configuration
Without profiles, it would be necessary to configure separate rules for different activation settings and confidence levels. With profiles, you get customization and efficiency.

SmartConsole includes these default Threat Prevention profiles:

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

### Optimized Protection Profile Settings

The **Optimized** profile is activated by default, because it gives excellent security with good gateway performance.

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

<table>
<thead>
<tr>
<th>Goal</th>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply settings to all the Threat Prevention Software Blades</td>
<td>Blades Activation</td>
<td>Activate the profile for IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction.</td>
</tr>
<tr>
<td>Do not have a critical effect on performance</td>
<td>Performance impact</td>
<td>Activate protections that have a Medium or lower effect on performance.</td>
</tr>
<tr>
<td>Protect against important threats</td>
<td>Severity</td>
<td>Protect against threats with a severity of Medium or above.</td>
</tr>
<tr>
<td>Reduce false-positives</td>
<td>Confidence</td>
<td>Set to Prevent the protections with an attack confidence of Medium or High. Set to Detect the protections with a confidence of Low.</td>
</tr>
</tbody>
</table>

### Profiles Pane

The pane shows a list of profiles that have been created, their confidence levels, and performance impact settings. The Profiles pane contains these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Creates a new profile.</td>
</tr>
<tr>
<td>View</td>
<td>Shows an existing profile.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies an existing profile.</td>
</tr>
<tr>
<td>Clone</td>
<td>Creates a copy of an existing profile.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes a profile.</td>
</tr>
<tr>
<td>Where Used</td>
<td>Shows you reference information for the profile.</td>
</tr>
<tr>
<td>Search</td>
<td>Searches for a profile.</td>
</tr>
<tr>
<td>Last Modified</td>
<td>Shows who last modified the selected profile, when and on which client.</td>
</tr>
</tbody>
</table>
Performance Impact
Performance impact is how much a protection affects the gateway performance. Some activated protections might cause issues with connectivity or performance. You can set protections to not be prevented or detected if they have a higher impact on gateway performance.

There are three options:
- High or lower
- Medium or lower
- Low

Severity
Severity of the threat. Probable damage of a successful attack to your environment.

There are three degrees of severity:
- Low or above
- Medium or above
- High or above

Activation Settings
- Prevent - The protection action that blocks identified virus or bot traffic from passing through the gateway. It also logs the traffic, or tracks it, according to configured settings in the Rule Base.
- Detect - The protection action that allows identified virus or bot traffic to pass through the gateway. It logs the traffic, or tracks it, according to configured settings in the Rule Base.
- Inactive - The protection action that deactivates a protection.

Confidence Level
The confidence level is how confident the Software Blade is that recognized attacks are actually virus or bot traffic. Some attack types are more subtle than others and legitimate traffic can sometimes be mistakenly recognized as a threat. The confidence level value shows how well protections can correctly recognize a specified attack.

Creating Profiles
You can choose from multiple pre-configured Profiles, but not change them. You can create a new profile or clone a profile. When you create a new profile, it includes all the Threat Prevention Software Blades by default.

When HTTPS inspection is enabled on the Security Gateway, Threat Emulation, Anti-Bot, and Anti-Virus can analyze the applicable HTTPS traffic.

To create a new Threat Prevention profile:
1. In SmartConsole, select Security Policies > Threat Prevention.
2. From the Threat Tools section, click Profiles.
   The Profiles page opens.
3. Right-click a profile and select New.
4. Configure the settings for the profile.
5. Click OK.
6. Install the Threat Prevention policy.

## Cloning Profiles

You can create a clone of a selected profile and then make changes. You cannot change the out-of-the-box profiles: Basic, Optimized, and Strict.

**To clone a Threat Prevention profile:**

1. In SmartConsole, select Security Policies > Threat Prevention.
2. From the Threat Tools section, click Profiles.
   The Profiles page opens.
3. Right-click the profile and select Clone.
4. The Name field shows the name of the copied profile plus _copy.
5. Rename the profile.
6. Click OK.
7. Publish the changes.

## Editing Profiles

You can change the settings of the Threat Prevention profile according to your requirements.

**To edit a profile:**

1. In SmartConsole, select Security Policies > Threat Prevention.
2. From the Threat Tools section, click Profiles.
   The Profiles page opens.
3. Right-click the profile and select Edit.

## Deleting Threat Prevention Profiles

You can delete a profile, but you cannot delete the default Threat Prevention profiles.

**To delete a profile:**

1. In SmartConsole, select Security Policies > Threat Prevention.
2. From the Threat Tools section, click Profiles.
   The Profiles page opens.
3. Right-click the profile, and click Delete.
   A window opens and shows a confirmation message.
4. Click Yes.
   If the profile is used by another object, you cannot delete it. The error message is shown in the Tasks window.
5. Install Policy.
To show the objects that use a profile:
1. From the Profiles page, select the profile.
   The Summary
2. From the Where Used section in the Summary tab, click Where Used.
   The Where Used window opens and shows the profile.
3. Right click the rule and select View in policy.

Showing Changes to a Threat Prevention Profile

You can show the Audit log and see changes that were made to a Threat Prevention profile.

To show the Audit log for a Threat Prevention profile:
1. In SmartConsole, click Logs & Monitor.
2. Click the Audit tab, or press CTRL + T and click Open Audit Logs View.
3. In Enter search query, enter the name of the profile.
4. To refine the search:
   a) Right-click the Object Type column heading and select Add Filter.
   b) Enter Threat Prevention Profile.
   c) Click the filter to add it to the search.
   d) Click OK.
      The search results are filtered to Threat Prevention profiles.
5. To see more information about the changes to a profile, double-click the Audit log.
Creating Threat Prevention Rules

In This Section:

- Configuring Mail Settings ................................................................. 41
- Configuring IPS Profile Settings ...................................................... 45
- Configuring Anti-Bot Settings ............................................................ 46
- Configuring Anti-Virus Settings ......................................................... 48
- Configuring Threat Emulation Settings .............................................. 50
- Configuring Threat Extraction Settings ............................................. 53
- Configuring a Malware DNS Trap ...................................................... 55
- SandBlast Use Cases ......................................................................... 56
- Exception Rules .................................................................................. 57
- Exception Groups ................................................................................ 59

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

- The **Threat Prevention** page shows the rules and exceptions for the Threat Prevention policy. The rules set the Threat profiles for the network objects or locations defined as a protected scope.

Click the **Add Rule** button to get started.

- You can configure the Threat Prevention settings in the Threat Prevention profile for the specified rule.
- To learn about bots and protections, look through the ThreatWiki.

**Best Practice** - Disable a rule when you work on it. Enable the rule when you want to use it. Disabled rules do not affect the performance of the Gateway. To disable a rule, right click in the **No.** column of the rule and select **Disable**.

Configuring Mail Settings

**General**

**General**

- **Emulate emails for malicious content (requires Threat Emulation)** - When this option and the Threat Emulation blade are enabled, the Threat Emulation blade scans SMTP traffic.

- **Scan emails for viruses (requires Anti-Virus)** - When this option and the Anti-Virus blade are enabled, the Anti-Virus blade scans SMTP traffic.

- **Extract potentially malicious attachments (requires Threat Extraction)** - When this option and the Threat Extraction blade are enabled, the Threat Extraction blade scans SMTP traffic.

**Malicious Email Policy on MTA Gateways**

In this section you can decide whether to block or allow an email which was found malicious.
If you allow the email, you can select any or all of these options:

- **Remove attachments and links** - This option is selected by default. You can replace a link or an attachment found malicious with a neutralized version of the links and attachments. The neutralized email version is sent to the recipient with a customizable template. Click **Configure** to edit the template:
  - **Malicious Attachments** - Replaced by a neutralized txt file. You can customize the message which the user receives. Click **Insert Field** to add more file-related information to your message [for example: file name or MD5 hash].
  - **Failed to Scan Attachments** - If the scanning of the attachment fails and fail mode is set to fail-close, the attachment is replaced with a txt attachment. If fail mode is set to fail-open, the original attachment is allowed. Click **Insert Field** to add more file-related information to your message [for example: file name or MD5 hash].
  - **Malicious Links** - Replaced by a neutralized link. Click **Insert Field** to add more link-related information to your message, for example, neutralized url.
  - **Add an X-Header to the email** - Tag the email found malicious with an X-Header. The X-Header format is: “X-Check Point-verdict: <verdict>; confidence: <confidence>“. For example: “X-Check Point-verdict: malicious; confidence: high”. With this option, you can configure the MTA Next Hop to quarantine all emails with a specific X-Header.
  - **Add a prefix to the email subject** - Adds a prefix to the subject of an email found malicious. For example: you can add a warning message that the email is malicious. Click **Configure** to edit the prefix.
  - **Add customized text to the email body** - This option adds a section at the beginning of the email body, based on a customizable template, with an optional placeholder for the verdicts of the links and attachments found malicious or failed to be scanned. The links are given in their neutralized versions, and attachments are only given by file names. Click **Configure** to edit the template.

**Send a copy to the following list** - This option is available both if you allow or block the malicious email. With this option, the original email [with the malicious attachments and links] is attached to a new email, which contains: the verdict list with the neutralized links and attachment file names, and the SMTP envelope information. You can configure the email content on the gateway. You can use this option for research purposes. For example: The Incident Response Team needs to inquire the emails received in the organization for improved security and protection.

**Use Case**

The configuration in the Mail page lets you block or allow malicious emails. However, you do not want to configure a global decision regarding all malicious emails. You prefer to make a decision per each email separately, on a case-by-case basis. For that purpose, you need to create a system in which Threat Emulation allows the emails, but does not send them to the recipient right away. Instead, it puts them in a container where you can check them and then decide whether to block or allow them.

**To configure external quarantine for malicious emails:**

In SmartConsole:

1. Enable MTA on your gateway [on page 70].
2. Clone the Profile you wish to configure and rename it.
3. In the new profile, go to Mail > General > Malicious Email Policy on MTA Gateways and select **Allow the email**.
4. Clear **Remove attachments and links**.
5. Select **Add an X-Header** to the email.

   **Note** - When you add an X-Header to the email, the rest of the email is kept in the email’s original form. The other options: **Remove attachments and links**, **Add a prefix to the email subject** and **Add customized text to the email body**, change the email, and therefore must be cleared.
6. Click **OK**.
7. **Install Policy**.

   In the Next Hop:
1. Configure a rule which quarantines all emails which were marked with an X-Header by the MTA.

   You can now see the emails in the Next Hop in their original forms and examine them. After you examine the emails in the Next Hop, you can decide whether to allow or block them.

**Exceptions**

You can exclude specific email addresses from the Threat Emulation or Threat Extraction protections.

**To exclude emails from Threat Emulation:**

1. In **Emulation Exceptions**, click **Configure**.
2. In the **Recipients** section, click the + button to enter one or more emails.
   
   Emails and attachments that are sent to these recipients will not be sent for emulation.
3. In the **Senders** section, click the + button to enter one or more emails.
   
   Emails and attachments that are received from these senders will not be sent for emulation.

   **Note** - You can use a wildcard character to exclude more than one email address from a domain.
4. Click **OK**.

   **Note** - If you want to do emulation on outgoing emails, make sure that you set the Protected Scope to **Inspect incoming and outgoing files**.

**To exclude emails from Threat Extraction:**

1. In **Extraction Exclusion/Inclusion**:
   
   - Select **Scan all emails** (selected by default) and click **Exceptions**.
     
     Click the + button to exclude specific recipients, users, groups or senders.
   
   - Select **Scan mail only for specific users or groups** and click **Configure**.
     
     Click the Add button to exclude specific User Groups, Recipients or Senders.
2. Click **OK**.

**Examples:**

A **user** is an object that can contain an email address with other details.

A **group** is an AD group or an LDAP group of users

A **recipient** is an email address only.

Signed Email Attachments

Signed emails are not encrypted, but the mail contents are signed to authenticate the sender. If the received email differs from the email that was sent, the recipient gets a warning, and the digital signature is no longer valid.

Clean replaces the original attachment with an attachment cleaned of threats, or converts the attachment to PDF form. Both actions invalidate the digital signature. If the attachment does not include active content, the mail remains unmodified and the digital signature valid.

Allow does not change the email. The digital signature remains valid. Select this option to prevent altering digital signatures.

MIME Nesting

This is an optional configuration. In this section, you can configure the maximum number of MIME nesting levels to be scanned (A nesting level is an email within an email). These settings are the same for Anti-Virus, Threat Emulation and Threat Extraction.

- Maximum MIME nesting is (levels) - Set the maximum number of levels in the email which the engine scans.
- When nesting level is exceeded (action on file) - If there are more MIME nested levels than the configured amount, select to Block or Allow the email.

Configuring Inspection of Links Inside Mail

Inspection of Links Inside Mail scans URL links in email messages. Inspection of Links Inside Mail is on by default, and is supported with the Anti-Virus, Anti-Bot and Threat Emulation blades. Inspection of Links Inside Mail scans incoming mail with the Anti-Virus Software Blade and outgoing mail with Anti-Bot Software Blade. For the Threat Emulation blade, only URL links to files are scanned. You must enable MTA for inspection of Links Inside Mail to work with the Threat Emulation blade.

On this page, you can configure these settings:

- Inspect first <number> (B) of email messages
- Inspect first <number> URLs in email messages

To turn off Inspection of Links Inside Mail:

2. Right-click on a Links Inside Mail protection, and select Inactive Selected.
   
   Note - For each Software Blade (Anti-Bot and Anti-Virus) you must turn off the Links Inside Mail separately.

To turn on Inspection of Links Inside Mail:

2. Right-click on a Links Inside Mail protection, and select one of these -
   - Prevent Selected
   - Detect Selected
Configuring IPS Profile Settings

To configure IPS settings for a Threat Prevention profile:

1. In SmartConsole, select Security Policies > Threat Prevention.
2. From the Threat Tools section, click Profiles.
   The Profiles page opens.
3. Right-click the profile, and click Edit.
4. From the navigation tree, click IPS > Additional Activation.
5. Configure the customized protections for the profile [on page 45].
6. From the navigation tree, click IPS > Updates.
7. Configure the settings for newly downloaded IPS protections [on page 45].
8. If you import IPS profiles from a pre-R80 deployment:
   a) From the navigation tree, click IPS > Pre-R80 Settings.
   b) Activate the applicable Client and Server protections [on page 46].
   c) Configure the IPS protection categories to exclude from this profile [on page 46].
   Note - These categories are different from the protections in the Additional Activation page.
9. Click OK.
10. Install Policy.

Additional Activation Fields

For additional granularity, in the Additional Activation section of the Profile configuration window, you can select IPS protections to activate and to deactivate. The IPS protections are arranged into tags (categories) such as Product, Vendor, Threat Year, and others, for the ease of search. The gateways enforce activated protections, and do not enforce deactivated protections, regardless of the general profile protection settings.

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

These categories only filter out or add protections that comply with the activation mode thresholds (Confidence, Severity, Performance).
For example, if a protection is inactive because of its Performance rating, it is not enabled even if its category is in **Protections to activate**.

Updates

There are numerous protections available in IPS. It takes time to become familiar with those that are relevant to your environment. Some are easily configured for basic security and can be safely activated automatically.
In the Threat Prevention profile, you can configure an updates policy for IPS protections that were newly updated. You can do this with the IPS > Updates page in the Profiles navigation tree. Select one of these settings for Newly Updated Protections:

- **Active - According to profile settings** - Selected by default. Protections are activated according to the settings in the General page of the Profile. This is the Check Point recommended configuration.
  
  **Set activation as staging mode** - Newly updated protections remain in staging mode until you change their configuration. The default action for protections in staging mode is Detect. You can change the action manually in the IPS Protections page (on page 84). Click Configure to exclude specific protections from staging mode.

- **Inactive** - Newly updated protections are not activated

**Best Practice** - In the beginning, allow IPS to activate protections based on the IPS policy. During this time, you can analyze the alerts that IPS generates and how it handles network traffic, while you minimize the impact on the flow of traffic. Then you can manually change the protection settings to suit your needs.

**Pre-R80 Settings**

The Pre-R80 Settings are relevant for the pre-R80 gateways only.

**Protects Activation**

**Activate protections of the following types:**

- **Client Protections** - Select to activate protections that protect only clients (for example, personal computers).

- **Server Protections** - Select to activate protections that protect only servers.
  
  If a network has only clients or only servers, you can enhance gateway performance by deactivation of protections. If you select Client Protections and Server Protections, all protections are activated, except for those that are:
  
  - Excluded by the options selected here
  - Application Controls or Engine Settings
  - Defined as Performance Impact — Critical

**Excluded Protections Categories**

**Do not activate protections of the following categories** - The IPS protection categories you select here are not automatically activated. They are excluded from the Threat Prevention policy rule that has this profile in the action of the Rule Base.

**Configuring Anti-Bot Settings**

Here you can configure the Anti-Bot UserCheck Settings:

- **Prevent** - Select the UserCheck message that opens for a Prevent action

- **Ask** - Select the UserCheck message that opens for an Ask action
Blocking Bots

To block bots in your organization, install this default Threat Policy rule that uses the Optimized profile, or create a new rule.

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

To block bots in your organization:

1. In SmartConsole, click **Gateways & Servers**.
2. Enable the **Anti-Bot** Software Blade on the Gateways that protect your organization. For each Gateway:
   a) Double-click the Gateway object.
   b) In the **Gateway Properties** page, select the **Anti-Bot** Software Blade.
      The First Time **Activation** window opens.
   c) Select **According to the Anti-Bot and Anti-Virus policy**
   d) Click **OK**.
3. Click **Security Policies > Threat Prevention > Policy > Threat Prevention**.
   You can block bots with the out-of-the-box Threat Prevention policy rule with the default Optimized Profile.
   Alternatively, add a new Threat Prevention rule:
   a) Click **Add Rule**.
      A new rule is added to the Threat Prevention policy. The Software Blade applies the first rule that matches the traffic.
   b) Make a rule that includes these components:
      - **Name** - Give the rule a name such as **Block Bot Activity**.
      - **Protected Scope** - The list of network objects you want to protect. By default, the Any network object is used.
      - **Action** - The Profile that contains the protection settings you want (on page 37). The default profile is Optimized.
      - **Track** - The type of log you want to get when the gateway detects malware on this scope.
      - **Install On** - Keep it as **Policy Targets** or select Gateways to install the rule on.
4. Install the Threat Prevention policy (on page 27).

Monitoring Bot Activity

*Scenario:* I want to monitor bot activity in my organization without blocking traffic at all. How can I do this?
In this example, you will create this Threat Prevention rule, and install the Threat Prevention policy:

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Bot activity</td>
<td>*Any</td>
<td>A profile that has <strong>these</strong> changes relative to the Optimized profile: Go to the General Policy pane &gt; Activation Mode section, and set all Confidence levels to Detect.</td>
<td>Log</td>
<td>*Policy Targets</td>
</tr>
</tbody>
</table>

### To monitor all bot activity:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. Create a new profile:
   a) From the **Threat Tools** section, click **Profiles**. The Profiles page opens.
   b) Right-click a profile and select **Clone**.
   c) Give the profile a name such as **Monitoring_Profile**.
   d) Edit the profile, and under **Activation Mode**, configure all confidence level settings to **Detect**.
   e) Select the **Performance Impact** - for example, **Medium or lower**.

   This profile detects protections that are identified as an attack with low, medium or high confidence and have a medium or lower performance impact.
3. Create a new rule:
   a) Click **Threat Prevention > Policy > Threat Prevention**.
   b) Add a rule to the Rule Base.

   The first rule that matches is applied.
   c) Make a rule that includes these components:
      - **Name** - Give the rule a name such as **Monitor Bot Activity**.
      - **Protected Scope** - Keep **Any** so the rule applies to all traffic in the organization.
      - **Action** - Right-click in this cell and select **Monitoring_Profile**.
      - **Track** - Keep **Log**.
      - **Install On** - Keep it as **Policy Targets** or choose Gateways to install the rule on.
4. Install the Threat Prevention policy (on page 27).

### Configuring Anti-Virus Settings

You can configure Threat Prevention to exclude files from inspection, such as internal emails and internal file transfers. These settings are based on the interface type [internal or external, as defined in SmartConsole] and traffic direction [incoming or outgoing].

Before you define the scope for Threat Prevention, you must make sure that your DMZ interfaces are configured correctly. To do this:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
The gateway window opens and shows the General Properties page.
2. From the navigation tree, click Network Management and then double-click a DMZ interface.
3. In the General page of the Interface window, click Modify.
4. In the Topology Settings window, click Override and Interface leads to DMZ.
5. Click OK and close the gateway window.

Perform this procedure for each interface that goes to the DMZ.

You can configure these Anti-Virus settings in the Anti-Virus page:

- **Anti-Virus UserCheck Settings:**
  - Prevent - Select the UserCheck message that opens for a Prevent action.
  - Ask - Select the UserCheck message that opens for an Ask action.
- **Protected Scope:**
  - Inspect incoming files from:
    Sends only incoming files from the specified interface type for inspection. Outgoing files are not inspected. Select an interface type from the list:
    - External - Inspect incoming files from external interfaces. Files from the DMZ and internal interfaces are not inspected.
    - External and DMZ - Inspect incoming files from external and DMZ interfaces. Files from internal interfaces are not inspected.
    - All - Inspect all incoming files from all interface types.
  - Inspect incoming and outgoing files - Sends all incoming and outgoing files for inspection.
- **The Protocols** that Anti-Virus scans:
  - HTTP
  - Mail (SMTP) - Click Mail to configure the SMTP traffic inspection. This links you to the Mail (on page 41) page of the Profile settings.
- **File Types:**
  - Process file types known to contain malware
  - Process all file types - Select Enable deep inspection scanning, if needed. Remember, it impacts performance.
  - Process specific file types families

To configure the specific file type families:

a) Click Configure.

b) In the File Types Configuration window, for each file type, select the Anti-Virus action for the file type.

c) Click OK to close the File Types Configuration window.

- **Archives** - You can configure the Anti-Virus profile to enable archive scanning (on page 49).

**Enabling Archive Scanning**

You can configure the Anti-Virus settings to enable archive scanning. The Anti-Virus engine unpacks archives and applies proactive heuristics. The use of this feature impacts network performance.
Select Enable Archive scanning (impacts performance) and click Configure:

1. Stop processing archive after (seconds) - Sets the amount in seconds to stop processing the archive. The default is 30 seconds.
2. When maximum time is exceeded (action on file) - Sets to block or allow the file when the time for processing the archive is exceeded. The default setting is Allow.

Blocking Viruses

To block viruses and malware in your organization:

1. In SmartConsole, click Gateways & Servers and double-click the Security Gateway.
2. In the General Properties page, select the Anti-Virus Software Blade.
   The First Time Activation window opens.
3. Select According to the Anti-Bot and Anti-Virus policy and click OK.
4. Close the gateway Properties window and publish the changes.
6. Click Add Rule.
   A new rule is added to the Threat Prevention policy. The Software Blade applies the first rule that matches the traffic.
7. Make a rule that includes these components:
   - Name - Give the rule a name such as Block Virus Activity.
   - Protected Scope - The list of network objects you want to protect. In this example, the Any network object is used.
   - Action - The Profile that contains the protection settings you want (on page 37). The default profile is Optimized.
   - Track - The type of log you want to get when detecting malware on this scope. In this example, keep Log and also select Packet Capture to capture the packets of malicious activity. You will then be able to view the actual packets in SmartConsole > Logs & Monitor > Logs.
   - Install On - Keep it as All or choose specified gateways to install the rule on.
8. Install the Threat Prevention policy.

Configuring Threat Emulation Settings

Before you define the scope for Threat Prevention, you must make sure that your DMZ interfaces are configured correctly. To do this:

1. In SmartConsole, click Gateways & Servers and double-click the Security Gateway.
   The gateway window opens and shows the General Properties page.
2. From the navigation tree, click Network Management and then double-click a DMZ interface.
3. In the General page of the Interface window, click Modify.
4. In the Topology Settings window, click Override and Interface leads to DMZ.
5. Click OK and close the gateway window.
Do this procedure for each interface that goes to the DMZ.

If there is a conflict between the Threat Emulation settings in the profile and for the Security Gateway, the profile settings are used.
To configure Threat Emulation settings for a Threat Prevention profile:

1. In SmartConsole, select Security Policies > Threat Prevention.
2. From the Threat Tools section, click Profiles.
   The Profiles page opens.
3. Right-click the profile, and click Edit.
4. From the navigation tree, go to Threat Emulation and configure these settings:
   a) General Threat Emulation Settings (on page 51).
   b) Emulation Environment (on page 52)
   c) Advanced Threat Emulation Settings (on page 52).
5. Click OK and close the Threat Prevention profile window.
6. Install the Threat Prevention policy.

Threat Emulation General Settings

On the Threat Emulation > General page, you can configure these settings:

- **UserCheck Settings**:
  - Prevent - Select the UserCheck message that opens for a Prevent action
  - Ask - Select the UserCheck message that opens for an Ask action

- **Protected Scope**: Select an interface type and traffic direction option:
  - Inspect incoming files from the following interfaces:
    Sends only incoming files from the specified interface type for inspection. Outgoing files are not inspected. Select an interface type from the list:
    - External - Inspect incoming files from external interfaces. Files from the DMZ and internal interfaces are not inspected.
    - External and DMZ - Inspect incoming files from external and DMZ interfaces. Files from internal interfaces are not inspected.
    - All - Inspect all incoming files from all interface types.
  - Inspect incoming and outgoing files - Sends all incoming and outgoing files for inspection.

- **Protocols** to be emulated.
  - HTTP
  - Mail (SMTP) - Click Mail to configure the SMTP traffic inspection by the Threat Emulation blade. This links you to the Mail (on page 41) page of the Profile settings.

- **File Types**. Here you can configure the Threat Emulation Action and Emulation Location for each file type scanned by the Threat Emulation blade. Select one of these:
  - Process all enabled file types - This option is selected by default. Click the blue link to see the list of supported file types. Out of the supported file types, select the files to be scanned by the Threat Emulation blade.
    Note - you can find this list of supported file types also in Manage & Settings view > Blades > Threat Prevention > Advanced Settings > Threat Emulation > File Type Support.
  - Process specific file type families - Click Configure to change the action or emulation location for the scanned file types.
To change the emulation action for a file type, click the applicable action in the **Action** column and select one of these options:

- **Inspect** - The Threat Emulation blade scans these files.
- **Bypass** - Files of this type are considered safe and the Software Blade does not do emulation for them.

To change the emulation location for a file type, click **Emulation Location** and select one of these options:

- **According to gateway** - The **Emulation Location** is according to the settings defined in the **Gateway Properties** window of each gateway.
- **Locally** - Emulation for these file types is done on the gateway.
- **ThreatCloud** - These file types are sent to the ThreatCloud for emulation.

- **Archives** - Block archives containing these prohibited file types. Click **Configure** to select the prohibited file types. If a prohibited file type is in an archive, the gateway drops the archive.

---

**Emulation Environment**

You can use the **Emulation Environment** window to configure the emulation location and images that are used for this profile:

- **The Analysis Locations** section lets you select where the emulation is done:
  
  - To use the Security Gateway settings for the location of the virtual environment, click **According to the gateway**.
  
  - To configure the profile to use a different location of the virtual environment, click **Specify** and select the applicable option.

  **Note** - In the **Remote Emulation Appliances** option, for R80.10 gateways with R80.10 Jumbo Hotfix Accumulator and R77.20 gateways, you can select multiple appliances for remote emulation. For older gateways, you can select only one appliance for remote emulation.

- **The Environments** section lets you select the operating system images on which the emulation is run. If the images defined in the profile and the Security Gateway or Emulation appliance are different, the profile settings are used.

  These are the options to select the emulation images:

  - To use the emulation environments recommended by Check Point security analysts, click **Use Check Point recommended emulation environments**
  
  - To select other images for emulation, that are closest to the operating systems for the computers in your organization, click **Use the following emulation environments**

---

**Advanced Threat Emulation Settings**

- **Emulation Connection Handling Mode** lets you configure Threat Emulation to allow or block a connection while it finishes the analysis of a file. You can also specify a different mode for SMTP and HTTP services.

  - **Background** - The connection is allowed and the file goes to the destination even if the emulation is not finished.
• **Hold** - A connection that must have emulation is blocked and Threat Emulation holds the file until the emulation is complete. This option can create a time-delay for users to receive emails and files.

• **Custom** - Lets you configure different modes for HTTP and SMTP. For example, you can set HTTP to **Background** and SMTP to **Hold**.

**Best Practice** - For configurations that use Hold mode for SMTP traffic, we recommend that you use an MTA deployment (on page 70).

If you use the **Prevent** action, a file that Threat Emulation already identified as malware is blocked. Users cannot get the file even in **Background** mode.

• **Static Analysis** optimizes file analysis by doing an initial analysis on files. If the analysis finds that the file is simple and cannot contain malicious code, the file is sent to the destination without additional emulation. Static analysis significantly reduces the number of files that are sent for emulation. If you disable it, you increase the percentage of files that are sent for full emulation. The Security Gateways do static analysis by default, and you have the option to disable it.

• **Logging** lets you configure the system to generate logs for each file after emulation is complete.

### Configuring Threat Extraction Settings

**To configure Threat Extraction settings for a Threat Prevention profile:**

1. In the **Security Policies** view > **Threat Tools** section, click **Profiles**.
2. Right-click a profile and select **Edit**.
   
   The **Profiles** properties window opens.
3. On the **General Policy** page in the **Blade Activation** area, select **Threat Extraction**.
4. Configure these Threat Extraction Settings:
   
   • **General** (on page 53)
   
   • **Advanced** (on page 55).
5. Click **OK**.

**Note** - You can configure some of the Threat Extraction features in a configuration file, in addition to the CLI and GUI. See sk114613 [http://supportcontent.checkpoint.com/solutions?id=sk114613](http://supportcontent.checkpoint.com/solutions?id=sk114613).

### Threat Extraction General Settings

On the **Threat Extraction > General** page, you can configure these settings:

• **UserCheck Settings**
  
  • Allow the user to access the original file
  
  • Allow access to original files that are not malicious according to Threat Emulation
    
    **Note** - This option is only configurable when the Threat Emulation blade is activated in the **General Properties** pane of the profile.

• **UserCheck Message**
  
  Select a message to show the user when the user receives the clean file. In this message, the user selects if they want to download the original file or not. To select the success or cancelation messages of the file download, go to **Manage & Settings > Blades > Threat**
Prevention > Advanced Settings > UserCheck (on page 93). You can create or edit UserCheck messages on the UserCheck page (on page 88).

- **Optional:** To give the user access to the original email, you can add the Send Original Mail field in the Threat Extraction Success Page. Go to Threat Prevention > Threat Tools > UserCheck > Threat Extraction Success Page > Right-click > Clone > Click inside the message > Insert Field > Select Send Original Mail.

Send Original Mail is added to the message body.

- **Protocol**
  - Mail (SMTP) - Click Mail to configure the SMTP traffic inspection by the Threat Extraction blade. This links you to the Mail (on page 41) page of the Profile settings.

- **Extraction Method**
  - Extract potentially malicious parts from files - Selected by default
    
    Click Configure to select which malicious parts the blade extracts. For example, macros, JavaScript, images and so on.
  
  - Convert to PDF -
    
    Converts the file to PDF, and keeps text and formatting.

**Best Practice** - If you use PDFs in right-to-left languages or Asian fonts, preferably select Extract files from potential malicious parts to make sure that these files are processed correctly.

- **Extraction Settings**
  - Process all files - selected by default
  
  - Process malicious files when the confidence level is:
    
    Set a low, medium or high confidence level. This option is only configurable when the Threat Emulation blade is activated in the General Properties pane of the profile.

- **File Types**
  
  - Process all enabled file types - This option is selected by default. Click the blue link to see the list of supported file types. Out of the supported file types, select the files to be scanned by the Threat Extraction blade.

**Note** - you can find this list of supported file type also in Manage & Settings view > Blades > Threat Prevention > Advanced Settings > Threat Extraction > Configure File Type Support.

- **Process specific file type families** -

  Here you can configure a different extraction method for certain file types. Click Configure to see the list of enabled file types and their extraction methods. To change the extraction method for a file type, right-click the file type and select: bypass, clean or convert to pdf.

**Notes:**

- For jpg, bmp, png, gif, and tiff files - Threat Extraction supports only extraction of potentially malicious content.
  
  - For hwp, jtd, eps, files - Threat Extraction supports only conversion to pdf.
  
  - For Microsoft Office and PDF files and all other file types on the list - Threat Extraction supports both extraction of potentially malicious content and conversion to pdf.
  
  - You can also configure supported file types in the configuration file. For explanation, see sk112240 [http://supportcontent.checkpoint.com/solutions?id=sk112240](http://supportcontent.checkpoint.com/solutions?id=sk112240).
Threat Extraction Advanced Settings

On the Threat Extraction > Advanced page, you can configure these settings:

- **Logging**
  - **Log only those files from which threats were extracted** - Logs only files on which an operation was performed (clean or convert).
  - **Log every file** - Every file that is selected in Threat Extraction > General > File Types is logged, even if no operation was performed on them.

- **Threat Extraction Exceptions**
  - **Corrupted files**
    Block or Allow corrupted files attached to the email or downloaded from the web. Corrupted files are files the blade fails to process, possibly because the format is incorrect. Despite the incorrect format, the related application (Word, Adobe Reader) can sometimes show the content.

  *Block* removes the corrupted file and sends the recipient a text which describes how the file contained potentially malicious content. You can block corrupt files if they are malicious according to Threat Emulation. If the action is block, you can deny access to the original corrupted file.

  *Allow* lets the recipient receive the corrupted file.

  - **Encrypted files**
    Block or Allow encrypted files attached to the email or downloaded from the web.

    *Block* removes the encrypted file and sends the recipient a text file which describes how the file contained potentially malicious content.

    If the action is block, you can also deny access to the original encrypted file.

    *Allow* lets the recipient receive the encrypted file.

Configuring a Malware DNS Trap

The Malware DNS trap works by configuring the Security Gateway to return a false (bogus) IP address for known malicious hosts and domains. You can use the Security Gateways external IP address as the DNS trap address but:

- Do not use a gateway address that leads to the internal network
- Do not use the gateway internal management address
- If the gateway external IP address is also the management address, select a different address for the DNS trap.

You can also add internal DNS servers to better identify the origin of malicious DNS requests.

Using the Malware DNS Trap you can detect compromised clients by checking logs with connection attempts to the false IP address.

At the Security Gateway level, you can configure the DNS Trap according to the profile settings or as a specific IP address for all profiles on the specific gateway.

**To set the Malware DNS Trap parameters for the profile:**

1. In SmartConsole, select Security Policies > Threat Prevention.
2. From the Threat Tools section, click Profiles.
   The Profiles page opens.
3. Right-click the profile, and click Edit.
4. From the navigation tree, click Malware DNS Trap.
5. Click Activate DNS Trap.
6. Enter the IP address for the DNS trap.
7. Optional: Add Internal DNS Servers to identify the origin of malicious DNS requests.
8. Click OK and close the Threat Prevention profile window.
9. Install the Threat Prevention policy.

To set the Malware DNS Trap parameters for a gateway:
1. In SmartConsole, click Gateways & Servers and double-click the Security Gateway.
   The gateway window opens and shows the General Properties page.
2. From the navigation tree, select Anti-Bot and Anti-Virus.
3. In the Malicious DNS Trap section, select one of these options:
   • According to profile settings - Use the Malware DNS Trap IP address configured for each profile.
   • IPv4 - Enter an IP address to be used in all the profiles assigned to this Security Gateway.
4. Click OK.
5. Install the policy.

SandBlast Use Cases

Scenario 1: Excluding senders from scanning
Scanning takes time and resources, so if you know a source is safe, you may want to stop scanning the reports from this source. For example:
• Control and Monitoring systems that send daily reports to IT departments.
• Reports sent by a Mail Relay server about spam emails that it stopped.
In SmartConsole, you can exclude specific senders from the Threat Extraction scanning.

To exclude a sender from the Threat Extraction scanning:
2. Right-click the profile name and select Clone.
   The Clone Object window opens.
3. Enter a name for the cloned profile.
4. Click OK.
5. In the new profile, go to Mail > Exceptions > Extraction Exclusion/Inclusion > Scan all emails, and click Exceptions.
   The Exclude/Include Users window opens.
6. In the Senders section, click the + sign to add the senders to exclude from the Threat Extraction scan.

Scenario 2: Allowing digitally signed emails without scanning
The attorneys at the legal department in Corp X send and receive contracts and other legal documents signed with a digital signature. According to Corp X’s security policy, the Threat Extraction blade scans all files received by the legal department. A digital signature must show the authenticity of a document. If the Threat Extraction blade scans the document, the digital signature can no longer prove the document’s authenticity. The configuration, therefore, must allow digitally signed emails.

In the profile settings > Mail > Exceptions > Threat Extraction Exceptions > Signed email attachments, the default option is Allow. This configuration makes sure that when you receive a digitally signed email, it will be allowed with no scanning, so the form of the email does not change.

**Scenario 3: Configuring Threat Emulation location**

Corp X is located in Threatland. The Threatland law does not allow you to send sensitive documents to cloud services which are outside of the country. The system administrator of Corp X has to configure the location for the Threat Emulation analysis, so that it is not done outside of the country.

**To configure the Threat Emulation analysis location:**

1. In the Gateways & Servers view, double-click a gateway, go to Threat Emulation > Analysis Location.
2. Select:
   - Locally
   OR
   - Remote Emulation Appliances. Click the + sign to select the applicable gateways from the drop-down list.
3. Click OK.

**Note** - You can also configure Threat Emulation analysis location in the profile settings. Go to Security Policies > Threat Prevention > Profiles > double-click a profile > Threat Emulation > Emulation Environment > Analysis Location > Specify.

**Exception Rules**

If necessary, you can add an **exception** directly to a rule. An exception sets a different **Action** to an object in the **Protected Scope** from the Action specified Threat Prevention rule. In general, exceptions are designed to give you the option to reduce the level of enforcement of a specific protection and not to increase it. For example: The Research and Development (R&D) network protections are included in a profile with the **Prevent** action. You can define an exception which sets the specific R&D network to **Detect**. For some Anti-Bot and IPS signatures only, you can define exceptions which are stricter than the profile action.

You can add one or more exceptions to a rule. The exception is added as a shaded row below the rule in the Rule Base. It is identified in the **No.** column with the rule’s number plus the letter E and a digit that represents the exception number. For example, if you add two exceptions to rule number 1, two lines will be added and show in the Rule Base as E-1.1 and E-1.2.

You can use exception groups to group exceptions that you want to use in more than one rule. See the Exceptions Groups Pane.

You can expand or collapse the rule exceptions by clicking on the minus or plus sign next to the rule number in the **No.** column.
To add an exception to a rule:
1. In the **Policy** pane, select the rule to which you want to add an exception.
2. Click **Add Exception**.
3. Select the **Above**, **Below**, or **Bottom** option according to where you want to place the exception.
4. Enter values for the columns. Including these:
   - **Protected Scope** - Change it to reflect the relevant objects.
   - **Protection** - Click the plus sign in the cell to open the Protections viewer. Select the protection[s] and click **OK**.
5. **Install Policy**.

**Note** - You cannot set an exception rule to an inactive protection or an inactive blade.

Disabling a Protection on One Server

*Scenario:* The protection Backdoor.Win32.Agent.AH blocks malware on windows servers. How can I change this protection to detect for one server only?

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

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

**To add an exception to a rule:**
1. In SmartConsole, click **Threat Prevention > Policy > Layer**.
2. Click the rule that contains the scope of Server_1.
3. Click the **Add Exception** toolbar button to add the exception to the rule. The gateway applies the first exception matched.
4. Right-click the rule and select **New Exception**.
5. Configure these settings:
   - **Name** - Give the exception a name such as **Exclude**.
   - **Protected Scope** - Change it to **Server_1** so that it applies to all detections on the server.
   - **Protection/Site** - Click + in the cell. From the drop-down menu, click the category and select one or more of the items to exclude.

**Note** - To add EICAR files as exceptions, you must add them as Whitelist Files (on page 120). When you add EICAR files through Exceptions in Policy rules, the gateway still blocks them, if archive scanning is enabled.

- **Action** - Keep it as **Detect**.
- **Track** - Keep it as **Log**.
• **Install On** - Keep it as **Policy Targets** or select specified gateways to install the rule on.

6. **Install Policy.**

**Blade Exceptions**

You can also configure an exception for an entire blade.

**To configure a blade exception:**

1. In the **Policy**, select the Layer rule to which you want to add an exception.
2. Click **Add Exception**.
3. Select the **Above, Below, or Bottom** option according to where you want to place the exception.
4. In the **Protection/Site** column, select **Blades** from the drop-down menu.
5. Select the blade you want to exclude.
6. **Install Policy.**

**Creating Exceptions from IPS Protections**

**To create an exception from an IPS protection:**

1. Go to **Security Policies > Threat Prevention > Policy > IPS Protections**.
2. Right-click a protection and select **Add Exception**.
3. Configure the exception rule.
4. Click **OK**.
5. **Install Policy.**

**Exception Groups**

An exception group is a container for one or more exceptions. You can attach an exception group to all rules or only to some rules. With exception groups, you can manage your exceptions more easily, because you can attach the same exception group to multiple rules, instead of manually define exceptions for each rule.

The Exception Groups pane shows a list of exception groups that were created, the rules that use them, and any comments related to the defined group. The Exceptions Groups pane contains these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Creates a new exception group.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies an existing exception group.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes an exception group.</td>
</tr>
<tr>
<td>Search</td>
<td>Search for an exception group.</td>
</tr>
</tbody>
</table>

**Global Exceptions**

The system comes with a predefined group named Global Exceptions. Exceptions that you define in the Global Exceptions group are automatically added to every rule in the Rule Base. For other exception groups, you can decide to which rules to add them.
Exception Groups in the Rule Base

Global exceptions and other exception groups are added as shaded rows below the rule in the Rule Base. Each exception group is labeled with a tab that shows the exception group’s name. The exceptions within a group are identified in the No column using the syntax: $E - <rule number>.<exception number>$, where $E$ identifies the line as an exception. For example, if there is a Global Exceptions group that contains two exceptions, all rules show the exception rows in the Rule Base No column as E-1.1 and E-1.2. Note that the numbering of exception varies when you move the exceptions within a rule.

To view exception groups in the Rule Base:
Click the plus or minus sign next to the rule number in the No column to expand or collapse the rule exceptions and exception groups.

Creating Exception Groups

When you create an exception group, you create a container for one or more exceptions. After you create the group, add exceptions to them. You can then add the group to rules that require the exception group in the Threat Prevention Rule Base.

To create an exception group:
1. In SmartConsole, select Security Policies > Threat Prevention > Exceptions.
2. In the Exceptions section, click New.
3. In Apply On, configure how the exception group is used in the Threat Prevention policy.
   - Manually attach to a rule - This exception group applies only when you add it to Threat Prevention rules.
   - Automatically attached to each rule with profile - This exception group applies to all Threat Prevention rules in the specified profile.
   - Automatically attached to all rules - This exception group applies to all Threat Prevention rules.
4. Click OK.
5. Install the Threat Prevention policies.

Adding Exceptions to Exception Groups

To use exception groups, you must add exception rules to them (on page 32).

To add exceptions to an exception group:
1. In SmartConsole, select Security Policies > Threat Prevention > Exceptions.
2. In the Exceptions section, click the exception group to which you want to add an exception.
3. Click Add Exception Rule.
4. Configure the settings for the new exception rule.
5. Install the Threat Prevention policy.

Adding Exception Groups to the Rule Base

You can add exception groups to Threat Prevention rules. This only applies to exception groups that are configured to Manually attach to a rule.
To add an exception group to the Rule Base:
2. Right-click the rule and select Add Exception Group > <group name>.
3. Install the Threat Prevention policies.

Creating Exceptions from Logs or Events
In some cases, after evaluating a log or an event in the Logs & Monitor view, it may be necessary to update a rule exception in the SmartConsole Rule Base. You can do this directly from within the Logs & Monitor view. You can apply the exception to a specified rule or apply the exception to all rules that show under Global Exceptions.

To update a rule exception or global exception from a log:
1. Click Logs & Monitor > Logs tab.
2. Right-click the log and select Add Exception.
3. Configure the settings for the exception.
4. Click OK.
5. In the New Exception Rule window:
   • To show the exception in the policy, click Go to
   • Otherwise, click Close
6. Install Policy.
Configuring Threat Emulation on the Gateway

In This Section:
- Using Local or Remote Emulation ................................................................. 62
- Changing the Analysis Location ........................................................................ 63
- Setting the Activation Mode ............................................................................... 64
- Optimizing System Resources ........................................................................... 64
- Managing Images for Emulation ........................................................................ 65

Using Local or Remote Emulation

This section is for deployments that use an Emulation appliance and run emulation in the internal network.

Note - Prepare the network for the Emulation appliance before you run the First Time Configuration Wizard (on page 22).

To enable an Emulation appliance for Local and Remote emulation:
1. In SmartConsole, go to Gateways & Servers and double-click the Emulation appliance.
   The Gateway Properties window opens.
2. From the Network Security tab, select SandBlast Threat Emulation.
   The Threat Emulation First Time Configuration Wizard opens and shows the Emulation Location page.
4. Click Next.
   The Summary page opens.
5. Click Finish to enable Threat Emulation on the Emulation appliance and close the First Time Configuration Wizard.
6. Click OK.
   The Gateway Properties window closes.
7. For Local emulation, install the Threat Prevention policy on the Emulation appliance.

To enable Threat Emulation on the Security Gateway for Remote emulation:
1. In SmartConsole, go to Gateways & Servers and double-click the Security Gateway.
   The Gateway Properties window opens.
2. From the Network Security tab, select Threat Emulation.
   The Threat Emulation First Time Configuration Wizard opens and shows the Emulation Location page.
3. Configure the Security Gateway for Remote Emulation:
   a) Select Other Threat Emulation appliances.
b) Click **Next**.

c) Click the + sign to add the emulation appliances. For R80.10 gateways with R80.10 Jumbo Hotfix Accumulator and R77.20 gateways, you can add multiple appliances for remote emulation. For older gateways, you can select only one remote emulation appliance.

4. Click **Next**.
   
The Summary page opens.

5. Click **Finish** to enable Threat Emulation on the Security Gateway close the First Time Configuration Wizard.

6. Click **OK**.
   
The Gateway Properties window closes.


### Changing the Analysis Location

When you run the Threat Emulation First Time Configuration Wizard, you select the location of the emulation analysis. You can use the Threat Emulation window in Gateway Properties to change the location.

**Note** - The Threat Prevention policy defines the analysis location that is used for emulation [on page 52].

You can send files that are not supported on the local Emulation appliance to the ThreatCloud for emulation.

**To change the location of the emulation analysis:**

1. Double-click the **Emulation appliance**.
   
The Gateway Properties window opens.

2. From the navigation tree, select **Threat Emulation**.
   
The Threat Emulation page opens.

3. From the Analysis Location section, select the emulation location:
   
   - **According to the gateway** - According to the gateway configuration [on page 62]
   
   - **Specify** -
     
     - **Check Point ThreatCloud** - Files are sent to the Check Point ThreatCloud for emulation
     
     - **Local Gateway** - Select the Security Gateway that does the emulation and of the files
     
     - **Remote Emulation Appliances** - You can select one or more appliances on which the emulation is performed

4. **Optional**: Select **Emulate files on ThreatCloud if not supported locally**.
   
   If files are not supported on the Emulation appliance and they are supported in the ThreatCloud, they are sent to the ThreatCloud for emulation. No additional license is necessary for these files.

5. Click **OK**.

6. Install the policy on the Emulation appliance.
Setting the Activation Mode

You can change the Threat Emulation protection Activation Mode of the Security Gateway or Emulation appliance. The emulation can use the Prevent action that is defined in the Threat Prevention policy or only Detect and log malware.

To configure the activation mode:
1. Double-click the Emulation appliance.
   The Gateway Properties window opens.
2. From the navigation tree, select Threat Emulation.
   The Threat Emulation page opens.
3. From the Activation Mode section, select one of these options:
   - According to policy
   - Detect only
4. Click OK and then install the policy.

Optimizing System Resources

The Resource Allocation settings are only for deployments that use an Emulation appliance. Threat Emulation uses system resources for emulation to identify malware and suspicious behavior. You can use the Resource Allocation settings to configure how much of the Emulation appliance resources are used for emulation. When you change these settings, it can affect the network and emulation performance. You can configure the settings for these system resources:

Minimum available hard disk space (If no emulation is done on a file, the Threat Prevention Fail Mode settings determine if the file is allowed or blocked)

Maximum available RAM that can be used for Virtual Machines

If you plan to change the available RAM, these are the recommended settings:
If the appliance is only used for Threat Emulation, increase the available RAM
If the appliance is also used for other Software Blades, decrease the available RAM

To optimize the system resources for the Emulation appliance:
1. Double-click the Emulation appliance.
   The Gateway Properties window opens.
2. From the navigation tree, select Threat Emulation > Advanced.
   The Advanced page opens.
3. Stopping the emulation is determined when the Log storage mechanism automatically deletes log files. Therefore, in order to change the relevant configured value [Note - It also affects the Log’s files deletion]. Navigate to Logs > Local Storage. And from When disk space is below <value> Start deleting old files, you can then change the <value>. Default is 5GB.
4. To configure the maximum amount of RAM that is available for emulation, select Limit memory allocation.
   The default value is 70% of the total RAM on the appliance.
5. Optional: To change the amount of available RAM:
   a) Click Configure.
The **Memory Allocation Configuration** window opens.

b) Enter the value for the memory limit:

- **% of total memory** - Percentage of the total RAM that Threat Emulation can use. Valid values are between 20 - 90%.
- **MB** - Total MB of RAM that Threat Emulation can use. Valid values are between 512MB - 1000GB.

c) Click **OK**.

6. From **When limit is exceeded traffic is accepted with track**, select the action if a file is not sent for emulation:
   - **None** - No action is done
   - **Log** - The action is logged
   - **Alert** - An alert is sent to SmartView Monitor

7. Click **OK** and then install the policy.

### Managing Images for Emulation

You can define the operating system images that Threat Emulation uses, for each appliance, and for each Threat Emulation profile. If different images are defined for a profile and for an appliance, Threat Emulation will use the images that are selected in both places. An image that is selected only for the appliance or for the profile will not be used for emulation.

**To manage the images that the appliance uses for emulation:**

1. Double-click the **Emulation appliance**. The **Gateway Properties** window opens.

2. From the navigation tree, select **Threat Emulation > Advanced**. The **Advanced** page opens.

3. From the **Image Management** section, select the applicable option for your network:
   - **Use all the images that are assigned in the policy** - The images that are configured in the **Emulation Environment** window are used for emulation.
   - **Use specific images** - Select one of more images that the Security Gateway can use for emulation.

4. Click **OK** and then install the policy.
Configuring Threat Extraction on the Gateway

In This Section:

- Configuring Threat Extraction on the Security Gateway ........................................... 66
- Configuring Threat Extraction in a Cluster ................................................................. 66
- Threat Extraction Statistics ......................................................................................... 67
- Using the Gateway CLI .............................................................................................. 67
- Backup to External Storage ......................................................................................... 68

Configuring Threat Extraction on the Security Gateway

To configure the Threat Extraction blade on the gateway:

1. Enable the Threat Extraction Blade:
      The Threat Extraction First Time Activation Wizard opens.
   b) Configure the Domain and Next Hop.
   c) Click Next.
   d) Click Finish.
2. Enable the gateway as a Mail Transfer Agent (MTA) (on page 70).
3. In the Gateways & Servers view, open the gateway properties > Threat Extraction page.
4. Make sure the Activation Mode is set to Active.
5. In the Resource Allocation section, configure the resource settings.
6. Click OK.
7. Install the Access Control Policy.

Configuring Threat Extraction in a Cluster

The Cluster configuration is similar to gateway configuration, except for specific instructions that are only relevant to cluster.

To configure Threat Extraction in a cluster:

1. In the Gateways & Servers view, right-click the cluster and click edit.
2. Open the ClusterXL and VRRP page.
3. Select High Availability.

Notes:
- Load Sharing is not supported.
The original files are synchronized between the two members of the cluster, so in case of failure, there is still access to the original files.

**Threat Extraction Statistics**

You can see Threat Extraction statistics in the CLI:

1. Open the command line interface of the gateway with the Threat Extraction enabled.
2. Run these commands:
   - `cpview`
   - `cpstat scrub -f threat_extraction_statistics`

**Using the Gateway CLI**

The gateway has a Threat Extraction menu to:

- Control debug messages
- Get information on queues
- Send the initial email attachments to recipients
- Download updates automatically from the ThreatCloud

To use the Threat Extraction command line:

1. Log in to the Security Gateway.
2. Enter expert mode.
3. Enter: `scrub`
   
   A menu shows these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug</td>
<td>Controls debug messages.</td>
</tr>
<tr>
<td>queues</td>
<td>Shows information on Threat Extraction queues. This command helps you understand the queue status and load on the mail transfer agent (MTA) and the <code>scrubd</code> daemon. The command shows:</td>
</tr>
<tr>
<td>send_orig_email</td>
<td>Sends original email to recipients. To send the original email get:</td>
</tr>
</tbody>
</table>

- Number of pending requests from the MTA to the `scrubd` daemon
- Maximum number pending requests from the MTA to the `scrubd` daemon
- Current number of pending requests from `scrubd` to `scrub_cp_file_convert`
- Maximum number of pending requests from `scrubd` to `scrub_cp_file_convert`
- The reference number - Click on link in the email received by the user.
- The email ID - Found in the **Logs & Monitor** logs or debug logs.
### Backup to External Storage

When you run out of disk space, you can back e-mail attachments or web downloads to external storage.

**Notes:**
- In a cluster, both members must have the same configuration.
- End-users cannot access files in external storage, only the administrator can access these files.

**To backup original files to external storage:**

1. Create the backup folder.
   Run: `mkdir /mnt/<local_backup_folder>`

2. Mount the backup folder to the remote folder.
   Run: `mount -t cifs <remote_folder> /mnt/<local_backup_folder>`
   **Example:** `mount -t cifs //MyServer/MyBackupFolder /mnt/MyLocalBackupFolder`

   **Best Practice** - To preserve the mount configuration after reboot, configure a Scheduled Job to the applicable "mount" command "At startup" (in the Gaia portal, go to System Management>Job Scheduler).

   a) Change the `enabled` value from "0" to "1".
   b) In the `external_path` parameter, write the full path to the local backup folder:
   c) The `expired_in_days` parameter sets the backup date. The value you enter for this parameter specifies how many days before expiration the backup is performed.

   **Example:**
   ```
   :external_storage (  
     enabled (1)  
     external_path ("/mnt/MyLocalBackupFolder")  
     expired_in_days (5)
   ```
To manually test the backup:

1. Run this command: scrub backup_expired_mail <days for expired entries> <external_path>
   
   In days for expired entries enter “0”.
Mail Transfer Agent

In This Section:

Using an MTA ................................................................. 70
MTA Engine Updates ....................................................... 74
MTA Monitoring................................................................. 74

Using an MTA

You can enable the Security Gateway as an MTA (Mail Transfer Agent) to manage SMTP traffic. The MTA works with these blades: Threat Emulation, Threat Extraction, and Anti-Spam and Mail Security.

When a gateway scans SMTP traffic, sometimes the email client is not able to keep the connection open for the time that is necessary to handle the email. In such cases, there is a timeout for the email. An MTA deployment prevents this problem. The MTA first accepts the email from the previous hop, does the necessary actions on the email and then relays the email to the next hop. The MTA is able to scan SMTP encrypted traffic for the supported blades.

**Note** - MTA is also supported on VSX gateways. The MTA configuration is the same for VSX and non-VSX gateways.

To use the Security Gateway as an MTA:

1. Enable the Security Gateway as an MTA (on page 70).
2. Configure the network to forward emails to the MTA (on page 73).

Enabling MTA on the Security Gateway

When selected, the Security Gateway is an MTA for SMTP traffic. For a topology that uses TLS between the previous hop and the Security Gateway, you must import the mail server certificate to the Security Gateway.

To enable the Security Gateway as an MTA:

1. In SmartConsole, go to **Gateways & Servers** and double-click the Security Gateway.
2. From the navigation tree, select **Mail Transfer Agent**.
   The **Mail Transfer Agent** page opens.
3. Select **Enable as a Mail Transfer Agent**.
4. In the **Mail Forwarding** section, add one or more rules. These rules define traffic that is sent to the mail servers after the scanning is complete.
   a) Click the add rule button.
   b) Right-click the **Domain** cell and select **Edit**.
   c) Enter the domain for the SMTP traffic for this rule. The default setting is to use the wildcard * to accept all recipient domains.
   d) Click **OK**.
e) Click the Next Hop cell and select the node object that is the mail server for this rule.

**Note** - From R80.20, you can define a domain object as the Next Hop. This lets you use multiple mail servers based on a DNS name. This DNS configuration allows load balancing and high-availability capabilities based on DNS configuration.

You can also configure the MTA to only scan the emails and not forward them to the mail server (on page 73).

5. **Optional**: Select **Add signature to scanned emails** and enter the message to add to the end of the email body after it is successfully processed.

6. If the mail server uses TLS inspection, do these steps to enable the MTA to support it:
   a) Click **Import**.
      
      The **Import Outbound Certificate** window opens.
   b) Click **Browse** and select the certificate file.
   c) Enter the **Private key password** for the certificate.
   d) Click **OK**.
   e) Select **Enable SMTP/TLS**.

7. **Configure the MTA Implied Rule**.
   By default, when you enable a gateway as an MTA, an implied rule is created at the top of the Access Control Policy, which opens port 25 for connections destined to the gateway. The default source in the implied rule is any source IP. You can configure the source column to allow traffic from specific sources.
   To disable this implied rule, clear **Create an implied rule at the top of the Access Control Policy**

8. **Optional**: In the **Advanced Settings** section, click **Configure Settings** and configure the MTA interface and email settings (on page 71).

9. Click **OK** and then install the Threat Prevention policy.
   An MTA rule is created at the top of the Threat Prevention Rule Base.

**Configuring MTA Advanced Settings**

The MTA Advanced Settings window lets you configure which interfaces on the Security Gateway are listening to SMTP traffic that is sent to Threat Emulation.

Use the **Mail Settings** section to define these settings:

- Maximum time that emails are kept in the MTA queue.
- The MTA hard drive limit. When this limit is reached, the MTA stops processing emails.
- Use the **Troubleshooting** section to generate a log or send an alert if emails are delayed in the MTA.

Emails that are in the MTA longer than the **Maximum delayed time** are blocked or allowed without processing. The Troubleshooting setting lets you receive a log or alert when one of the limits is exceeded.

**To configure the MTA advanced settings:**

1. Double-click the Security Gateway and from the navigation tree select **Mail Transfer Agent**.
   The **Mail Transfer Agent** page opens.
2. In the Advanced Settings section, click Configure Settings. The MTA Advanced Settings window opens.

3. To configure the interfaces for SMTP traffic, select one of these options:
   - **All interfaces** - SMTP traffic from all the interfaces is sent for scanning
   - **All external** - SMTP traffic from the external interfaces is sent for scanning
   - **Use specific** - SMTP traffic from the list of specified interfaces is sent for scanning. To add an interface to the list, click the plus sign (+). To remove a selected interface from the list, click the minus sign (-).

4. To change the maximum number of minutes that the MTA keeps emails, configure **Maximum delay time**.

5. To change the MTA hard drive limit, configure these settings:
   - **% of storage** - The percentage limit of MTA hard disk space.
   - **MB** - Total MB limit of MTA hard disk space.

6. To change the action and tracking settings when the specified Mail Settings are exceeded, configure these settings:
   - **Allow** - SMTP traffic is allowed
   - **Block** - SMTP traffic is blocked
   - **None** - No logs are generated
   - **Log** - A log is generated in the Logs & Monitor view
   - **Alert** - Logs the event and sends the configured alert

7. To change the MTA Troubleshooting settings, configure these settings:
   - **When mail is delayed for more than** - Set the maximum number of minutes that email is delayed in the MTA before the track option is done
   - **Track** - Select None [no logs are generated], Log [logs generated in the Logs & Monitor view], Alert [logs the event and sends the configured alert].

8. Click **OK**.

9. **Install OK**.

### Disabling the MTA

To disable the MTA:

1. Configure the network to disable the MTA (on page 72).

### Configuring the Network to Disable the MTA

The MTA address can be saved in the cache. If the MTA queue is not empty, or you disable the MTA first, it is possible to lose emails that are sent to the network.

**To disable MTA for email that is sent to the internal mail server:**

1. Connect to the DNS settings for the network.
2. Change the MX records, and define the mail server as the next hop.
3. Wait for 24 hours.
4. Disable the MTA on the Security Gateway.
To disable MTA for email that is sent to a different MTA:
1. Connect to the SMTP settings on the MTA that sends SMTP traffic to the internal mail server.
2. Change the SMTP settings and define the mail server as the next hop.
3. Make sure that the MTA queue is empty.
4. Disable the MTA on the Security Gateway.

Configuring the Network to Use an MTA

After you configure the Security Gateway as an MTA, change the settings to send SMTP traffic from external networks to the Security Gateway. Each organization has an MX record that points to the internal mail server, or a different MTA. The MX record defines the next hop for SMTP traffic that is sent to the organization. These procedures explain how to change the network settings to send SMTP to the Check Point MTA.

⚠️ Important - If it is necessary to disable the MTA on the Security Gateway (on page 72), change the SMTP settings or MX records first. Failure to do so can result in lost emails.

To configure an MTA for email that is sent to the internal mail server:
1. Connect to the DNS settings for the network.
2. Change the MX records, and define the Security Gateway as the next hop.

To configure an MTA for email that is sent to a different MTA:
1. Connect to the SMTP settings on the MTA that sends email to the internal mail server.
2. Change the SMTP settings and define the Security Gateway as the next hop.

Deploying MTA in Monitor Only Mode

You can use the Check Point MTA to only monitor SMTP traffic.
Configure the MTA to only scan the emails, but not to forward them to the mail server.

Note - Make sure that the mail relay in the network can send a copy of the emails to the Check Point MTA.

To configure the MTA not to forward emails:
1. In SmartConsole, create a new Host object.
2. Configure these settings:
   - **Name** - For example, No_Forward
   - **IPv4 Address** - Enter 0.0.0.0
3. In the Gateways & Servers view, double-click the Security Gateway.
4. From the navigation tree, click Mail Transfer Agent.
   - The Mail Transfer Agent page opens.
5. Make sure to delete all the Mail Forwarding rules.
6. Click the Add rule button.
7. Double-click the Next Hop cell.
8. From the drop-down list, select the new Host object you created in Step 1.
9. Click OK.
10. Install the Threat Prevention policy.

**MTA Engine Updates**

The Mail Transfer Agent Engine Update is an accumulation of new features and bug fixes to the MTA engine. MTA updates are available to users of R80.10 with Jumbo HFA take 142 and up, and users of R80.20 GA.

It is delivered in the form of a CPUSE Hotfix and can be installed and upgraded manually through the CPUSE User Interface and CLISH commands. `cpstop/cpstart` or reboots are not required. The updates do not conflict with the regular Jumbo HFAs (for example, R80_10_jumbo_hf) and can be updated independently.

**To update the MTA engine:**

Open the Gaia Portal > **upgrades (CPUSE) > Status and Actions > MTA Engine Updates**

For more information on the MTA engine updates, see sk123174 http://supportcontent.checkpoint.com/solutions?id=sk123174.

To check the current version of Mail Transfer Agent Update, run this command:

```bash
cat $FWDIR/conf/mta_ver
```

**MTA Monitoring**

There are 3 new views for MTA monitoring in SmartView available for R80.10 gateways with Jumbo Hotfix take 142 or R80.20 gateways:

- **MTA Live Monitoring**
- **MTA Overview**
- **MTA Troubleshooting**

**To see these views:**

1. In SmartConsole, go to the **Logs & Monitor** view.
2. Click the + sign to open a new tab.
3. At the bottom left corner, click **SmartView**.
   
   SmartView opens.
4. Click the + sign to open a new tab.
5. In the navigation tree at the top left corner, select **Views**.
6. Select the relevant MTA Monitoring view from the list.

The views are based on logs that are updated with each email status change. You can change the time frame of the views in the upper left corner of the MTA Live Monitoring page. You can customize the views, create new widgets and export the views to Excel/PDF.

Here is a description of each one of the new views:

- **MTA Live Monitoring** - Shows the current status of the email traffic which passed through the MTA in the selected time frame.

  The left side shows the distribution of the emails in queue in a graph and a table. If you right-click the Action column in the table, you can do these actions on the email:
  - **Retry** - Try to handle the email again
• Drop - Delete the email
• Bypass - Do not perform the security inspection and send the email to the next hop
The right side shows these views for the selected time frame:
• Statistical information on the number of emails in the queue.
• The number of emails delivered.
• Email Status - a diagram which shows a distribution of the email traffic which passed through the MTA, based on these statuses:
  ▪ Bounced - The MTA sent the Emails back to the sender.
  ▪ Deferred - A temporary failure occurred. The MTA will retry to perform the applicable action again.
  ▪ Dropped - The MTA did not transfer the emails to the next hop.
  ▪ Skipped - The MTA bypassed the emails. No performance was performed.
When you click a column in the diagram, a window opens with a list of the logs that the column is based on.

• MTA Overview - This view shows statistical data on the email traffic which passed through the MTA in 3 timelines:
  • Emails by Status Timeline.
  • Email Content Timeline.
  • Emails in Queue Timeline.
You can use compare the 3 timelines to identify trends in email traffic and analyze the root cause for all kinds of situations. For example, if the emails in queue timeline shows many emails in the queue at a certain point in time, you can look at the other timelines to check the possible reasons for this. If the content timeline shows many emails with links and attachments at the same point in time, this could explain it, because they take longer to scan.

• MTA Troubleshooting
  This view shows the causes of failure and the number of failures for each cause. For example: too many parallel requests for scanning or exceeded operation timeout.
  The most common failure timeline shows the X top failures. The default is 5.
The Email Failure timeline shows all failures.
ICAP Server

In This Section:

Introduction to ICAP .................................................................76
ICAP Server Sample Workflow ....................................................78
ICAP Server support for Threat Prevention ...............................78
Related Configuration on the ICAP Client .................................80
Use Case .....................................................................................81

Introduction to ICAP

The Internet Content Adaptation Protocol (ICAP) is a request and response protocol, similar to the HTTP/1.1 protocol, and allows a proxy (or other devices) to send HTTP traffic for inspection by a remote host. This frees up resources and standardizes the way in which new features are implemented. The remote host can allow, block, or modify the content. ICAP is an RFC protocol, which lets devices from different vendors communicate. Check Point devices can work with third party devices without changing the network topology.


ICAP server can work with multiple ICAP clients.

ICAP server is supported only on R80.20 GA gateways and above and supports only the Threat Emulation and Anti-Virus blades. For more information and updates, see sk123412 http://supportcontent.checkpoint.com/solutions?id=sk123412.

ICAP packet structure

The ICAP message is encapsulated into the TCP

![ICAP packet structure diagram]

ICAP methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REQMOD</td>
<td>Client Request Modification. The ICAP Client uses this method for an HTTP / HTTPS request modification.</td>
</tr>
<tr>
<td>RESPMOD</td>
<td>Server Response Modification. The ICAP Client uses this method for an HTTP / HTTPS response modification.</td>
</tr>
<tr>
<td>OPTIONS</td>
<td>The ICAP Client uses this method to retrieve configuration information from the ICAP Server.</td>
</tr>
</tbody>
</table>
ICAP server actions

The ICAP server has 2 possible actions:

<table>
<thead>
<tr>
<th>ICAP Action</th>
<th>Description and Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
<td>• ICAP sends an error to the Client.</td>
</tr>
<tr>
<td></td>
<td>• ICAP sends a block page to the Client.</td>
</tr>
<tr>
<td></td>
<td>For example: A Check Point UserCheck page presented by the Threat Emulation or Anti-Virus Software Blades.</td>
</tr>
<tr>
<td>Continue / Not modified</td>
<td>A default gateway or a proxy server can forward the HTTP Request / Response to its original destination.</td>
</tr>
</tbody>
</table>

ICAP server response codes

These are the ICAP response codes that are different from their HTTP counterparts:

<table>
<thead>
<tr>
<th>Category</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1yz Informational codes</td>
<td>100</td>
<td>Continue after ICAP preview.</td>
</tr>
<tr>
<td>2yz Success codes</td>
<td>204</td>
<td>No Content. No modification is required.</td>
</tr>
<tr>
<td></td>
<td>206</td>
<td>Partial Content.</td>
</tr>
<tr>
<td>4yz Client error codes</td>
<td>400</td>
<td>Bad request.</td>
</tr>
<tr>
<td></td>
<td>404</td>
<td>ICAP Service not found.</td>
</tr>
<tr>
<td></td>
<td>405</td>
<td>Method not allowed for service (for example, RESPMOD requested for service that supports only REQMOD).</td>
</tr>
<tr>
<td></td>
<td>408</td>
<td>Request timeout. ICAP Server timed out waiting for a request from an ICAP Client.</td>
</tr>
<tr>
<td></td>
<td>418</td>
<td>Bad composition. ICAP Server needs encapsulated sections different from those in the request.</td>
</tr>
<tr>
<td>5yz Server error codes</td>
<td>500</td>
<td>Server error. Error on the ICAP Server, such as “out of disk space”.</td>
</tr>
<tr>
<td></td>
<td>501</td>
<td>Method not implemented. This response is illegal for an OPTIONS request as implementation of OPTIONS is mandatory.</td>
</tr>
<tr>
<td></td>
<td>502</td>
<td>Bad Gateway. This is an ICAP proxy error.</td>
</tr>
<tr>
<td></td>
<td>503</td>
<td>Service overloaded. The ICAP server exceeded a maximum connection limit associated with this service. The ICAP Client should not exceed this limit in the future.</td>
</tr>
<tr>
<td></td>
<td>505</td>
<td>ICAP version is not supported by server.</td>
</tr>
</tbody>
</table>
ICAP Server Sample Workflow

<table>
<thead>
<tr>
<th>Item No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Client</td>
</tr>
<tr>
<td>2</td>
<td>Third party gateway or proxy</td>
</tr>
<tr>
<td>3</td>
<td>ICAP client</td>
</tr>
<tr>
<td>4</td>
<td>Web server</td>
</tr>
<tr>
<td>5</td>
<td>Check Point gateway</td>
</tr>
<tr>
<td>6</td>
<td>ICAP server</td>
</tr>
</tbody>
</table>

**Workflow for working with Check Point ICAP server in RESP.MOD:**
1. The client sends a request to the third party gateway/proxy server to download a file.
2. The third party gateway/proxy sends the download request to the Web server.
3. The Web server sends the requested file to the third party gateway/proxy.
4. The ICAP client forwards the file to the ICAP server which is in the Check Point Threat Emulation gateway.
5. The ICAP server sends the file to the Threat Emulation engine.
6. The Threat Emulation checks the file:
   a) The Threat Emulation engine returns a verdict (block, modified or continue) to the ICAP server.
   b) The ICAP server sends the verdict to the ICAP client.
   c) The ICAP client sends the verdict to the client.

**ICAP Server support for Threat Prevention**

ICAP server is only supported with the Threat Emulation and Anti-Virus blades. Any other blades in a Threat Prevention profile are ignored. If you enable ICAP server on the gateway and not enable the Threat Emulation or the Anti-Virus blades, the ICAP server runs but without inspection.

Any Security Gateway can function as an ICAP server.
ICAP server functionality is not supported in VSX mode.

If you enable the ICAP Server on a Check Point Cluster object:

- You must configure your ICAP Clients to communicate with the applicable Virtual IP Address of the Check Point Cluster.
- ICAP connections do not survive cluster failover.

**To enable ICAP server support on the Check Point Security Gateway or cluster:**

1. In SmartConsole, go to the **Gateways & Servers** view and double-click a Security Gateway or cluster.
   The gateway object window opens.
2. Navigate to the **ICAP Server** page.
3. Select **Enable ICAP Server**.
   In Service, the default service is tcp ICAP which runs on port 1344.
4. Configure Fail Mode - In case of an error, configure if requests to the ICAP server are blocked or allowed.
5. Configure Advanced ICAP Server options [on page 79].
6. Click **OK**.
7. Install policy.

You can create a new ICAP service which runs on a port different than 1344 and select it

**To create a new ICAP service:**

1. Go to the objects bar and select **New > More > Service > TCP**.
2. Enter the object name and add a comment if necessary.
3. In **General**, do not select a protocol.
4. In **Match By**, select the **Port** you want the service to run on.
5. Optional: Configure the **Advanced** features. For a detailed explanation on the advanced service features, check the online help.
6. Click **OK**.

The new service now appears in the drop-down **Service** list.

When you enable ICAP server on the gateway object, an auto-generated rule is created in the Threat Prevention Rule Base. One rule is created for each gateway that has ICAP Server enabled. You can only configure the profile column in this rule. You can select a different profile for each ICAP rule. Unlike other Threat Prevention rules, there is no option to create exceptions for an ICAP rule.

Currently, there is no implied rule for ICAP server in the Access Control policy. Make sure that the ICAP port (service) is open in the Access Control policy on all relevant gateway targets.

**Note** - ICAP Server supports only Anti-Virus deep-scan. Any additional functionality, such as MD5 hash, URL reputation, and signature-based protection, is not supported.

**Advanced ICAP Server Configuration on the Gateway**

The ICAP server (CICAP) uses processes to handle the requests it receives from the ICAP client. Each process generates multiple threads, and each thread handles one request from the ICAP client to the ICAP server.
The ICAP server supports dynamic scaling of the number of processes for optimal performance. The number of available threads increases or decreases as needed. The minimum number of processes is 3.

- **The maximum allowed number of server processes** is configured on the gateway. In addition, you can configure **The number of threads per a child process**.

- **The maximum allowed number of server processes** multiplied by **The number of threads per a child process** is the number of maximum concurrent connections that the ICAP server can handle.

- **Start a new child process if the number of available threads is less than [x]** - This option allows dynamic growth and lets you configure the number of new threads as needed. The ICAP server counts the total number of available (idle) threads. If this number is lower than the number configured in this field, it creates a new child process.

- **End a child process if the number of available threads is more than [x]** - This option allows dynamic reduction of the number of threads as needed. The ICAP server counts the total number of available (idle) threads. If this number is higher than the number configured in this field, it ends a child process.

**Threat Prevention Settings and ICAP Server**

The ICAP server operates according to the relevant settings defined for Threat Emulation and Anti-Virus in the selected Threat Prevention profile and engine settings.

**Emulation Connection Handling Mode and ICAP Server**

In the Threat Prevention default profiles (**Basic**, **Optimized**, and **Strict**), Threat Emulation is set to **Background mode**.

**Background mode** means that connections are allowed until emulation is complete.

In **Hold mode**, the connections are blocked until emulation handling is complete. You can create a new profile and change the mode to **Hold mode**, and apply the profile to the relevant gateways.

**Related Configuration on the ICAP Client**

When you work with Check Point ICAP server, make sure to set this configuration on your ICAP client:

- Direct the ICAP modification requests to the ICAP server **sandblast** service. For example: `icap://<ip_address>:1344/sandblast`

- Set the ICAP client to send these headers, if possible: `X-Client-IP`, `X-Server-IP`, `X-Authentication-User` (the headers are used in the ICAP server logs).

- Make sure the operation timeout for the ICAP Client is equal or higher than the operation timeout for the ICAP server. Note that the **sandblast** service on the Check Point ICAP server, can take some time to respond.

- For HTTPS traffic, configure the ICAP client to send clear HTTP (decrypted HTTPS) traffic to the Check Point ICAP server. If this option is not available on your ICAP client, the ICAP server is not able to process the traffic.

**Note** - For a detailed explanation on how to configure a Check Point ICAP client, see the **R80.20 Next Generation Security Gateway Administration Guide**

https://sc1.checkpoint.com/documents/R80.20_GA/WebAdminGuides/EN/CP_R80.20_NextGenSec
For a detailed explanation on how to configure a third party ICAP client, see your vendor’s documentation.

Use Case

You can use the ICAP technology to communicate HTTPS content.

You are a system administrator, who manages a network that includes a third party gateway/proxy and a Check Point gateway. The Check Point gateway enforces the Threat Emulation and Anti-Virus blades. The third party gateway/proxy has HTTPS inspection enabled, but the Check Point Security Gateway does not. With the ICAP client and Check Point ICAP server enabled and configured to work together, the ICAP client can send the decrypted traffic to the ICAP server for inspection. This way, the Check Point gateway can read the HTTPS content for the Threat Emulation and Anti-Virus blades, even if no HTTPS inspection is enabled on the gateway.

The workflow for ICAP technology in HTTPS inspection:

<table>
<thead>
<tr>
<th>Item No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HTTPS client</td>
</tr>
<tr>
<td>2</td>
<td>Third party gateway or proxy</td>
</tr>
<tr>
<td>3</td>
<td>ICAP client</td>
</tr>
<tr>
<td>4</td>
<td>Check Point gateway</td>
</tr>
<tr>
<td>5</td>
<td>Check Point ICAP server</td>
</tr>
<tr>
<td>6</td>
<td>Web server</td>
</tr>
</tbody>
</table>

1. The HTTPS client initiates an HTTPS connection, which is sent to the proxy server.
2. Proxy server forwards the HTTPS connection to the Check Point gateway.
3. The Check Point gateway forwards the HTTPS connection to the web server.
4. The web server sends the requested data over HTTPS to the Check Point gateway.
5. The Check Point gateway forwards the HTTPS connection to the proxy server.
6. The ICAP client decrypts the HTTPS connection (the ICAP client is configured to work in RESPMOD).
7. The ICAP client sends the decrypted HTTPS content to the ICAP server for a verdict.
8. The ICAP server returns a verdict to the ICAP client.
9. Based on the verdict, the proxy server allows or blocks the requested HTTPS data.
IPS Protections

In This Section:

- Protections Browser ................................................................. 82
- Protection Types ............................................................... 83
- Browsing IPS Protections .................................................. 83
- Activating Protections ....................................................... 84
- Editing Core IPS Protections ........................................... 85
- Updating IPS Protections .................................................. 85
- IPS Protections Follow Up ................................................ 86

Protections Browser

The Protection browser shows the Threat Prevention Software Blades protection types and a summary of important information and usage indicators.

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

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>Name of the protection. A description of the protection type is shown in the bottom section of the pane.</td>
</tr>
<tr>
<td>Industry Reference</td>
<td>International CVE or CVE candidate name for attack.</td>
</tr>
<tr>
<td>Performance Impact</td>
<td>How this protection affects the performance of a Security Gateway. If possible, shows an exact figure.</td>
</tr>
<tr>
<td>Severity</td>
<td>Probable severity of a successful attack on your environment.</td>
</tr>
<tr>
<td>Confidence Level</td>
<td>How confident IPS is in recognizing the attack.</td>
</tr>
<tr>
<td>profile_name</td>
<td>The Activation setting for the protection for each IPS profile.</td>
</tr>
</tbody>
</table>

Severity

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

For example, if a protection has a rating of Severity: High, and Performance Impact: Critical, make sure that the protection is necessary for your environment before you activate the protection.

Confidence Level

Some attack types are less severe than others, and legitimate traffic may sometimes be mistakenly recognized as a threat. The confidence level value shows how well the specified protection can correctly recognize the specified 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 granular configurations might be required on this protection.

**Performance Impact**

Some protections require the use of more resources or apply to common types of traffic, which adversely affects the performance of the gateways on which they are activated.

**Note** - The Performance Impact of protections is rated based on how they affect gateways of the R80.20 version. The Performance Impact on other gateways may be different than the rating listed on the protection.

For example, you might want to make sure 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 necessary.

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] computers.

Use the value of this parameter to set an optimal protection profile, in order to prevent overload on the gateway resources.

**Protection Types**

The IPS protections are divided into two main types:

- **Core protections** - These protections are included in the product and are assigned per gateway. They are part of the Access Control policy.
- **ThreatCloud protections** - Updated from the Check Point cloud (on page 85). These protections are part of the Threat Prevention policy.

**Browsing IPS Protections**

The **IPS Protections** summary lets you quickly browse all IPS protections and their settings.

**To show IPS protections:**

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

You can search the Protections page by protection name, engine, or by any information type that is shown in the columns.

**To filter the protections:**

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

To sort the protections list by information:
Click the column header of the information you want.

Activating Protections

Each profile is a set of activated protections and instructions for what IPS does if traffic inspection matches an activated protection. The procedures in this section explain how to change the action for a specified protection.

Activating Protections for All Profiles

To manually activate a protection in all profiles:
1. In SmartConsole, select Security Policies > Threat Prevention.
2. From the Threat Tools section, click IPS Protections. The IPS Protections page opens.
3. Right-click on the protection and select the action that you want to apply to all the Threat Prevention profiles.
   Make sure that the action is on all profiles.
4. Click OK and close the Threat Prevention profile window.
5. Install Policy.

Activating Protections for a Specific Profile

To manually activate a protection for a specific profile:
1. In the Protections Browser, find the protection to activate.
2. Click Edit.
3. Select the profile to activate for this protection.
4. Click Edit.
   You can activate the protection for one profile and deactivate it for another profile. It will be active for some gateways and inactive for others.
   If the protection is inactive according to the policy, you can override the policy preference or change the policy criteria.
   To override the settings for this one protection, continue with this procedure.
5. Click Override with.
6. Select the action 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.
7. Configure the **Logging** settings:
   - **Track**: Define how administrators get notifications (log, alert, mail, or other options).
   - **Capture Packets**: Captures packets relevant to the protection for further analysis.
8. **Install Policy**.

**Removing Activation Overrides**

You can remove the manually activated IPS protections and restore them to the profile settings. You can remove overrides on one protection, on selected protections or on all protections at the same time.

**To remove IPS protection overrides on selected protections:**

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **IPS Protections**.
   - The **IPS Protections** page opens.
3. Click the protections in the applicable profile column.
   - **Note** - Press CTRL to select more than one protection.
4. Right-click the highlighted cell or cells and select **Restore to profile settings**.
5. Select **All Profiles** or **Displayed Profiles**.
   - A warning message opens.
6. Click **Yes**.
7. **Install Policy**.

**To remove IPS protection overrides from all protections:**

1. In the **IPS Protections** page, go to **Actions** and select **Profile Cleanup**.
   - The **Profile Cleanup** window opens.
2. In the Action area, select **Remove all user modified, Clear all staging**, or both.
3. In the **Select Profiles** area, select the profiles on which to operate these actions.
4. Click **OK**.
5. **Install Policy**.

**Editing Core IPS Protections**

**To edit core protections:**

1. Go to **Security Policies > Threat Prevention > Threat Tools > IPS Protections**.
   - **Note** - to filter for core protections, select **Type Core** in the **Filters** pane.
2. Right-click a core protection and select **Edit**.
3. Configure the required settings.
4. Install the Access Control policy.

**Updating IPS Protections**

Check Point constantly develops and improves its protections against the latest threats. You can immediately update IPS with real-time information on attacks and all the latest protections. You
can manually update the IPS protections and also set a schedule when updates are automatically downloaded and installed. IPS protections include many protections that can help manage the threats against your network. Make sure that you understand the complexity of the IPS protections before you manually modify the settings.

Note - To enforce the IPS updates, you must install the Threat Prevention Policy.

**To update IPS Protections:**
1. In SmartConsole, click **Security Policies > Threat Prevention.**
2. In the **Threat Tools** section, click **Updates.**
3. In the **IPS** section > **Update Now,** from the drop-down menu, select:
   - **Download with SmartConsole** - If your Security Management Server has no internet access.
   - **Download with Security Management Server**
   - **Offline Update** - If you want to manually upload the file. Select the required file for the update and click **Open.**
4. **Install Policy.**

Note - From R77.20, IPS purge runs automatically after every IPS update. The Security Management Server saves only the versions from the last 30 days, and deletes the others.

**Scheduling IPS Updates**

You can configure a schedule for downloading the latest IPS protections and protection descriptions [on page 141].

**Reverting to an Earlier IPS Protection Package**

For troubleshooting or for performance tuning, you can revert to an earlier IPS protection package.

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

**Reviewing New Protections**

**To see newly downloaded protections:**
1. In SmartConsole, click **Security Policies > Threat Prevention.**
2. In the **Threat Tools** section, click **IPS Protections.**
3. Sort the protections by **Update Date** to see the latest protections.

**IPS Protections Follow Up**

The follow up mark lets you monitor specific IPS protections according to your selection. After you select the protections you wish to monitor, you can filter for them in the IPS Protections page and not have to search for them again.
**To view protections marked for follow up:**

In SmartConsole, go to Security Policies > Threat Prevention > IPS Protections > Filters, and select Follow Up.

You can mark individual protections for follow up or mark all updated protections for follow up in the IPS Updates page.

**Manually Marking Protections for Follow Up**

You can mark individual protections for Follow Up, which lets you quickly review the identified protections in the **IPS Protections** page. To make the Follow Up feature efficient, make sure to keep the list of marked protections as short as possible. 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 configured them in the best way for your environment, for now. The longer the Follow Up list is, the more difficult it is to use it as a workable task list.

**To manually mark protections for follow up:**

In the **IPS Protections** page, select one or more protections, right-click and select **Follow Protection** from the menu.

To unmark the protection, right-click the protection and clear **Follow Protection**.

Each time the IPS protections are updated, they will be automatically marked for follow up. To unmark the protections for follow up, click **Unfollow Protections**. To unmark all marked protections, go to **Actions > Cleanup Options > Remove All Follow Up Flags**.

**Note** - You can add significant information about a protection in the protection’s comment field. To add a comment to a protection, double-click a protection and enter a comment in the **Enter Protection Comment** field, below the protection’s name. You can only add comments to ThreatCloud protections (and not Core protections). You can enter information such as the package version or date of update. Such information is useful because you can search for it at a later date.

**Automatically Marking New Protections for Follow Up**

Check Point provides new and updated protections as they become available [see Updating IPS Protections (on page 85)]. To give you complete control over the process of integrating new IPS protections, you can have them automatically marked for Follow Up, which gives you time to evaluate the impact the protections have on your environment.

**To have new protections marked automatically:**

In SmartConsole > Security Policies > Threat Prevention > Threat Tools > Updates > IPS > select Follow Protections.
Threat Prevention and UserCheck

In This Section:

- Using the Threat Prevention UserCheck Pane ...................................................... 88
- Configuring the Security Gateway for UserCheck ..................................................... 89
- Creating Threat Prevention UserCheck Objects ..................................................... 90
- Editing UserCheck Objects ...................................................................................... 92
- Selecting Approved and Cancel UserCheck Messages ............................................. 93

UserCheck handles specified threat incidents. UserCheck notifications inform the user of data capture. If the action is Ask, the user must provide a reason to allow the traffic. User decisions are logged. You can develop an effective prevention policy based on logged user responses.

For each Threat Prevention profile, you can define the action that is taken when a malicious file or activity is identified.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ask</td>
<td>The Software Blade blocks the file or traffic until the user makes sure that the gateway should send it. The user decides if the file or traffic are allowed or not. The decision itself is logged in the User Response field in the Ask User log.</td>
</tr>
<tr>
<td>Prevent</td>
<td>The Software Blade blocks the file or traffic. You can show a UserCheck Prevent message to the user.</td>
</tr>
<tr>
<td>Detect</td>
<td>The Software Blade allows the file or traffic. The event is logged and is available for your review and analysis in the Logs &amp; Monitor view.</td>
</tr>
</tbody>
</table>


Using the Threat Prevention UserCheck Pane

On the UserCheck page, you can create, edit, and preview UserCheck interaction objects and their messages. It has these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Creates a new UserCheck object</td>
</tr>
<tr>
<td>Edit</td>
<td>Modifies an existing UserCheck object</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes an UserCheck object</td>
</tr>
<tr>
<td>Clone</td>
<td>Clones the selected UserCheck object</td>
</tr>
</tbody>
</table>

These are the default UserCheck messages:

<table>
<thead>
<tr>
<th>Name</th>
<th>Action Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Blade Blocked</td>
<td>Block</td>
<td>Shows when a request is blocked.</td>
</tr>
<tr>
<td>Name</td>
<td>Action Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Company Policy Software Blade</td>
<td>Ask</td>
<td>Shows when the action for the rule is ask. It informs users what the company policy is for that site and they must click OK to continue to the site.</td>
</tr>
<tr>
<td>Software Blade Success Page</td>
<td>Approve</td>
<td>Shows when the action for the rule is Approve. From the Success page you can download the links to the original file or receive the original email.</td>
</tr>
<tr>
<td>Cancel Page Anti-Malware</td>
<td>Cancel</td>
<td>The Ask and Approve pages include a Cancel button that you can click to cancel the request.</td>
</tr>
</tbody>
</table>

You can preview each message page in these views:

- **Regular view** - How the message shows in a web browser on a PC or laptop
- **Mobile Device** - How the message shows in a web browser on a mobile device
- **Email** - How the message shows in an email
- **Agent** - How the message shows in the UserCheck agent

### Configuring the Security Gateway for UserCheck

Enable or disable UserCheck directly on the Security Gateway. Make sure that the UserCheck is enabled on each Security Gateway in the network. To enable UserCheck, enable a blade that has the UserCheck functionality.

The Security Gateway has an internal persistence mechanism that preserves UserCheck notification data if the Security Gateway or cluster reboots. Records of a user answering or receiving notifications are never lost.

**To configure UserCheck on a Security Gateway:**

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway. The **Gateway Properties** window opens.
2. From the navigation tree, click **UserCheck**. The **UserCheck** page opens.
3. Make sure **Enable UserCheck for active blades** is selected.
4. In the **UserCheck Web Portal** section:
   - In the **Main URL** field, enter the primary URL for the web portal that shows the UserCheck notifications.
   - If users connect to the Security Gateway remotely, make sure that the Security Gateway internal interface [in the **Network Management** page] is the same as the Main URL.
   - **Note** - The **Main URL** field must be manually updated if:
     - The Main URL field contains an IP address and not a DNS name.
     - You change a gateway IPv4 address to IPv6 or vice versa.
5. **Optional**: Click **Aliases** to add URL aliases that redirect different hostnames to the **Main URL**. The aliases must be resolved to the portal IP address on the corporate DNS server.
6. In the **Certificate** section, click **Import** to import a certificate that the portal uses to authenticate to the Security Management Server.
   - By default, the portal uses a certificate from the Check Point Internal Certificate Authority [ICA]. This might generate warnings if the user browser does not recognize Check Point as a
trusted Certificate Authority. To prevent these warnings, import your own certificate from a recognized external authority.

**Note** - After you download your certificate, you can click **Replace** to replace it with a different certificate, and click **View** to see the certificate information.

7. In the **Accessibility** section, click **Edit** to configure interfaces on the Security Gateway through which the portal can be accessed. These options are based on the topology configured for the Security Gateway. The topology must be configured.

Users are sent to the UserCheck portal if they connect:

- **Through all interfaces**
- **Through internal interfaces** *(default)*
  - Including undefined internal interfaces
  - Including DMZ internal interfaces
  - Including VPN encrypted interfaces *(default)*
    
    **Note**: Make sure to add a rule to the Firewall Rule Base that allows the encrypted traffic.

- **According to the Firewall Policy**. Select this option if there is a rule that states who can access the portal.

If the **Main URL** is set to an external interface, you must set the **Accessibility** option to one of these:

- **Through all interfaces** - necessary in VSX environment
- **According to the Firewall Policy**

8. In the **Mail Server** section, configure a mail server for UserCheck. This server sends notifications to users that the Gateway cannot notify using other means, if the server knows the email address of the user. For example, if a user sends an email which matched on a rule, the Gateway cannot redirect the user to the UserCheck portal because the traffic is not http. If the user does not have a UserCheck client, UserCheck sends an email notification to the user.

- **Use the default settings** - Click the link to see which mail server is configured.
- **Use specific settings for this gateway** - Select this option to override the default mail server settings.
- **Send emails using this mail server** - Select a mail server from the list, or click **New** and define a new mail server.

9. Click **OK**.

10. If there is encrypted traffic through an internal interface, add a new rule to the Firewall Layer of the Access Control Policy. This is a sample rule:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Services &amp; Applications</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Security Gateway on which UserCheck client is enabled</td>
<td>Any</td>
<td>UserCheck</td>
<td>Accept</td>
</tr>
</tbody>
</table>

11. Install the Access Control Policy.

**Creating Threat Prevention UserCheck Objects**

Create a UserCheck Interaction object from the **UserCheck** page or Threat Prevention Software Blade profile **Settings**.
You can write the UserCheck message with formatting buttons, like Bold and bullets, or directly enter HTML code.

**To show the Threat Prevention UserCheck objects:**
1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **UserCheck**.
   The **UserCheck** page opens.

**To change text input modes:**
From the menu-bar in the UserCheck object window, click the applicable option:
- **Source** - Enter HTML code
- **Design** - Enter text with formatting buttons and options

**To create a new Threat Prevention UserCheck object:**
1. From the **UserCheck** page, click **New** and select the object type.
   The window opens for the new UserCheck object.
2. Enter a **Name**.
3. **Optional**: Click **Language** and select one or more languages for the message.
   The default language for messages is English.
4. Enter the text for the message.
   - Title, subtitle, and body
   In the body of the message click these options for additional functionality:
   - **Insert Field** - Dynamic text such as: Original URL, Source IP address, and so on
   - **Insert User Input** - Such as: Confirm check box, Report Wrong Category and so on
5. **Optional**: Click **Add logo** to add a graphic to the message.
   The size of the graphic must be 176 x 52 pixels.
6. You can also click **Settings** from the navigation tree to configure one or more of these options:
   - Using a Fallback Action (on page 91)
   - Redirecting to an External Portal (on page 92)
   - Configuring User Interaction (on page 92)
7. Click **OK**.
8. Install the Threat Prevention policy.

**Using a Fallback Action**
Configure the default action for an Ask UserCheck object if the user cannot see the message. You can select one of these options:
- **Drop** - The connection or traffic is dropped and does not enter the internal network
- **Accept** - The connection or traffic is accepted and enters the internal network

**To configure a fallback action for an Ask object:**
1. From the navigation tree, click **Settings**.
2. In the **Fallback Action** section, select to **Drop** or **Accept** traffic when the user cannot see the UserCheck message.
Redirecting to an External Portal

You can configure UserCheck to redirect the user to an external UserCheck portal and the user does not see this UserCheck message.

To redirect a user to an external portal:
1. From the navigation tree, click Settings.
2. Click Redirect to External Portal.
3. In External Portal URL, enter the URL for the external portal.
   The specified URL can be an external system that obtains authentication credentials from the user, such as a user name or password. It sends this information to the Security Gateway.
4. Optional: Select Add UserCheck Incident ID to the URL query to add an incident ID to the end of the URL query.

Configuring User Interaction

You can configure the necessary user interaction for an Ask UserCheck object. The traffic is allowed only after the user does the necessary actions.

The UserCheck message can contain these items that require user interaction [shown with sample messages]:

- **Confirm checkbox** - I am ignoring the warning
- **Textual input** - Enter the reason that you are ignoring the Threat Prevention warning

To configure the necessary user interaction for an Ask object:
1. From the navigation tree, click Settings.
2. In the **Conditions** section, select one or more of these options:
   - User accepted and selected the confirm checkbox
   - User entered the required textual input in the user input field
   The traffic or connection is blocked until the user does the necessary actions.

Editing UserCheck Objects

To edit a UserCheck object:
2. Right-click the UserCheck page and select Clone.
   The New Object Editor opens.
3. Enter a name for the new object.
4. Make the necessary changes.
5. Click **OK**.
Selecting Approved and Cancel UserCheck Messages

In this section, you can select Approved Page and Cancel Page:

- **Approved Page** - Only applicable for Threat Extraction. When Threat Extraction sends you a clean file, you can select to download the original file. If you select to download the original file, you receive a UserCheck success message. If you select not to download the original file, you receive a UserCheck cancel message.

- **The Cancel Page** - Applicable to all the Threat Prevention Software Blade. The page shows after you refuse to receive access to a page or a file.

**To select Approved and Cancel pages:**

1. Go to **Manage & Settings > Blades > Threat Prevention > UserCheck**.
2. From the drop-down menus, select an **Approved Page**, a **Cancel Page** or both.
3. Click **OK**.
4. **Install Policy**.
Monitoring Threat Prevention

In This Section:

Log Sessions ................................................................................................................................. 94
Using the Log View in SmartConsole .................................................................................... 95
Viewing Threat Prevention Rule Logs .................................................................................... 96
Predefined Queries .................................................................................................................. 96
Creating Custom Queries ........................................................................................................ 97
Selecting Query Fields ........................................................................................................... 100
Packet Capture ....................................................................................................................... 101
Advanced Forensics Details .................................................................................................... 101
Threat Analysis in the Logs & Monitor View ........................................................................ 101

Log Sessions

Gateway traffic generates a large amount of activity. To make sure that the amount of logs is manageable, by default, logs are consolidated by session. A session is a period that starts when a user first accesses an application or site. During a session, the gateway records one log for each application or site that a user accesses. All activity that the user does within the session is included in the log.

To see the number of connections made during a session, see the Suppressed Logs field of the log in the Logs & Monitor view.

Session duration for all connections that are prevented or detected in the Rule Base, is by default 10 hours. You can change this in the Manage & Settings view in SmartConsole > Blades > Threat Prevention > Advanced Settings > General > Connection Unification.
Using the Log View in SmartConsole

In SmartConsole:
1. Go to Logs and Monitoring > View.
2. Click New, and select New View.
3. In the New View window, enter:
   - Name
   - Category – For example, select Access Control
   - Description (optional)
4. In the new window that opens, create a query. Click Options > View Filter and select blade and app control.
5. Click Add Widget to customize how you see the data that comes back from the query.

   Start with a Timeline of all events.

   In Table, you can create a table that contains multiple fields such as user, application name, and the amount of traffic. There are more widgets you can use: map, infographic, rich text, chart, and container (for multiple widgets).

   After you save the dashboard (done), you can schedule and get an automatic email at multiple intervals.

This is an example of the Log view.

---

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Queries - Predefined and favorite search queries.</td>
</tr>
<tr>
<td>2</td>
<td>Time Period - Search with predefined custom time periods.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>3</td>
<td>Query search bar - Define custom queries in this field. You can use the GUI tools or manually enter query criteria. Shows the query definition for the most recent query.</td>
</tr>
<tr>
<td>4</td>
<td>Log statistics pane - Shows top results of the most recent query.</td>
</tr>
<tr>
<td>5</td>
<td>Results pane - Shows log entries for the most recent query.</td>
</tr>
</tbody>
</table>

### Viewing Threat Prevention Rule Logs

**To see logs generated by a specified rule:**

1. In SmartConsole, go to the Security Policies view.
2. In the Threat Prevention Policy, select a rule.
3. In the bottom pane, click one of these tabs to see:
   - **Summary** - Rule name, rule action, rule creation information, and the hit count. Add custom information about the rule.
   - **Logs** - Log entries according to specified filter criteria - Source, Destination, Blade, Action, Service, Port, Source Port, Rule (Current rule is the default), Origin, User, or Other Fields.

### Predefined Queries

The Logs & Monitor Logs tab provide a set of predefined queries, which are appropriate for many scenarios.

Queries are organized by combinations of event properties, for example:

- **Threat Prevention > by Blades.**
- **More > such as by UA Server or UA WebAccess.**
- **Anti-Spam & Email Security Blade > such as by Blocklist Anti-Spam or IP Reputation Anti-Spam.**
Creating Custom Queries

Queries can include one or more criteria. You can modify an existing predefined query or create a new one in the query box.

To modify a predefined query:
Click inside the query box to add search filters.

To save the new query in the Favorites list:
1. Click Queries > Add to Favorites.
   The Add to Favorites window opens.
2. Enter a name for the query.
3. Select or create a new folder to store the query
4. Click Add.
Selecting Criteria from Grid Columns

You can use the column headings in the Grid view to select query criteria. This option is not available in the Table view.

To select query criteria from grid columns:
1. In the Results pane, right-click on a column heading.
2. Select Add Filter.
3. Select or enter the filter criteria.
   The criteria show in the Query search bar and the query runs automatically.

To enter more criteria, use this procedure or other procedures.
Manually Entering Query Criteria

You can enter query criteria directly in the **Query search bar**. You can manually create a new query or make changes to an existing query that shows in the **Query search bar**.

As you enter text, the **Search** shows recently used query criteria or full queries. To use these search suggestions, select them from the drop-down list.
Selecting Query Fields

You can enter query criteria directly from the Query search bar.

**To select field criteria:**

1. If you start a new query, click Clear $\times$ to remove query definitions.
2. Put the cursor in the Query search bar.
3. Select a criterion from the drop-down list or enter the criteria in the Query search bar.
Packet Capture

You can capture network traffic. The content of the packet capture provides a greater insight into the traffic which generated the log. With this feature activated, the Security Gateway sends a packet capture file with the log to the log server. You can open the file, or save it to a file location to retrieve the information a later time.

For some blades, the packet capture option is activated by default in Threat Policy.

**To deactivate packet capture (in Threat Policy only):**

1. In SmartConsole, in the Security Policies view
2. In the Track column of the rule, right-click and clear Packet Capture.

**To see a packet capture:**

1. In SmartConsole, go to the Logs & Monitor view.
2. Open the log.
3. Click the link in the Packet Capture field.
   - The Packet Capture opens in a program associated with the file type.
4. Optional - Click Save to save the packet capture data on your computer.

Advanced Forensics Details

From R80.30, some logs contain additional fields which can be found in the Advanced Forensics Details section in the log. These protocols are supported: DNS, FTP, SMTP, HTTP, and HTTPS. The additional information is used by the Check Point researchers to analyze attacks. The advanced forensics details also show in the gateway statistics files which are sent to the Check Point Cloud.

**To enable the Advanced Forensics Details feature:**

In SmartConsole, go to >, Go to Security Policies > Threat Prevention > Policy > Track > from the drop-down menu, select Forensics.

The Advanced Forensics Details do not show if the connection closes before this information is saved. This depends on the traffic and configuration of the Software Blades. For example:

- When the gateway finds the connection is malicious before the additional details are saved.
- When Threat Emulation or Anti-Virus are in Background mode, and the file is downloaded and the connection closes before the examination of the file is complete. In such case, the forensics details may not show.

Threat Analysis in the Logs & Monitor View

The Logs & Monitor view supplies advanced analysis tools with filtering, charts, reporting, statistics, and more, of all events that travel through enabled Security Gateways.

You can filter the Threat Prevention Software Blade information for fast monitoring and useful reporting on connection incidents related to them.

- Real-time and historical graphs and reports of threat incidents
- Graphical incident timelines for fast data retrieval
• Easily configured custom views to quickly view specified queries
• Incident management workflow
• Reports to data owners on a scheduled basis

Views

Views window tells administrators and other stakeholders about security and network events. A View window is an interactive dashboard made up of widgets. Each widget is the output of a query. A Widget pane can show information in different formats, for example, a chart or a table.

SmartConsole comes with several predefined views. You can create new views that match your needs, or you can customize an existing view. Views are accurate to the time they were generated or refreshed.

In the Logs & Monitor view, clicking the (+) tab opens a catalog of all views and reports, predefined and customized. To open a view, double-click the view or select the desired view and click Open from the action bar.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Widget</strong> - The output of a query. A Widget can show information in different formats, for example, a chart or a table. To find out more about the events, you can double-click most widgets to drill down to a more specific view or raw log files.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Options</strong> - Customize the view, restore defaults, Hide Identities, export.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Query search bar</strong> - Define custom queries using the GUI tools, or manually entering query criteria. Shows the query definition for the most recent query.</td>
</tr>
<tr>
<td>4</td>
<td><strong>Time Period</strong> - Specify the time periods for the view.</td>
</tr>
</tbody>
</table>

For more information on using and customizing reports, see the *R80.20 Logging and Monitoring Administration Guide*
Reports

A report has multiple pages, and applies to the time that the report is generated. There are several predefined reports, and you can create new reports. A report gives more details than a view. Reports can be customized, filtered, generated and scheduled. You cannot drill down into a report.

In the **Logs & Monitor** view, clicking the {+} tab opens a catalog of all views and reports, predefined and customized. To open a report, double-click the report or select the desired report and click **Open** from the action bar.

A report is divided onto pages, usually, one view on one page. Editing a report is done per page, in the same way as you edit a view. You can customize and generate a report, and specify the report time period, the same way you did for views. In the query search bar, you can define custom queries using the GUI tools or manually enter a query.

For more information on using and customizing Reports, see the **R80.20 Logging and Monitoring Administration Guide**
Configuring Advanced Threat Prevention Settings

In This Section:

- Threat Prevention Engine Settings ........................................................................................................ 104
- SNORT Signature Support ...................................................................................................................... 107
- Optimizing IPS ......................................................................................................................................... 118
- Using the Whitelist ............................................................................................................................... 120
- Threat Indicator Settings ....................................................................................................................... 120
- Using Anti-Bot and Anti-Virus with VSX ............................................................................................... 124
- Using Threat Extraction with VSX ........................................................................................................ 125
- Threat Prevention CLI Commands ....................................................................................................... 126

Threat Prevention Engine Settings

This section explains how to configure advanced Threat Prevention settings that are in the Engine Settings window, including: inspection engines, the Check Point Online Web Service (ThreatCloud repository), internal email whitelist, file type support for Threat Extraction and Threat Emulation and more.

To get to the Engine Settings window, go to Manage & Settings > Blades > Threat Prevention > Advanced Settings.

The Threat Prevention Engine Settings window opens.

Fail Mode

Select the behavior of the ThreatSpect engine if it is overloaded or fails during inspection. For example, if the Anti-Bot inspection is terminated in the middle because of an internal failure. By default, in such a situation all traffic is allowed.

- **Allow all connections (Fail-open)** - All connections are allowed in a situation of engine overload or failure (default).
- **Block all connections (Fail-close)** - All connections are blocked in a situation of engine overload or failure.

Check Point Online Web Service

The Check Point Online Web Service is used by the ThreatSpect engine for updated resource categorization. The responses the Security Gateway gets are cached locally to optimize performance.

- **Block connections when the web service is unavailable**
  - When selected, connections are blocked when there is no connectivity to the Check Point Online Web Service.
  - When cleared, connections are allowed when there is no connectivity (default).
• **Resource categorization mode** - You can select the mode that is used for resource categorization:
  - **Background - connections are allowed until categorization is complete** - When a connection cannot be categorized with a cached response, an uncategorized response is received. The connection is allowed. In the background, the Check Point Online Web Service continues the categorization procedure. The response is cached locally for future requests (default). This option reduces latency in the categorization process.
  - **Hold - connections are blocked until categorization is complete** - When a connection cannot be categorized with the cached responses, it remains blocked until the Check Point Online Web Service completes categorization.
  - **Custom - configure different settings depending on the service** - Lets you set different modes for Anti-Bot and Anti-Virus. For example, click **Customize** to set Anti-Bot to Hold mode and Anti-Virus to Background mode.

**Connection Unification**

Gateway traffic generates a large amount of activity. To make sure that the amount of logs is manageable, by default, logs are consolidated by session. A session is a period that starts when a user first accesses an application or a site. During a session, the gateway records one log for each application or site that a user accesses. All activity that the user does within the session is included in the log. For connections that are allowed or blocked in the Anti-Bot, Threat Emulation, and Anti-Virus Rule Base, the default session is 10 hours (600 minutes).

**To adjust the length of a session:**
1. Go to **Manage & Settings > Blades > Threat Prevention > Advanced Settings > General > Connection Unification > Session unification timeout (minutes).**
2. Enter the required value.
3. Click **OK**.

**Configuring Anti-Bot Whitelist**

The Suspicious Mail engine scans outgoing emails. You can create a list of email addresses or domains whose internal emails are not inspected by Anti-Bot.

**To add an email address or domain whose internal emails are not scanned by Anti-Bot:**
1. Go to **Manage & Settings > Blades > Threat Prevention > Advanced Settings > Anti-Bot.**
2. Click the + sign.

In this window, you can also edit or remove the entries in the list.

**Selecting Emulation File Types**

You can select the file types that are sent for emulation for all the Threat Prevention profiles. Each profile defines an **Inspect** or **Bypass** action for the file types.

**To select Threat Emulation file types that are supported in Threat Prevention profiles:**
1. In **SmartConsole**, select **Manage & Settings > Blades.**
2. From the **Threat Prevention** section, click **Advanced Settings.**
The **Threat Prevention Engine Settings** window opens.

3. From the **Threat Emulation Settings** section, click **Configure file type support**.
   The **File Types Support** window opens.

4. Select the file types that are sent for emulation. By default all file types are sent for emulation.
   The **Emulation supported on column** shows the emulation environments that support the file type.

5. Click **OK** and close the **Threat Prevention Engine Settings** window.

6. Install the Threat Prevention policy.

### Configuring Advanced Engine Settings for Threat Extraction

Advanced Threat Extraction engine settings let you configure file type support and mail signatures for the Threat Extraction.

### Configuring File Type Support

**To configure file type support:**

1. In the **Threat Prevention Engine Settings** window **Threat Extraction**, click **Configure File Type Support**.
   The **Threat Extraction Supported File Types** window opens.

2. From the list select the file types which the Threat Extraction blade supports.

3. Click **OK**.

### Configuring Mail Signatures

**To configure mail signatures:**

1. In the **Threat Prevention Engine Settings** window > **Threat Extraction**, click **Configure Mail Signatures**.
   The **Threat Extraction Mail Signatures** window opens.
   Use this window to configure text for:

   - **Mail signatures for attachments with potential threats extracted**
     The first signature is always attached to an email that had threats extracted.
     The second signature is added to the first if the email recipient has access to the original file.

   - **Mail signatures for unmodified attachments**
     You can insert predefined field codes into the signature text, such as:
     - A link to the file before it was modified by the blade.
     The link opens the UserCheck Portal. The portal shows a list of attachments the recipient can download.
     - Reference ID.
     Use this ID to send the file to the recipient. You can also find the ID in the logs.

     On the gateway, run the command: **scrub send_orig_email**.
2. Click **OK**.

## SNORT Signature Support

SNORT is a popular, open source, Network Intrusion Detection System (NIDS). For more information about SNORT see snort.org [http://www.snort.org](http://www.snort.org).

Check Point supports the use of SNORT rules as both the GUI and the SmartDomain Manager API’s options.

When you import a SNORT rule, it becomes a part of the IPS database.

You can perform these actions on a Check Point Management Server:

- Import existing SNORT rules from a file
- After import and conversion:
  1. Snort Protection names are Snort imported: `<value of the 'msg' field in the original SNORT rule>`. See Creating SNORT Rule Files (on page 114).
  2. Snort Protections get these attributes automatically:
     - Performance Impact - **High**
     - Severity - **High**
     - Confidence Level - **Low** or **Medium**
  3. Delete the existing SNORT rules

### Importing SNORT Protection Rules to the Security Management Server

Make sure you have the SNORT rule file. It holds SNORT rules and usually has the extension: `.rules`.

In a Multi-Domain Security Management environment, import SNORT rules to the Security Management Server. Then assign Global policy to the Domain Management Servers. This downloads the new SNORT protections to the Domain Management Servers.

**To import SNORT Protection rules to the Security Management Server:**

1. Connect with SmartConsole to the Security Management Server that manages the applicable Security Gateway or Security Cluster.
2. Open the applicable policy.
3. From the left navigation panel, click **Security Policies**.
4. In the top section of **Threat Prevention**, click **Policy**.
5. In the bottom section **Threat Tools**, click **IPS Protections**.
6. From the top toolbar, click **Actions > Snort Protections > Import Snort rules**.
7. Select the file with the SNORT rules and click **Open**.
   - The tool converts the rules to Check Point syntax and updates the protections database.
Important - SmartConsole shows the converted SNORT rules as IPS protections whose names start with Snort imported.

8. Publish the session.

To override the profile settings for a specific SNORT protection, see Action on SNORT Protection Rules (on page 111).

Deleting SNORT Protection Rules from the Security Management Server

To delete SNORT protection rules from the Security Management Server:
1. Connect with SmartConsole to the Security Management Server that manages the applicable Security Gateway or Security Cluster.
2. Open the applicable Policy.
3. From the left navigation panel, click Security Policies.
4. In the top section Threat Prevention, click Policy.
5. In the bottom section Threat Tools, click IPS Protections.
6. From the top toolbar, click **Actions > Snort protections > Delete all snort protections.**

7. Publish the session.

8. Install the **Threat Prevention Policy** on the applicable Security Gateway or Security Cluster.

**Importing SNORT Protection Rules to the Multi-Domain Server**

Make sure you have the SNORT rule file. It holds SNORT rules and usually has the extension: 

```
.rules
```

In a Multi-Domain Security Management environment, import SNORT rules to the Multi-Domain Server. Then assign Global policy to the Domain Management Servers. This downloads the new SNORT protections to the Domain Management Servers.

**To import SNORT rules to the Multi-Domain Server:**

1. Connect with SmartConsole to the Multi-Domain Server to the MDS context.
2. From the left navigation panel, click **Multi Domain > Domains.**
3. Right-click on the **Global Domain** and select **Collect to domain.**
4. From the left navigation panel, click **Security Policies.**
5. Open the applicable global policy.
6. In the top section **Threat Prevention**, click **Policy.**
7. In the bottom section **Threat Tools**, click **IPS Protections**.

8. From the top toolbar, click **Actions > Snort Protections > Import Snort rules**.

9. Select the required file with the SNORT rules and click **Open**.

   The tool converts the rules to Check Point syntax and updates the protections database.

   **Important** - SmartConsole shows the converted SNORT rules as IPS protections whose names start with Snort imported.

10. Publish the session.

11. Close the SmartConsole connected to the Global Domain.

12. From the left navigation panel, click **Multi Domain > Global Assignments**.

13. Reassign the Global Policy to the Local Domains.

14. Connect with SmartConsole to the applicable Domain Management Server that manages the applicable Security Gateway or Security Cluster.

15. Install the **Threat Prevention Policy** on the applicable Security Gateway or Security Cluster.

To override the profile settings for a specific SNORT protection, see Action on SNORT Protection Rules (on page 111).

---

**Deleting SNORT Protection Rules from the Multi-Domain Server**

**To delete SNORT protection rules from the Multi-Domain Server:**

1. Connect with SmartConsole to the Multi-Domain Server to the mds context.

2. From the left navigation panel, click **Multi Domain > Domains**.

3. Right-click on the **Global Domain** and select **Collect to domain**.

4. From the left navigation panel, click **Security Policies**.

5. Open the applicable global policy.

6. In the top section **Threat Prevention**, click **Policy**.

7. In the bottom section **Threat Tools**, click **IPS Protections**.
8. From the top toolbar, click **Actions > Snort Protections > Delete all Snort protections.**

9. Publish the session.
10. Close the SmartConsole connected to the Global Domain.
11. From the left navigation panel, click **Multi Domain > Global Assignments.**
12. Reassign the Global Policy to the Local Domains.
13. Connect with SmartConsole to the applicable Multi-Domain Server that manages the applicable Security Gateway or Security Cluster.

### Action on SNORT Protection Rules

The Security Gateway enforces SNORT protection rules based on the profile which is installed on the Security Gateway. For example, if the profile installed on the Security Gateway is **Optimized**, by default the Security Gateway does not enforce SNORT protection rules, because their performance impact is **High** and the allowed performance impact defined in the **Optimized** profile is **Medium** or lower.

**To override the profile settings for a specific SNORT protection:**

1. In **IPS Protections**, right-click a SNORT protection and select **Edit.**
Note - The SNORT protection names start with **Snort imported**.

2. Right-click the profile and select **Edit**.

3. In the **Main Action** area, select **Override with**.

4. From the drop-down menu, select the required action.

5. Click **OK**.
6. Click **Close**.
7. Publish the session.
8. Install the Threat Prevention Policy.

**Note** - The images here follow the example described above. If you are on a different profile, or want a different action, change steps 2 or 4 accordingly.

**Alternative Methods to add and delete SNORT Protection Rules**

These alternative methods on the Management Server let you can add and delete SNORT protection rules:

- `mgmt_cli` tool
- SmartConsole CLI
- Gaia Clish
• POST Requests

Adding SNORT Rules

The applicable command accepts two arguments:
• package-format” which always takes the string value “snort”
• “package-path” which is the path to the protections’ package

The command returns:
Upon success: 0
Upon failure: 1 along with several parameters describing the error upon failure

Examples:
• From the mgmt_cli tool, run this command:
  mgmt_cli add threat-protections package-path "/path/to/community.rules" package-format "snort" --version 1.2 --format json

• From the SmartConsole CLI, run this command:
  add threat-protections package-path "/path/to/community.rules" package-format "snort" --version 1.2 --format json

• From the Gaia Clish, run this command:
  mgmt add threat-protections package-path "/path/to/community.rules" package-format "snort" --version 1.2 --format json

Note - The --format json part is optional. By default, the output is presented in plain text.

• POST Request Method
  A post request must:
  • Be sent to the following URL: https://<ip-address-of mgmt-server>:<port>/web_api/v1.2/add-threat-protections
  • Have the request headers **Content-Type** set to **application/json** and **X-chkp-sid** set to the unique session identifier returned by the login request.
  • Have the Content-Type arguments **package-format** and **package-path** in the request body.

The server returns:
Upon success: Status code 200
Upon failure: The appropriate status code

Example:
```
POST {{server}}/v1.2/add-threat-protections
Content-Type: application/json
X-chkp-sid: {{session}}
{
  "package-path" : "/path/to/community.rules",
  "package-format" : "snort"
}
```

Deleting SNORT Protections

The applicable command accepts one argument “package-format”, which always takes the string value “snort”.
The command returns:

Upon success: 0
Upon failure: 1 along with several parameters describing the error upon failure

Examples:

- From the `mgmt_cli` tool, run this command:
  ```
  mgmt_cli delete threat-protections package-format "snort" --version 1.2
  ```

- From the SmartConsole CLI, run this command:
  ```
  delete threat-protections package-format "snort" --version 1.2
  ```

- From the Gaia Clish, run this command:
  ```
  mgmt delete threat-protections package-format "snort" --version 1.2
  ```

- POST Request method
  A POST Request must be send to this URL:
  ```
  https://<IP-address-of-mgmt-server>:<port>/web_api/v1.2/delete-threat-protections
  ```

With the request headers `Content-Type` set to `application/json` and `X-chkp-sid` set to the unique session identifier returned by the login request. The argument `package-format` must be sent in the request body.

The server returns:

Upon success: Status code 200
Upon failure: The appropriate status code

Example:

```
POST {{server}}/v1.2/delete-threat-protections
Content-Type: application/json
X-chkp-sid: {{session}}
{
  "package-format" : "snort"
}
```

Creating SNORT Rule Files

You can write your own SNORT rules and then import them to a Check Point Management Server to become IPS protections. For more information about SNORT, see snort.org


Check Point supports SNORT 2.9 version and lower.

SNORT rules use signatures to define attacks. A SNORT rule has a rule header and rule options. The name of the imported SNORT protection is the value of the `msg` field in the original SNORT rule.

- If one SNORT rule has multiple `msg` strings with the same value, Management Server aggregates these values in one IPS SNORT protection.
- If you import a SNORT rule at different times, and it has the same `msg` string, the latest import overrides the existing IPS SNORT protection.
SNORT Rule Syntax:

```plaintext
<Action> <Protocol> <Source IP Address> <Source Port> <Direction> <Destination IP Address> <Destination Port> (msg:"<Text>"; <Keyword>:"<Option>");
```

SNORT rules have two logical parts: Rule Header and Rule Options.

- **SNORT Rule Header:**
  ```plaintext
  <Action> <Protocol> <Address> <Port> <Direction> <Address> <Port>
  <keyword>:"<option>"
  ```

**Example:**

```plaintext
alert tcp any any -> any 1:65535 (msg:"Possible exploit"; content:"|90|";)
```

Where:

- **Action** = alert
- **Protocol** = TCP
- **Source IP Address** = any
- **Source Port** = any
- **Direction** = ->
- **Destination IP Address** = any
- **Destination Port** (Range) = 1:65535
- **Name of protection rule in IPS** = Possible exploit
- **Keyword** = content
- **Option** = |90|

Supported Snort syntax:

These are the generally supported syntax components. There are some limitations (on page 116).

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>length</td>
<td>Specifies the original length of the content that is specified in a protected_content rule digest</td>
</tr>
<tr>
<td>pcree</td>
<td>Lets you write rules with Perl-compatible regular expressions. Example: alert tcp any any -&gt; any 80 (content:&quot;/foo.php?id=&quot;; pcree:&quot;///foo.php?id=[0-9]{1,10}/iU&quot;);</td>
</tr>
<tr>
<td>flowbits</td>
<td>Lets rules track states during a transport protocol session. Used in conjunction with conversation tracking from the Session preprocessor. Example: alert tcp $HTTP_SERVERS any -&gt; $EXTERNAL_NET 21 (msg:&quot;Does not match state in FTP path&quot;; flow: established, to_server; content: &quot;targetfile&quot;; nocase; fast_pattern; flow bits: isset,INFTPBPATH,no_match);</td>
</tr>
<tr>
<td>Keyword</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| byte_test  | Tests a byte field for a specific value [with operator]. Example:
  `alert udp $EXTERNAL_NET any -> $HOME_NET 123 (msg: "Header length longer than maximum"); content: "length|3d|"; byte_test: 4, >, 1024, 1, relative;)` |
| byte_jump  | Lets you write rules that skip over specific portions of the length-encoded protocols and perform detection in very specific locations. Example:
  `alert udp any any -> any 123 (msg: "Check for 0001 after 0123"; content: |30 31 32 33|; byte_jump: 4,4, relative; content: |30 30 30 31|; distance: 1; relative;)` |
| isdataat   | Verifies that the payload has data at a specified location. Example:
  `alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg: "\r\n\r\nHas 300 byte after"); flow: established, to_server; content: |0a 0d 0a 0d|; isdataat: 300,relative; sid:11111111;)` |
| no_match   | Does not block traffic even if the rule matches. Used with the "flow bits" key word to set a flag without performing a block. Example:
  `alert tcp $HTTP_SERVERS any -> $EXTERNAL_NET 21 (msg: "Does not match state in FTP path"); flow: established, to_server; content: "targetfile"; nocase; fast_pattern; flow bits: isset,INFTPATH,no_match; sid: 55555555;)` |

- Supported Content Keyword Modifiers: "nocase“, “rawbytes“, “depth“, “offset:“, “distance:“, “within“, ”urilen“
- Supported Threshold Rule Types - Threshold, Both [Limit is not supported.]
- Supported Macros - HTTP_PORTS [Interpreted as 80 and 8080 ports.]

**Note** - Make sure that SNORT Rules with the same `flowbits` flag have the same content in the `msg` field. Otherwise, they will not be under the same protection.

**Debugging:**
The `$FWDIR/log/SnortConvertor.elf` file on the Management Server contains is updated with the debug messages from the last SnortConvertor run import of SNORT rules.

To find failed rule debugs in this file, search for `Failed to convert rule`

**Unsupported SNORT Syntax**
This syntax is not supported and will not convert:
- pcire regular expression with lookahead assertion: ?!
- Using `byte_test` keyword with operator not in: <, >, =, & , ^
- `http_method` is not supported if it is the only http modifier type in the Snort Rule
- Protocols: icmp, ip, [all is interpreted as UDP and TCP protocols]
- Snort Rule without content keyword
- All `PORT` macros, except `HTTP_PORTS`
- Specification of source port (only any is supported)
• Specification of destination port "any" (you must specify an exact destination port number, or range of destination port numbers).

The conversion will change the behavior of these macros and syntax.

• Specification of IP Addresses – Enforced on all IP Addresses.
  • HOME_NET macro - Interpreted as any IP Addresses.
  • EXTERNAL_NET macro - Interpreted as any IP Addresses.
  • HTTP_SERVERS macro - Interpreted as any IP Addresses.

These combinations of keywords and modifiers are implemented differently in the IPS blade as Snort protection rules than in SNORT Rules. **Best Practice** - Test them before activating them in a production environment.

• rawbytes content, or B pcre modifiers with http_uri content or U pcre modifiers

• With http content or pcre modifiers:
  • http_raw_uri content or I pcre modifiers
  • http_stat_msg content or Y pcre modifiers
  • http_stat_code content or S pcre modifiers

• Without http content or pcre modifiers:
  • Two or more uses of http_header content or H pcre modifiers
  • Two or more uses of http_raw_header content or D pcre modifiers

• With depth or offset content and http content that is one of these on the same content keyword, or ^ (carrot) in pcre with one of these http pcre modifiers on the same pcre keyword:
  • http_header content or H pcre modifiers
  • http_raw_header content or D pcre modifiers
  • http_stat_msg content or Y pcre modifiers
  • http_stat_code content or S pcre modifiers
  • http_uri content or U pcre modifiers

• Use of depth or offset content, or ^ (carrot) in pcre, without any http content, and with destination ports that are not HTTP_PORTS macro
  • http_client_body content or F pcre modifier

• A pcre keyword with () (curly braces) quantifier

• Use of both content and byte_test keywords

• http_header content modifiers or H pcre modifiers enforced only on raw http data (not decoded and normalized header data)

• Use of the urilen keyword, except in a SNORT Rule that has only http_uri and U pcre modifiers, or http_raw_uri content modifier and I pcre modifiers.
  • If the SNORT Rule has only http_uri content or U pcre modifiers, the size will be of the decoded and normalized buffer.
  • If the SNORT Rule has only http_raw_uri content or I pcre modifiers, the size will be of the raw uri buffer.
Optimizing IPS

IPS is a robust solution which protects your network from threats. Implementation of the recommendations in this chapter 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, which places greater weight on protocols such as HTTP, DNS, and SMTP. If your network traffic has high levels of other network protocols, you need to take that into consideration when you assess the 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.

Bypass Under Load

To help you integrate IPS into your environment, enable Bypass Under Load on the Gateway to disengage IPS activities during times of heavy network usage. IPS inspection can make a difference in connectivity and performance. Usually, the time it takes to inspect packets is not noticeable, but under heavy loads it may be a critical issue. IPS allows traffic to pass through the gateway without inspection, and IPS then resumes inspection after gateway’s resources return to acceptable levels.

Best Practice - Because IPS protections are temporarily disabled, apply Bypass Under Load only during the initial deployment of Threat Prevention. After you optimize the protections and performance of your Gateway, disable this feature to make sure that your network is protected against attacks.

To bypass IPS inspection under heavy load:

1. In SmartConsole, click Gateways & Servers and double-click the Security Gateway.
   The gateway window opens and shows the General Properties page.
2. From the navigation tree, click IPS.
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.
9. Click OK.
10. Install Policy.

Tuning Protections

This section shows you how to tune protections to suit your needs.
**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.

**Best Practice** - 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.

*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.

**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**

**SecureXL**


**CoreXL**

For Security Gateways running on multi-core hardware, CoreXL lets 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 R80.20 Performance Tuning Administration Guide https://sc1.checkpoint.com/documents/R80.20_GA/WebAdminGuides/EN/CP_R80.20_PerformanceTuning_AdminGuide/html_frameset.htm.
Using the Whitelist

Whitelist is a list of files that are trusted. Check Point Threat Prevention engine does not inspect trusted files for malware, viruses, and bots, which helps decrease resource utilization on the gateway.

Adding a File to the Whitelist

To configure files on the Threat Prevention Whitelist:

1. In SmartConsole, click Security Policies > Threat Prevention > Policy > Threat Tools > Whitelist Files.
2. Click New.
   The Whitelist File window opens.
3. Enter the Object Name and MD5 signature for the new file exception.
   Note - To edit or remove Whitelist files, right-click the file and select the applicable option.
4. Click OK.
5. Install the Threat Prevention policy.

Threat Indicator Settings

Threat Indicators lets you upload Indicator (on page 12) files that contain sets of observables (on page 12). These observables are added to the Threat Prevention policy.

Indicator – Set of observables which represent a malicious activity in an operational cyber domain, with relevant information on how to interpret it and how to handle it.

Observable – An event or a stateful property that can be observed in an operational cyber domain. For example: IP address, MD5 file signature, URL, Mail sender address.

Indicators of Compromise convey an attack campaign by:
- Specific observable patterns
- Additional information intended to represent artifacts & behaviors of interest within a cyber-security context

Indicators are derived from intelligence, self-analysis and/or governments, partners etc.

To use Threat Indicators:

Indicator files must be in CSV or STIX XML format, and contain records of equal size. If an Indicator file has records which do not have the same number of fields, it will not load.

Each record in the Indicator file has these fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Valid Values</th>
<th>Value Criteria</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIQ-NAME</td>
<td>Name of the observable</td>
<td>Free text</td>
<td>Must be unique</td>
<td>No</td>
</tr>
<tr>
<td>VALUE</td>
<td>A value that is valid for the type of the observable</td>
<td>See the table below</td>
<td>See the table below</td>
<td>No</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Valid Values</td>
<td>Value Criteria</td>
<td>Optional</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------</td>
<td>---------------------------------------</td>
<td>----------------------</td>
<td>----------</td>
</tr>
<tr>
<td>TYPE</td>
<td>Type of the observable</td>
<td>• URL</td>
<td>Not case sensitive</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Domain</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IP Range</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MD5</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Mail-subject</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Mail-from</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Mail-to</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Mail-cc</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Mail-reply-to</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CONFIDENCE</td>
<td>Degree of confidence the observable</td>
<td>• low</td>
<td>Default - high</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>presents</td>
<td>• medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• high</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• critical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEVERITY</td>
<td>Degree of threat the observable presents</td>
<td>• low</td>
<td>Default - high</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• high</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• critical</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRODUCT</td>
<td>Check Point Software Blade that processes</td>
<td>• AV</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>the observable</td>
<td>• AB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COMMENT</td>
<td>Free text</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Notes** -
- If an optional field is empty, the default value is used.
- If a mandatory field is empty, the Indicator file will not load.

These are the values that are valid for each observable type:

<table>
<thead>
<tr>
<th>Observable Type</th>
<th>Validation Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Any valid URL</td>
</tr>
<tr>
<td>Domain</td>
<td>Any URL domain</td>
</tr>
<tr>
<td>IP</td>
<td>Standard IPv4 address</td>
</tr>
</tbody>
</table>
### Requirements for validation of CSV Indicator files:

- Use commas to separate the fields in a record
- Enter one record per line, or use `\n` to separate the records
- If free text contains quotation marks, commas, or line breaks, it must be enclosed in quotation marks
- To enclose part of free text in quotations, use double quotation marks: `""<text>""`

### Notes -

- As of this release, STIX 2.0 (JSON file) is not supported.
- Custom Indicators CLI `load_indicators` are not supported.
- SHA1/SHA256 is not supported as a valid MD5 value.
- **Condition Type Enum** and **Condition Application Enum** support **Equals** and **Any**.

---

### Example of a CSV Indicator File

```
# ! DESCRIPTION = indi file,,
# ! REFERENCE = Indicator Bulletin; Feb 20, 2014,,
# FILE FORMAT:,
# All lines beginning ""#"" are comments,,
# All lines beginning ""#!"" are metadata read by the SW",
# UNIQ-NAME,VALUE,TYPE,CONFIDENCE,SEVERITY,PRODUCT,COMMENT,,
observ1,8d9b6b8912a2ed175b77acc40ceb9a73,MD5,medium,medium,AV,FILENAME:WUC Invitation Letter Guests.doc
observ2,76700f862a0c241b8f4b754f76957bda,MD5,high,high,AV,FILENAME:essais-.swf|
NOTE:FWS type Flash file
observ7,http://somemaliciousdomain.com/uploadfiles/upload/exp.swf?info=789c333432d333b4d4b330d77acd40cbe9a73,MD5,medium,medium,AV,FILENAME:WUC
observ8,svr01.passport.ServeUser.com,Domain,low,high,AB,TCP:80|
IPV4ADDR:196.168.25.25
```
Example of a STIX 1.0 XML Indicator File

```xml
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://stix.mitre.org/stix-1"
    xmlns:indicator="http://stix.mitre.org/Indicator-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xsi:schemaLocation="http://stix.mitre.org/stix-1 ../stix_core.xsd
                        http://stix.mitre.org/Indicator-2 ../indicator.xsd
                        http://stix.mitre.org/default_vocabularies-1
                        http://cybox.mitre.org/objects#FileObject-2 ..cybox/objects/File_Object.xsd
                        http://cybox.mitre.org/default_vocabularies-2
                        ...
                        http://cybox.mitre.org/default_vocabularies.xsd"
    id="example:STIXPackage-ac823873-4c51-4dd1-936e-a39d40151cc3"
    version="1.0.1">
  <stix:STIX_Header>
    <stix:Title>Example file watchlist</stix:Title>
    <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators - Watchlist</stix:Package_Intent>
  </stix:STIX_Header>
  <stix:Indicators>
    <stix:Indicator id="example:Indicator-611935aa-4db5-4b63-88ac-ac651634f09b">
      <stix:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">File Hash Watchlist</stix:Type>
      <stix:Description>Indicator that contains malicious file hashes.</stix:Description>
      <stix:Observable id="example:Observable-c9ca84dc-4542-4292-af54-3c5c914ccbcc">
        <cybox:Object id="example:Object-c670b175-bfa3-48e9-a218-aa7c55f1f884">
          <cybox:Properties xsi:type="FileObj:FileObjectType">
            <FileObj:Hashes>
              <cyboxCommon:Hash xsi:type="cyboxVocabs:HashNameVocab-1.0" condition="Equals">MD5</cyboxCommon:Hash>
            </FileObj:Hashes>
          </cybox:Properties>
        </cybox:Object>
      </stix:Observable>
    </stix:Indicator>
  </stix:Indicators>
</stix:STIX_Package>
```
Configuring Advanced Threat Prevention Settings

<cyboxCommon:Simple_Hash_Value
condition="Equals"
apply_condition="ANY">0522e955aaee70b102e843f14c13a92c##comma##0522e955aaee70b102e843f14c13a92d##comma##0522e955aaee70b102e843f14c13a92e</cyboxCommon:Simple_Hash_Value>
</cyboxCommon:Hash>
</FileObj:Hashes>
</cybox:Properties>
</cybox:Object>
</indicator:Observable>
</stix:Indicator>
</stix:Indicators>
</stix:STIX_Package>

Configuring Indicators in SmartConsole

Define network objects to hold the Indicator files.

To load Indicators:
   The Indicators page opens.
2. Click New.
   The Indicators configuration window opens.
3. Enter a Name.
   Each Indicator must have a unique name.
4. Enter Object Comment (optional).
5. Click Import to browse to the Indicator file.
   The content of each file must be unique. You cannot load duplicate files.
6. Select an action for this Indicator:
   • Ask - Threat Prevention Software Blade asks what to do with the detected observable
   • Prevent - Threat Prevention Software Blade blocks the detected observable
   • Detect - Threat Prevention Software Blade creates a log entry, and lets the detected observable go through
   • Inactive - Threat Prevention Software Blade does nothing
7. Add Tag.
8. Click OK.
   If you leave an optional field empty, a warning notifies you that the default values will be used in the empty fields. Click OK. The Indicator file will load.

To delete Indicators:
1. Select an Indicator.
2. Click Delete.
3. In the window that opens, click Yes to confirm.

You can edit properties of an Indicator object, except for the file it uses. If you want an Indicator to use a different file, you must delete it and create a new one.

Using Anti-Bot and Anti-Virus with VSX

When you configure Virtual Systems to use the Anti-Bot and Anti-Virus Software Blades, make
sure the Software Blade:

- Is enabled and configured on the relevant Virtual Systems and enabled and configured on the VSX Gateway (VSO)
  VSO handles contract validation for all Virtual Systems.
- Can connect to the internet
  A Virtual System gets updates through the VSX Gateway (VSO). If the VSX Gateway fails, each Virtual System uses its proxy settings to get the update from the internet.

**Note** - Where applicable, make sure the routing, DNS, and proxy settings for the VSX Gateway (VSO) are configured correctly.

**To enable Anti-Bot and Anti-Virus on Virtual Systems:**

1. If applicable, configure proxy settings for the VSX Gateway (VSO) or the Virtual Systems or both:
   a) From the **Network Object** tree, double-click the VSX Gateway (VSO).
   b) From the navigation tree, select **Topology > Proxy**.
   c) Configure the proxy settings, and click **OK**.
2. Enable **Anti-Bot** and **Anti-Virus** on the VSX Gateway (VSO) for all Virtual Systems that use **Anti-Bot** and **Anti-Virus**:
   a) From the **Network Object** tree, double-click the Virtual System.
   b) In the **Network Security** section, select **Anti-Bot** and **Anti-Virus**.
   c) Click **OK**.
3. Select the Threat Prevention and configure the policies.
4. Install the Threat Prevention policy (and access policy if needed) on the VSX Gateway (VSO) and the relevant Virtual Systems.

**Using Threat Extraction with VSX**

When you configure Virtual Systems to use the Threat Extraction Software Blade, make sure that the Software Blade:

- Is enabled and configured on the relevant Virtual Systems and enabled and configured on the VSX Gateway (VSO).
- The Virtual Systems are configured with a Mail Transfer Agent (MTA).

**Note** - Where applicable, make sure that the routing, DNS, and proxy settings for the VSX Gateway (VSO) are configured correctly.

**To enable Threat Extraction on Virtual Systems:**

1. In the Gateways & Servers view, right-click the Virtual System object and select **Edit**. The **Virtual System Properties** window opens.
3. In the **Next Hop Configuration** window, select **Skip this configuration now**, and click **Next**.
4. In the **Summary** window, click **Finish**.
5. In the VS Properties window, go to Mail Transfer Agent in the navigation tree, and select Enable as Mail Transfer Agent (MTA).
6. Add the MTA definitions to **Mail Forwarding**.
7. Click **OK**.
8. Install the Standard policy on the Virtual Systems (including VS0).

### Threat Prevention CLI Commands

You can run commands from the CLI (Command Line Interface) to install Threat Prevention policy and for IPS and advanced Threat Emulation management.

In any case of conflict between the CLI commands and the SmartConsole configuration, the CLI commands will be enforced.

#### mgmt_cli install-policy

**Description:** Run this command on the Security Management Server to install the Threat Prevention policy on the specified Security Gateways.

**Syntax:**

```
mgmt_cli install-policy <options>
```

**Note:** For more information, see Management API Reference [https://sc1.checkpoint.com/documents/latest/APIs/index.html](https://sc1.checkpoint.com/documents/latest/APIs/index.html).

#### te_add_file

**Description:** Use this command to manually send files for threat emulation. The command has to be run from expert mode. For a complete explanation of all the available parameters, run `te_add_file`.

**Syntax:**

```
te_add_file -f=<file path> -d=<directory path>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f=</td>
<td>Specifies the path to the file. You must include the file name at the end of the path.</td>
</tr>
<tr>
<td>-d=</td>
<td>Specifies the path to a directory. The command takes all the files in the directory and sends them for emulation.</td>
</tr>
</tbody>
</table>

**Example:**

```
te_add_file -f=/home/admin/test.pdf
```

[Expert@gaia]# te_add_file -f=/home/admin/test.pdf

# Sending files... Wait for response: True
# Trying to connect to ted...
# Connected to ted...Ready to send...
# File path: /home/admin/test.pdf
# File type: pdf
# Got response from ted...

```{json}
{
    :event_id ("000000A5-006D-0045-9D15-D6896862D148")
    :action (drop)
    :confidence (high)
    :done (0)
    :file_path ("/home/admin/test.pdf")
    :md5_string (61baabd6fc12e01ff73ceacc07c84f9a)
}
```
# Got response from ted...
{
    :event_id ("{000000A5-006D-0045-9D15-D6896862D148}")
    :action (drop)
    :confidence (high)
    :done (1)
    :file_path ("/home/admin/test.pdf")
    :md5_string (61baabd6fc12e01ff73ceacc07c84f9a)
}

/home/admin/test.pdf
Verdict: drop Time: 1 *

Total Files: 1
Verdicts distribution:
drop: 1

# Done 1 files in 1 seconds...Bye Bye...

Comments: ted is the Threat Emulation daemon.

tecli

Use the tecli commands to:
  - Control local cache
  - Show information about the Threat Emulation system
  - Run advanced options
  - Show status of emulation downloads, statistics and processes
  - Configure affinity for TED [Threat Emulation Daemon]

**tecli advanced clear**

**Description:** Resets the emulation statistics for the Security Gateway or appliance.
**Syntax:** tecli advanced clear

**tecli cache clean**

**Description:** Deletes all the records in the local cache.
**Syntax:** tecli cache clean

**tecli control sizing**

**Description:** Controls the sizing mode tool that lets you estimate the resources that Threat Emulation will use in your network http://supportcontent.checkpoint.com/solutions?id=sk93598.
**Syntax:** tecli control sizing {enable|disable|status}

**Note:** For more about using sizing mode, go to sk93598 http://supportcontent.checkpoint.com/solutions?id=sk93598.

**tecli debug**

**Description:** Enable and disable debug mode for Threat Emulation.
**Syntax:** tecli debug {on|off|scan local {enable|disable}}
### Configuring Advanced Threat Prevention Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Enables debug mode</td>
</tr>
<tr>
<td>off</td>
<td>Disables debug mode</td>
</tr>
<tr>
<td>scan local</td>
<td>Enables the appliance or Security Gateway to scan local connection</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>scan local</td>
<td>Disables the appliance or Security Gateway to scan local connection</td>
</tr>
<tr>
<td>disable</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

`tecli d o r tecli debug on`

`tecli d s l e o r tecli debug scan local enable`

**tecli show**

The `tecli show` commands show data and statistics about the Threat Emulation Software Blade. You can also use abbreviated parameters to run `tecli show` commands. These are some useful command combinations:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tecli s s</td>
<td>Shows emulation statistics</td>
</tr>
<tr>
<td>tecli s c i</td>
<td>Shows information about ThreatCloud emulation</td>
</tr>
<tr>
<td>tecli s c q</td>
<td>Shows the quota for ThreatCloud emulation</td>
</tr>
<tr>
<td>tecli s e e</td>
<td>Shows the current status of the emulation queue</td>
</tr>
<tr>
<td>tecli s u a</td>
<td>Shows all the parts of file emulation</td>
</tr>
</tbody>
</table>

**tecli show cloud**

**Description:** Shows data and statistics about your ThreatCloud account.

**Syntax:** `tecli show cloud {identity|info|quota}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>identity</td>
<td>Shows data about how the Security Gateway or Emulation appliance connects to the ThreatCloud</td>
</tr>
<tr>
<td>info</td>
<td>Shows data about your file emulation in the ThreatCloud</td>
</tr>
<tr>
<td>quota</td>
<td>Shows data about your ThreatCloud monthly emulation quota</td>
</tr>
</tbody>
</table>

**Example:**

`tecli s c id o r tecli show cloud identity`

`tecli s c in o r tecli show cloud info`

**tecli show emulator**

**Description:** Shows data about Threat Emulation queue and VMs (Virtual Machines).

**Syntax:** `tecli show emulator {emulations|vm {synopsis|detailed|id <ID>}}`
### emulations

- **Parameter:** emulations
  - **Description:** Shows the current status of the emulation queue

### synopsis
- **Parameter:** synopsis
  - **Description:** Shows a summary of the VMs

### detailed
- **Parameter:** detailed
  - **Description:** Shows data and details of the VMs

### id <ID>
- **Parameter:** id <ID>
  - **Description:** Shows data for the VM with this ID

#### Example:

```
tecli s e e or tecli show emulator emulations
```

```
tecli s e v s or tecli show emulator vm synopsis
```

### tecli show downloads

**Description:** Shows data and statistics about files and rules that Threat Emulation is downloading.

**Syntax:** `tecli show downloads {all|images|dr|sa|raw|types}`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Shows the status of all downloads</td>
</tr>
<tr>
<td>images</td>
<td>Shows download status of operating system images</td>
</tr>
<tr>
<td>dr</td>
<td>Shows download status of malware detection rules</td>
</tr>
<tr>
<td>sa</td>
<td>Shows download status of static analysis rules</td>
</tr>
<tr>
<td>raw</td>
<td>Shows download status of general Threat Emulation files</td>
</tr>
<tr>
<td>types</td>
<td>Shows the file extensions that are being sent for emulation</td>
</tr>
</tbody>
</table>

#### Example:

```
tecli s d a or tecli show downloads all
```

```
tecli s d i or tecli show downloads images
```

### tecli show remote

**Description:** Shows data and statistics about the Emulation appliance

**Syntax:** `tecli s r i or tecli show remote information`

### tecli show statistics

**Description:** Shows statistics to the Emulation appliance or Security Gateway.

**Syntax:** `tecli s s or tecli show statistics`
tecli show throughput

**Description:** Shows data about file emulation for each time interval.

**Syntax:** tecli show throughput {minute|hour|day|month}

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>minute</td>
<td>Shows how many files completed emulation for each minute</td>
</tr>
<tr>
<td>hour</td>
<td>Shows how many files completed emulation for each hour</td>
</tr>
<tr>
<td>day</td>
<td>Shows how many files completed emulation for each day</td>
</tr>
<tr>
<td>month</td>
<td>Shows how many files completed emulation for each month</td>
</tr>
</tbody>
</table>

**Example:**

```
tecli show throughput minute
```

**tecli show unit**

**Description:** Shows all the parts of file emulation:

- Prepare
- Processing
- Finalizing

The output shows the number of files for each task in the emulation part.

**Syntax:** tecli u a or tecli show unit all
Managing IPS gateways - CLI

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

To see all available commands:
1. On the gateway, go to the expert mode.
2. Type `ips` and press **Enter**.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| ips on/off [-n]    | Enable or disable IPS on the Security Gateway.  
<p>|                    | <strong>-n</strong> Empty templates table [applies <code>fwaccel off</code>; <code>fwaccel on</code> immediately]. Otherwise, this command takes effect in a few minutes. |
| ips stat           | Show the IPS status of the Security Gateway.                                |
| ips bypass stat    | Show the Bypass Under Load status.                                          |
| ips bypass on/off  | Enable or disable Bypass Under Load.                                        |
| ips bypass set cpulmem low|high &lt;threshold&gt;                                                               |
|                    | Set the Bypass Under Load threshold.                                        |
|                    | <strong>threshold</strong> Valid range is 1 to 99. Unit is percent.                      |
| ips debug [-e filter] -o &lt;output_file&gt; | Create an IPS debug file. Filter valid values are the same as for <code>fw ctl debug</code>. Consult with Check Point Technical Support. |
| ips refreshcap     | Refresh the sample capture repository.                                      |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ips stats [&lt;ip_address&gt; -m] [-g &lt;seconds&gt;] [&lt;ip_address&gt; &lt;seconds&gt;]</td>
<td>Print IPS and Pattern Matcher performance statistics. Without arguments, runs on current Security Gateway for 20 seconds. This is a resource intensive command. Do not run it on a system with a high load.</td>
</tr>
<tr>
<td>-g</td>
<td>Collect statistics for current Security Gateway.</td>
</tr>
<tr>
<td>seconds</td>
<td>period in which statistics are gathered</td>
</tr>
<tr>
<td>ips pmstats reset</td>
<td>Reset pattern matcher statistics.</td>
</tr>
<tr>
<td>ips pmstats -o &lt;output_file&gt;</td>
<td>Print pattern matcher statistics.</td>
</tr>
</tbody>
</table>
Configuring Advanced Threat Emulation Settings

In This Section:

Updating Threat Emulation...........................................................................................................133
Fine-Tuning the Emulation Appliance..............................................................................................134

Updating Threat Emulation

Threat Emulation connects to the ThreatCloud to update the engine and the operating system images. The default setting for the Threat Emulation appliance is to automatically update the engine and images.

The default setting is to download the package once a day.

Best Practice - Configure Threat Emulation to download the package when there is low network activity.

Update packages for the Threat Emulation operating system images are usually more than 2GB. The actual size of the update package is related to your configuration.

To enable or disable Automatic Updates for Threat Emulation:

1. In SmartConsole, select Security Policies > Threat Prevention.
2. From the Threat Tools section, click Updates.
   
   The Updates page opens.


4. Select or clear these settings:
   
   - Enable Threat Emulation engine scheduled update
   - Enable Threat Emulation images scheduled update

5. Click Configure to configure the schedule for Threat Emulation engine or image updates.

6. Configure the automatic update settings to update the database:
   
   - To update once a day, select At and enter the time of day
   - To update multiple times a day, select Every and set the time interval
   - To update once or more for each week or month:
     a) Select At and enter the time of day.
     b) Click Days.
     c) Click Days of week or Days of month.
     d) Select the applicable days.

7. Click OK and then install the Threat Prevention policy.
Updating Threat Emulation Images

Update packages for the Threat Emulation operating system images are usually more than several Gigabytes. The actual size of the update package is related to your configuration.

The default setting is to download the package once a week on Sunday. If Sunday is a work day, we recommend that you change the update setting to a non-work day.

To update the operating system image for Threat Emulation on a gateway:

1. In SmartConsole, select Security Policies > Threat Prevention.
2. From the Threat Tools section, click Updates.
   The Updates page opens.
4. Select a gateway and click OK.
5. Install the Threat Prevention policy.

Fine-Tuning the Emulation Appliance

You can change these advanced settings on the Emulation appliance to fine-tune Threat Emulation for your deployment.

Emulation Limits

To prevent too many files that are waiting for emulation, configure these emulation limits settings:

- Maximum file size
- Maximum time that the Software Blade does emulation
- Maximum time that a file waits for emulation in the queue (for Emulation appliance only)

If emulation is not done on a file for one of these reasons, the Fail Mode settings for Threat Prevention define if a file is allowed or blocked.

You can configure the maximum amount of time that a file waits for the Threat Emulation Software Blade to do emulation of a file. There is a different setting that configures the maximum amount of time that emails are held in the MTA.

If the file is waiting for emulation more than the maximum time:

- Threat Emulation Software Blade - The Threat Prevention profile settings define if a file is allowed or blocked
- MTA - The MTA settings define if a file is allowed or blocked

Configuring Emulation Limits

1. In SmartConsole, select Manage & Settings > Blades > Threat Prevention > Advanced Settings.
   The Threat Emulation Engine Settings window opens.
2. Click Configure settings.
   The Threat Emulation Settings window opens.
3. Configure the settings for the emulation limits.
   - From When limit is exceeded traffic is accepted with track, select the action if a file is not
sent for emulation:
- None - No action is done
- Log - The action is logged
- Alert - An alert is sent to SmartView Monitor

4. Click **OK** and then install the policy.

**Changing the Local Cache**

When a Threat Emulation analysis finds that a file is clean, the file hash is saved in a cache. Before Threat Emulation sends a new file to emulation, it compares the new file to the cache. If there is a match, it is not necessary to send it for additional emulation. Threat Emulation uses the cache to help optimize network performance.

**Best Practice** - Do not change this setting.

**Changing the Size of the Local Cache**

1. In SmartConsole, select **Manage & Settings > Blades > Threat Prevention > Advanced Settings**.
   The **Threat Prevention Engine Settings** window opens.
2. Click **Configure Settings**.
   The **Threat Emulation Settings** window opens.
3. From **Number of file hashes to save in local cache**, configure the number of file hashes that are stored in the cache.
4. Click **OK** and then install the policy.

**Threat Emulation Virtual Interface**

The Emulation appliance must have a virtual IP address and netmask to do file emulation. This setting is not used for emulation in the ThreatCloud.

⚠️ **Important** - Only change this virtual IP address if it is already used in your network.

**To change the IP address of the virtual interface:**

1. In SmartConsole, select **Manage & Settings > Blades > Threat Prevention**.
2. Under **Threat Prevention**, click **Advanced Settings**.
3. Scroll down and from the **Threat Emulation Settings** section, click **Configure settings**.
   The **Threat Emulation Settings** window opens.
4. Enter the **Network** and **Mask** for the IP address for the virtual interface.
5. Click **OK** and then install the policy.
Threat Prevention API

In This Section:

What is the Threat Prevention Web API? ................................................................. 136
Using the Local Threat Extraction Web API ......................................................... 136

What is the Threat Prevention Web API?

The Security Gateways inspect files intercepted from traffic. With the Threat Prevention API, you can upload files which were intercepted by traffic for inspection by the Security Gateways.

For example: The organizational Human Resources portal receives CVs from external users. When the files are sent directly to the Security Gateway, the Threat Emulation process can take a few minutes, during which the user must wait for a message that the file was uploaded. To improve user experience and prevent the wait, you can keep these files in a separate container, let the user know that the files were uploaded, and only then use the API to send the files for inspection by the gateway.

There are two types of Threat Prevention API:


• Local API on the gateway which supports only Threat Extraction (on page 136).

Using the Local Threat Extraction Web API

To use the Threat Extraction API, you need to create an API key. After you create the API key, you can use it to connect to the gateway and send files for extraction.

To create the Threat Extraction Web API key:

1. In SmartConsole, double-click the gateway.
2. From the navigation tree, select Threat Extraction.
3. Select Enable API.
4. Install Policy.

The Web API key is created.

After the Web API key is created, you can deploy it to the clients.

To find the Web API key:

1. Open the CLI.
2. Open this file: vi/opt/CPUserCheckPortal/phpincs/conf/TPAPI.ini
3. The API key is in the api_key field.

   Note – You can change the api_key in the TPAPI.ini file. Changes are effective immediately.
For more information, see sk113599
The Check Point ThreatCloud

In This Section:
  Configuring Check Point ThreatCloud on a Gateway...............................................139
  Check Point ThreatCloud Network..............................................................................139
  The ThreatCloud Intellistore.........................................................................................140

Check Point ThreatCloud is a dynamically updated service that is based on an innovative global network of threat sensors and organizations that share threat data and collaborate to fight against modern malware. Customers can send their own threat data to the ThreatCloud and benefit from increased security and protection and enriched threat intelligence. The ThreatCloud distributes attack information, and turns zero-day attacks into known signatures that the Anti-Virus Software Blade can block. The Security Gateway does not collect or send any personal data.

Participation in Check Point information collection is a unique opportunity for Check Point customers to be a part of a strategic community of advanced security research. This research aims to improve coverage, quality, and accuracy of security services and obtain valuable information for organizations.

The ThreatCloud repository contains more than 250 million addresses that were analyzed for bot discovery and more than 2,000 different botnet communication patterns. The ThreatSpect engine uses this information to classify bots and viruses.

For the reputation and signature layers of the ThreatSpect engine, each Security Gateway also has:

- A local database, the Malware database that contains commonly used signatures, URLs, and their related reputations. You can configure automatic or scheduled updates for this database.
- A local cache that gives answers to 99% of URL reputation requests. When the cache does not have an answer, it queries the ThreatCloud repository.
  - For Anti-Virus - the signature is sent for file classification.
  - For Anti-Bot - the host name is sent for reputation classification.

Access the ThreatCloud repository from:

- **SmartConsole** - You can add specific malwares to rule exceptions when necessary. From the Threat Prevention Rule Base in SmartConsole, click the plus sign in the Protection column in the rule exceptions, and the Protection viewer opens.

- **ThreatWiki** - A tool to see the entire Malware database. Open ThreatWiki in SmartConsole or access it from the Check Point website.

Data which Check Point Collects

When you enable information collection, the Check Point Security Gateway collects and securely submits event IDs, URLs, and external IPs to the Check Point Lab regarding potential security risks.

For example:

```xml
<entry engineType="3" sigID="-1" attackName="CheckPoint - Testing Bot" sourceIP="7a1ec646fe17e2cd" destinationIP="d8c8f142" destinationPort="80" host="www.checkpoint.com" path="/za/images/threatwiki/pages/TestAntiBotBlade.html" numOfAttacks="20" />
```
This is an example of an event that was detected by a Check Point Security Gateway. It includes the event ID, URL, and external IP addresses. Note that the data does not contain confidential data or internal resource information. The source IP address is obscured. Information sent to the Check Point Lab is stored in an aggregated form.

Configuring Check Point ThreatCloud on a Gateway

To configure the Security Gateway to share information with the Check Point ThreatCloud:

1. Double-click the Security Gateway.
   The gateway window opens and shows the General Properties page.
2. Configure the settings for the Anti-Bot and Anti-Virus Software Blades.
   a) From the navigation tree click Anti-Bot and Anti-Virus.
      The Anti-Bot and Anti-Virus page opens.
   b) To configure a Security Gateway to share Anti-Bot and Anti-Virus information with the ThreatCloud, select Share anonymous attack information with Check Point ThreatCloud.
      To disable sharing Anti-Bot and Anti-Virus information with the ThreatCloud, clear this option.
3. Configure the settings for the Threat Emulation Software Blade.
   Note - These settings are not relevant when you use the ThreatCloud emulation service, because with this service, the files are already sent to the ThreatCloud service for emulation.
   a) From the navigation tree click Threat Emulation > Advanced.
      The Threat Emulation page opens.
   b) To configure a Security Gateway to share Threat Emulation information with the ThreatCloud, select Share anonymous attack information with Check Point ThreatCloud.
      To disable sharing Threat Emulation information with the Check Point cloud, clear this option.
   c) Select Share malicious files with Check Point to send malicious malware files that the Threat Emulation Software Blade identified to the ThreatCloud. To disable sending malicious files to the Check Point cloud, clear this option.
4. Configure the settings for the IPS Software Blade.
   a) From the navigation tree click IPS.
      The IPS page opens.
   b) To configure a Security Gateway to share IPS information with the ThreatCloud, select Help Improve Check Point Threat Prevention product by sending anonymous information about feature usage, infections details and product customizations. To disable sharing IPS information with the Check Point cloud, clear this option.
5. Click OK.

Check Point ThreatCloud Network

By default, all gateways send threat information to the ThreatCloud.
You can change this default behavior in SmartConsole.

**To configure all gateways not to send information to the ThreatCloud:**

1. Open **Global Properties > Security Management Access**.
2. In the **Internet Access** area, clear this setting: **Improve product experience by sending data to Check Point**.
3. Click **OK**.
4. Restart SmartConsole.
5. **Install Policy**.

**The ThreatCloud Intellistore**

ThreatCloud Intellistore is a threat intelligence marketplace which supplements ThreatCloud and provides intelligence data from leading cyber security vendors. The data includes threat information such as IPs, domains, URLs, command and control networks, DOS attacks and more. Intellistore classifies the information feeds according to specific geographies, types of attacks or industries, and you can select the feeds that best suit your needs.

A security feed represents specialized intelligence gathered and analyzed by the vendors. ThreatCloud translates these feeds into protections which run on Security Gateways.
Threat Prevention Scheduled Updates

In This Section:

- Introduction to Scheduled Updates ............................................................... 141
- Configuring Threat Prevention Scheduled Updates ........................................ 141
- Checking Update Status ................................................................................. 142
- Turning Off IPS Automatic Updates on a Gateway ....................................... 142
- IPS Updates Use Cases .................................................................................. 143

Introduction to Scheduled Updates

Check Point wants the customer to be protected. When a protection update is available, Check Point wants the configuration to be automatically enforced on the gateway. You can configure automatic gateway updates for the Anti-Virus, Anti-Bot, Threat Emulation and IPS blades.

For the Anti-Virus, Anti-Bot and Threat Emulation, the gateways download the updates directly from the Check Point cloud.

For the IPS blade, prior to R80.20, the updates were downloaded to the Security Management Server, and only after you installed policy, the gateways could enforce the updates. Starting from R80.20, the gateways can directly download the updates. For R80.20 gateways and higher with no internet connectivity, you must still install policy to enforce the updates.

When you configure automatic IPS updates on the gateway, the action for the newly downloaded protections is by default according to the profile settings.

IPS, Anti-Virus and Anti-Bot updates are performed every two hours by default. Threat Emulation engine updates are performed daily at 05:00 by default, and Threat Emulation image updates are performed daily at 04:00 by default.

You can see the list of Anti-Bot and Anti-Virus protections in Threat Tools > Protections, and the list of IPS protections in Threat Tools > IPS Protections. The update date appears next to each protection.

Configuring Threat Prevention Scheduled Updates

To configure Threat Prevention scheduled updates:

1. In SmartConsole, go to the Security Policies page and select Threat Prevention.
2. In the Threat Tools section of the Threat Prevention Policy, click Updates.
3. In the section for the applicable Software Blade, click Schedule Update.
   The Schedule Updates window opens.
4. Make sure Enable <blade> scheduled updates is selected.
5. For IPS, there are 2 more configuration options for scheduling Security Management Server updates:
   - On successful IPS update on the Security Management Server, install policy on the Security Gateway - automatically installs the policy on the devices you select after the IPS update is completed. Click Configure to select these devices.
Note - In pre-R80 gateways, IPS was part of the Access Control policy. Therefore, when you select this option, a message shows which indicates that for pre-R80 gateways, the Access Control policy is installed and for R80 and above gateways, the Threat Prevention policy is installed.

- **Perform retries on the Security Management Server when the update fails** - lets you configure the number of tries the scheduled update makes if it does not complete successfully the first time.

6. Click **Configure**.
7. In the window that opens, set the **Time of event**:
   - **Update every**: set the update frequency by hours
   OR:
   - **Update at**: set the update frequency by days:
     - **Daily**: Every day
     - **Days in week**: Select days of the week
     - **Days in month**: Select dates of the month
8. Click **OK**.
9. Click **Close**.
10. **Install Policy**.

### Checking Update Status

In **Threat Tools > Update**, a message shows which indicates the number of gateways which are up-to-date.

**To check if the protections are update on a specific gateway:**

1. In the **Gateways & Servers** view, select a gateway.
2. Click the **Monitor** button.
   The **Device & License Information** window opens.
3. The **Device Status** page shows the gateway status.

### Turning Off IPS Automatic Updates on a Gateway

You can turn off automatic IPS updates on a specific gateway.

**To turn off automatic IPS updates on a specific gateway:**

1. In SmartConsole, to the **Gateways & Servers** view, and double-click a gateway.
   The gateway properties window opens.
2. In the navigation tree, go to the **IPS** page.
3. In **IPS Update Policy**, select **Use IPS management updates**
4. Click **OK**.
5. **Install Policy**.
IPS Updates Use Cases

These scenarios explain how an upgrade of the Security Gateways or the Security Management Server or both, affects the Scheduled Updates configuration.

**Scenario 1: Upgrading the Security Management Server to R80.20, and not upgrading the gateways to R80.20**

If you do not upgrade the gateways, then after the upgrade, the gateways are still not able to receive the updates independently, only through the Security Management Server. In this case, the configuration stays the same compared to before the upgrade: Scheduled Updates will be enabled or disabled on the Security Management Server, depending on the configuration before the upgrade.

**Scenario 2: Upgrading the gateways to R80.20 (with or without Security Management Server upgrade)**

- If, before the upgrade, Scheduled Updates were configured on the Security Management Server with automatic policy installation, then after the upgrade, automatic IPS updates are still enabled on the Security Management Server, and are also applied to the upgraded gateways.
- If Scheduled Updates were disabled on the Security Management Server before the upgrade, then they remain disabled after the upgrade, both on the Security Management Server and the gateways.
- If, before the upgrade, Scheduled Updates were configured on the Security Management Server without automatic policy installation - then during the first policy installation after upgrade, a message shows which indicates that R80.20 gateways and above automatically update the IPS Protections. For older gateways than R80.20, you must install policy to apply the updates.
Using Threat Prevention with HTTPS Traffic

In This Section:

- Configuring HTTPS Inspection ................................................................. 145
- HTTP Inspection on Non-Standard Ports ......................................................... 154

You can use the HTTPS Inspection feature to unencrypt traffic and let the Threat Prevention Software Blades give protections against advanced threats, bots, and other malware.
Configuring HTTPS Inspection

HTTPS Internet traffic uses the SSL (Secure Sockets Layer) protocol and is encrypted to give data privacy and integrity. However, HTTPS traffic has a possible security risk and can hide illegal user activity and malicious traffic. Security Gateways cannot inspect HTTPS traffic because it is encrypted. You can enable the HTTPS Inspection feature to let the Security Gateways create new SSL connections with the external site or server. The Security Gateways are then able to decrypt and inspect HTTPS traffic that uses the new SSL connections.

There are two types of HTTPS Inspection:

- **Outbound HTTPS Inspection** - To protect against malicious traffic that is sent from an internal client to an external site or server.
- **Inbound HTTPS Inspection** - To protect internal servers from malicious requests that arrive from the Internet or an external network.

A Security Gateway uses certificates and becomes an intermediary between the client computer and the secure web site. All data is kept private in HTTPS Inspection logs. Only administrators with HTTPS Inspection permissions can see all the fields in such a log.

Inspecting HTTPS Packets

**Outbound Connections**

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

If the request matches an HTTPS Inspection rule, the Security Gateway validates the certificate from the server (on the Internet). The Security Gateway validates the certificate using the Online Certificate Status Protocol (OCSP) standard. OCSP is faster and uses much less memory than CRL Validation, which is used for certificate validation in releases lower than R80.10. For a new HTTPS connection to the server, the Security Gateway creates and uses a new certificate. There are two HTTPS connections, one to the internal client and one to the external server. It can then decrypt and inspect the packets according to the security policy. The packets are encrypted again and sent to the destination.
**Inbound Connections**

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

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

---

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

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

**Workflow overview**

1. Enable HTTPS Inspection on the Security Gateway.
2. Configure the Security Gateway to use the certificate.
   - Outbound Inspection - Generate a new certificate for the Security Gateway.
   - Inbound Inspection - Import the certificate for the internal server.
3. Configure the HTTPS Inspection Rule Base.
4. Install the Access Control Policy.
Enabling HTTPS Inspection

You must enable HTTPS Inspection on each Security Gateway.

To enable HTTPS Inspection on a Security Gateway:
1. From the SmartConsole Gateways & Servers view, edit the Security Gateway object.
2. Click HTTPS Inspection > Step 3.
3. Select Enable HTTPS Inspection.

The first time you enable HTTPS Inspection on one of the Security Gateways, you must create an outbound CA certificate for HTTPS Inspection or import a CA certificate already deployed in your organization. This outbound certificate is used by all Security Gateways managed on the 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 Security Gateways use this password to sign certificates for the sites accessed. You must keep the password because it is 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.

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

To create an outbound CA certificate:
1. In SmartConsole Gateways & Servers view, right-click the Security Gateway object and select Edit.
   The Gateway Properties window opens.
2. In the navigation tree, select HTTPS Inspection.
3. In Step 1 of the HTTPS Inspection page, click Create.
   The Create window opens.
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 (on page 148).

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.
Best Practice - Use private CA Certificates.

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. Use this password only when you import the certificate to a new Security Management Server.

To import a CA certificate:

1. If the CA certificate was created on another Security Management Server, export the certificate from the Security Management Server on which it was created (on page 148).
2. In the SmartConsole Gateways & Servers view, right-click the Security Gateway object and select Edit.
   The Gateway Properties window opens.
3. In the navigation tree, select HTTPS Inspection.
4. In Step 1 of the HTTPS Inspection page, click Import.
   The Import Outbound Certificate window opens.
5. Browse to the certificate file.
6. Enter the private key password.
7. Click OK.
8. If the CA certificate was created on another Security Management Server, deploy it to clients (on page 148).

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 with 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.

Command syntax:

```
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 this command:

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

Example

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

Exporting and Deploying the Generated CA

To prevent users from getting warnings about the generated CA certificates that HTTPS Inspection uses, install the generated CA certificate used by HTTPS Inspection as a trusted CA. You can distribute the CA with different distribution mechanisms such as Windows GPO. This adds the generated CA to the trusted root certificates repository on client computers.
When users run standard updates, the generated CA will be in the CA list and they will not receive browser certificate warnings.

To distribute a certificate with a GPO:

1. From the HTTPS Inspection window of the Security Gateway, click **Export certificate**.
2. Save the CA certificate file.
3. Use the Group Policy Management Console (on page 149) to add the certificate to the Trusted Root Certification Authorities certificate store.
4. Push the Policy to the client computers in the organization.
   - **Note**: Make sure that the CA certificate is pushed to the client computer organizational unit.
5. Test the distribution by browsing to an HTTPS site from one of the clients and verifying that the CA certificate shows the name you entered for the CA certificate that you created in the **Issued by** field.

**Deploying Certificates by Using Group Policy**

You can use this procedure to deploy a certificate to multiple client machines with Active Directory Domain Services and a Group Policy Object (GPO). A GPO can contain multiple configuration options, and is applied to all computers in the scope of the GPO.

Membership in the local Administrators group, or equivalent, is necessary to complete this procedure.

To deploy a certificate using Group Policy:

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

**Configuring Inbound HTTPS Inspection**

Configure the Security Gateway for inbound HTTPS Inspection.

To enable inbound HTTPS traffic inspection:

1. From the SmartConsole **Gateways & Servers** view, edit the Security Gateway object.
2. Click **HTTPS Inspection > Step 3**.
3. Select **Enable HTTPS Inspection**.
4. Import server certificates for servers behind the organization Security Gateways (on page 150).
5. Define an HTTPS Inspection policy:
   - Create rules
• Add a server certificate to the Certificate column of each rule.

**Assigning a Server Certificate for Inbound HTTPS Inspection**

Add the server certificates to the Security Gateway. This creates a server certificate object.

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

1. In SmartConsole, go to Security Policies > Shared Policies > HTTPS Inspection.
2. Click Open HTTPS Inspection Policy In SmartDashboard.
   
   SmartConsole opens.
3. Click Server Certificates.
4. Click Add.
   
   The Import Inbound Certificate window opens.
5. Enter a Certificate name and a Description (optional).
7. Enter the Private key password. Enter the same password that was used to protect the private key of the certificate on the server.
8. Click OK.

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

**HTTPS Inspection Policy**

The HTTPS Inspection rules define how the Security Gateways inspect HTTPS traffic. The HTTPS Inspection rules can use the URL Filtering categories to identify traffic for different websites and applications. For example, to protect the privacy of your users, you can use a rule to ignore HTTPS traffic to banks and financial institutions.

The HTTPS Inspection rules are applied to all the Software Blades that have HTTPS Inspection enabled. These are the Software Blades that support HTTPS Inspection:

• Access Control
  • Application Control
  • URL Filtering
  • Content Awareness
• Threat Prevention
  • IPS
- Anti-Virus
- Anti-Bot
- Threat Emulation
- Data Loss Prevention

**To open the HTTP Inspection Policy**

1. In SmartConsole, go to **Security Policies > Shared Policies > HTTPS Inspection**.
2. Click **Open HTTPS Inspection Policy In SmartDashboard**.

**HTTPS Inspection rules in SmartConsole**

These are the fields that manage the rules for the HTTPS Inspection security policy.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Rule number in the HTTPS Inspection Rule Base.</td>
</tr>
<tr>
<td>Name</td>
<td>Name that the system administrator gives this rule.</td>
</tr>
<tr>
<td>Source</td>
<td>Network object that defines where the traffic starts.</td>
</tr>
<tr>
<td>Destination</td>
<td>Network object that defines the destination of the traffic.</td>
</tr>
<tr>
<td>Services</td>
<td>The network services that are inspected or bypassed.</td>
</tr>
<tr>
<td>Site Category</td>
<td>Categories for applications or web sites that are inspected or bypassed.</td>
</tr>
<tr>
<td>Action</td>
<td>Action that is done when HTTPS traffic matches the rule. The traffic is inspected or ignored (Bypass).</td>
</tr>
<tr>
<td>Track</td>
<td>Tracking and logging action that is done when traffic matches the rule.</td>
</tr>
<tr>
<td>Install On</td>
<td>Network objects that will get the HTTPS Inspection rule. You can only select Security Gateways that have HTTPS Inspection enabled.</td>
</tr>
<tr>
<td>Certificate</td>
<td>The certificate that is used for this rule.</td>
</tr>
<tr>
<td></td>
<td>• Inbound HTTPS Inspection - Select the certificate that the internal server uses.</td>
</tr>
<tr>
<td></td>
<td>• Outbound HTTPS Inspection - Select the Outbound Certificate object that you are using for the computers in the network. 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 &gt; Server Certificates &gt; Add.</td>
</tr>
<tr>
<td>Comment</td>
<td>An optional field that lets you summarize the rule.</td>
</tr>
</tbody>
</table>

**Configuring HTTPS Inspection Rules**

Create different HTTPS Inspection rules for outbound and inbound traffic.

The outbound rules use the certificate that was generated for the Security Gateway.

The inbound rules use a different certificate for each internal server.

You can also create bypass rules for traffic that is sensitive and is not inspected. Make sure that the bypass rules are at the top of the HTTPS Inspection Rule Base.
After creating the rules, install the Access Control Policy.

Sample HTTPS Inspection Rule Base

This table shows a sample HTTPS Inspection Rule Base for a typical policy. [The Track and Install On columns are not shown. Track is set to None and Install On is set to Any.]

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Site Category</th>
<th>Action</th>
<th>Blade</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Inbound traffic</td>
<td>Any</td>
<td>WebCalendarServer</td>
<td>HTTPS</td>
<td>Any</td>
<td>Inspect</td>
<td>Any</td>
<td>WebCalendarServer CA</td>
</tr>
<tr>
<td>2</td>
<td>Financial sites</td>
<td>Any</td>
<td>Internet</td>
<td>HTTPS</td>
<td>Financial Services</td>
<td>Bypass</td>
<td>Any</td>
<td>Outbound CA</td>
</tr>
<tr>
<td>3</td>
<td>Outbound traffic</td>
<td>Any</td>
<td>Internet</td>
<td>HTTPS</td>
<td>Any</td>
<td>Inspect</td>
<td>Any</td>
<td>Outbound CA</td>
</tr>
</tbody>
</table>

1. **Inbound traffic** - Inspects HTTPS traffic to the network object WebCalendarServer. This rule uses the WebCalendarServer certificate.

2. **Financial sites** - This is a bypass rule that does not inspect HTTPS traffic to websites that are defined in the Financial Services category. This rule uses the Outbound CA certificate.

3. **Outbound traffic** - Inspects HTTPS traffic to the Internet. This rule uses the Outbound CA certificate.

Bypassing HTTPS Inspection for 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 for software updates:

1. In SmartConsole, go Manage & Settings > Blades > HTTPS Inspection > Configure In SmartDashboard.
2. In SmartDashboard, click the HTTPS Inspection tab.
3. Click Policy.
4. In the Policy pane, select Bypass HTTPS Inspection of traffic to well known software update services [list is dynamically updated]. This option is selected by default.
5. Click list to see the list of approved domain names.

Managing Certificates by Gateway

The Gateways pane lists the gateways with HTTPS Inspection enabled. Select a gateway and click Edit to edit the gateway properties.

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

If the Security Management Server which manages the selected Security Gateway does not have a generated CA certificate installed on it, you can add it with Import certificate from file.

- 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 (on page 148) 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 Security 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 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 for installation. The notification in SmartConsole 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 select 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 security certificate, but lets the user continue to the website.

You can change the default setting to block untrusted server certificates.

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 SmartConsole, 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

In the HTTPS Validation page of SmartConsole you can set options for

• Fail mode
• HTTPS site categorization mode
• Server validation.
• Certificate blacklisting
• Troubleshooting

To learn more about these options, see the Help. Click ? in the HTTPS Validation page.

Showing HTTPS Inspection Logs

The predefined log query for HTTPS Inspection shows all HTTPS traffic that matched the HTTPS Inspection policy, and was configured to be logged.
To see HTTPS Inspection Logs:

1. In the SmartConsole Logs & Monitor > Logs tab, click Favorites.
2. Select the HTTPS Inspection query.

The Logs tab includes an HTTP Inspection Action field. The field value can be inspect or bypass. If HTTPS Inspection was not done on the traffic, this field does not show in the log.

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, the Threat Prevention policy inspects all HTTP traffic, even if it is sent using nonstandard ports. This option is selected by default. You can configure this option in the Manage & Settings view > Blades > Threat Prevention > Advanced Settings.
Using Anti-Spam and Mail

In This Section:

- Introduction to Anti-Spam and Mail Security .......................................................... 155
- Mail Security Overview .............................................................................................. 155
- Configuring Anti-Spam ............................................................................................... 158
- Configuring Anti-Virus Protection for Mail ............................................................... 162
- Configuring a Disclaimer .......................................................................................... 164
- Anti-Spam Logging and Monitoring ........................................................................... 164

Introduction to Anti-Spam and Mail Security

The relentless and unprecedented growth in unwanted email now poses an unexpected security threat to the network. As the amount of resources [disk space, network bandwidth, CPU] devoted to handling unsolicited emails increases from year to year, employees waste more and more time sorting through unsolicited bulk email commonly known as spam. Anti-Spam and Mail provides network administrators with an easy and central way to eliminate most of the spam reaching their networks.

Anti-Spam and Mail Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content based Anti-Spam</td>
<td>The core of the Anti-Spam functionality is the content based classification engine.</td>
</tr>
<tr>
<td>IP Reputation Anti-Spam</td>
<td>Using an IP reputation service, most of the incoming spam is blocked at connect time.</td>
</tr>
<tr>
<td>Block List Anti-Spam</td>
<td>Block specific senders based on IP address or sender’s address.</td>
</tr>
<tr>
<td>Mail Anti-Virus</td>
<td>Scan and filter mail for malware.</td>
</tr>
<tr>
<td>Zero Hour Malware Protection</td>
<td>Filter mail using rapid response signatures.</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion prevention system for mail protection.</td>
</tr>
</tbody>
</table>

Mail Security Overview

On the Anti-Spam & Mail tab:

- Select gateways that enforce Anti-Virus checking
- Select gateways that enforce Anti-Spam protection
- Enable automatic updates
- View settings and logs
Anti-Spam

The Anti-Spam functionality employs unique licensed technology. Unlike many Anti-Spam applications that rely on searching for keywords and a lexical analysis of the content of an email message, Check Point Anti-Spam identifies spam by analyzing known and emerging distribution patterns. By avoiding a search for key words and phrases that might classify a legitimate email as spam and instead focusing on other message characteristics, this solution offers a high spam detection rate with a low number of false positives.

To preserve personal privacy and business confidentiality, only select characteristics are extracted from the message envelope, headers, and body (no reference to actual content or attachments are included). Hashed values of these message characteristics are sent to a Detection Center for pattern analysis. The Detection Center identifies spam outbreaks in any language, message format, or encoding type. Responses are returned to the enterprise gateway within 300 milliseconds.

Once identified, the network of spam generating machines is blacklisted. If the network changes its behavior, it is removed from the black list.
This figure illustrates the Anti-Spam workflow:

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internet</td>
</tr>
<tr>
<td>2</td>
<td>Proxy SMTP server</td>
</tr>
<tr>
<td>3</td>
<td>Detection Center</td>
</tr>
<tr>
<td>4</td>
<td>Enterprise front-end mail server in DMZ</td>
</tr>
<tr>
<td>5</td>
<td>Internal network</td>
</tr>
</tbody>
</table>

1. Proxy SMTP server on the gateway receives incoming mail.
2. The SMTP proxy uses the Anti-Spam daemon to extract selected message characteristics, and produce a hash fingerprint.
3. The Anti-Spam daemon queries the Detection Center with a special Anti-Spam protocol. The hashed fingerprint is compared to other fingerprints in the pattern repository to determine whether the email is spam.
4. The Detection Center classifies the email as spam or not spam, and returns the result to the gateway.
5. If the Detection Center classified the email as spam, the email is flagged as such (in the header or subject) and forwarded to the enterprise mail server.
6. The mail server forwards the email to its recipient on the network. Because the header or subject were flagged as spam, recipients can use that tag or marker to set up filtering rules in their native mail program — for example, in Microsoft Outlook you can configure a rule to delete all emails with the word SPAM in the subject line or the header.

To prevent delays while large email files are scanned for Spam, a feature known as Adaptive Continuous Download, transfers the email to the recipient while Anti-Spam detection takes place.

**Adaptive Continuous Download**

To prevent delays, *Adaptive Continuous Download* starts delivering the email to the recipient while Anti-Spam scanning is still in progress. If the email is designated as Spam, it is flagged as spam before it is completely transferred to the recipient. Both the SMTP and POP3 protocols support Adaptive Continuous Download for the entire email message.
Configuring Anti-Spam

Configuring a Content Anti-Spam Policy

To configure a content Anti-Spam policy:

1. In SmartConsole, select Manage & Settings > Blades > Anti-Spam & Mail and click Configure in SmartDashboard.
   SmartDashboard opens and shows the Anti-Spam & Mail tab.
2. On the Overview page, under Content based Anti-Spam, click Settings.
3. Use the slider to select an Anti-Spam policy protection level.
4. Select flagging options.
5. In the Security Gateway Engine settings section, set a maximum data size to scan.
6. In the UTM-1 Edge Engine settings section, set a confidence level for spam and suspected spam.
   A spam confidence level is a grade or rating (usually between zero and a hundred) used decide whether a particular email message should be treated as spam. For example, if the confidence level is set to 70, then all email messages rated at 70 or above will be treated as spam.
7. Select Tracking Options for Spam, Suspected Spam, or Non Spam. Tracking options include:
   • None [no logging]
   • Log
   • Popup Alert
   • Mail Alert
   • SNMP trap alert
   • Three custom user-defined scripts.
8. Click Save and then close SmartDashboard.
9. From SmartConsole, install the Access Control policy.

Configuring an IP Reputation Policy

This window enables IP reputation, an Anti-Spam mechanism that checks the IP address of the message sender [contained in the opening SYN packet] against a dynamic database of suspect IP addresses. If, according to the IP reputation service, the originating network has a reputation for sending spam, then the spam session is blocked at connect time. This way, the IP reputation feature creates a list of trusted email sources.

To configure an IP reputation policy:

1. In SmartConsole, select Manage & Settings > Blades > Anti-Spam & Mail and click Configure in SmartDashboard.
   SmartDashboard opens and shows the Anti-Spam & Mail tab.
2. On the Overview page, under IP Reputation Anti-Spam, click Settings.
3. Use the slider to select an IP Reputation Policy:
   • Off - IP Reputation service is disabled
   • Monitor - Monitors known and suspected spam but does not block it
   • Medium Protection - Blocks known spam and monitors suspected spam
   • High Protections - Blocks known and suspected spam
4. Select tracking options for **Spam**, **Suspected Spam**, or **Non spam**. Tracking options include
   - None [no logging]
   - Log
   - Popup Alert
   - Mail Alert
5. Click **Save** and then close SmartDashboard.
6. From SmartConsole, install the Access Control policy.
   - SNMP trap alert
   - Three custom user-defined scripts.

**Configuring a Block List**

You can configure a list of email sources to block according to the sender's name, domain name, or IP address.

**To configure a block list:**

1. In SmartConsole, select **Manage & Settings > Blades > Anti-Spam & Mail** and click **Configure in SmartDashboard**.
   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. On the **Overview** page, under **Block List Anti-Spam**, click **Settings**.
3. Use the slider to select a Block Policy:
   - **Off** - Not blocked
   - **Monitor Only** - Not Blocked, but monitors senders by IP address and email address
   - **Block** - Blocks senders by IP address and email address
4. In the **Blocked senders/domains** section, click **Add** and enter the name of a sender or domain to be rejected.
5. In the **Blocked IPs** section, click **Add** and enter an IP address that should be blocked.
6. From the drop-down list in the **Tracking** section, select a tracking option for blocked mail or non-spam.
7. Click **Save** and then close SmartDashboard.
8. From SmartConsole, install the Access Control policy.

**Configuring Anti-Spam SMTP**

SMTP traffic can be scanned according to direction or IPs.

**To configure Anti-Spam SMTP:**

1. In SmartConsole, select **Manage & Settings > Blades > Anti-Spam & Mail** and click **Configure in SmartDashboard**.
   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. From the navigation tree, click **Advanced > SMTP**.
3. Make sure that **Scan SMTP traffic with Anti-Spam engine for Anti-Spam, IP reputation and Block list protection** is selected.
4. Select to scan SMTP traffic **By Mail Direction** or **By IPs**.
   a) If you selected scan **By IPs**, click **Add Rule** to configure rules for IP addresses to scan.
b) If you selected scan **By Mail Direction**, select a scanning direction for:
   - Incoming files
   - Outgoing files
   - Internal files through the gateway

5. Select **Activate Continuous Download** to avoid client time-outs when large files are scanned.
   See Adaptive Continuous Download for further information.

6. Click **Save** and then close SmartDashboard.
7. From SmartConsole, install the Access Control policy.

### Configuring Anti-Spam POP3

POP3 traffic can be scanned according to direction.

1. In SmartConsole, select **Manage & Settings > Blades > Anti-Spam & Mail** and click **Configure in SmartDashboard**.
   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. From the navigation tree click **Advanced > POP3**.
3. Make sure that **Scan POP3 traffic with Anti-Spam engine for Anti-Spam, IP reputation and Block list protection** is selected.
4. Select to scan POP3 traffic **By Mail Direction** or **By IPs**.
5. If you selected scan **By IPs**, click **Add Rule** to configure rules for IP addresses to scan.
6. If you selected scan **By Mail Direction**, select a scanning direction for:
   - Incoming mail
   - Outgoing mail
   - Internal mail
7. Select **Activate Continuous Download** to avoid client time-outs when large files are scanned.
   See Adaptive Continuous Download for further information.
8. Click **Save** and then close SmartDashboard.
9. From SmartConsole, install the Access Control policy.

### Configuring Network Exceptions

An Anti-Spam policy can be enforced on all email traffic or only on traffic that was not deliberately excluded from the policy.

**To exclude sources and destinations:**

1. In SmartConsole, select **Manage & Settings > Blades > Anti-Spam & Mail** and click **Configure in SmartDashboard**.
   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. From the navigation tree click **Advanced > Network Exceptions**.
3. Select **Enforce the Anti-Spam policy on all traffic except for traffic between the following sources and destinations**.
4. Click **Add**. The **Network Exception** window opens.
5. For **Source** and **Destination**, select **Any**, or select **Specific** and one gateway from each list.
6. Click **OK**.
7. Click **Save** and then close SmartDashboard.
8. From SmartConsole, install the Access Control policy.

### Configuring an Allow List

You can configure a list of allowed email sources according to the sender’s name and domain name, or according to the IP address.

**To configure an allow list:**

1. In SmartConsole, select **Manage & Settings > Blades > Anti-Spam & Mail** and click **Configure in SmartDashboard**.
   
   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.

2. From the navigation tree click **Advanced > Allow List**.

3. In the **Allowed Senders / Domains** section, click **Add** and enter the name of a sender or domain to be allowed.

4. In the **Allowed IPs** section, click **Add** and enter an allowed IP address.

5. From the drop-down list in the **Tracking** section, select a tracking option.

6. Click **Save** and then close SmartDashboard.

7. From SmartConsole, install the Access Control policy.

### Selecting a Customized Server

You can select an alternative Detection Center for Anti-Spam analysis.

**To select a Detection Center:**

1. In SmartConsole, select **Manage & Settings > Blades > Anti-Spam & Mail** and click **Configure in SmartDashboard**.
   
   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.

2. From the navigation tree click **Advanced > Customized Server**.

3. Select **Use Customized Server**.

4. From the drop-down list, select a server.

5. Click **Save** and then close SmartDashboard.

6. From SmartConsole, install the Access Control policy.

### Anti-Spam on UTM-1 Edge Devices

Anti-Spam protection is available on UTM-1 Edge devices.

**To configure Anti-Spam on UTM-1 Edge devices:**

1. Open the **General Properties** window of the UTM-1 Edge gateway.

2. Select **Anti-Spam**.

### Bridge Mode and Anti-Spam

If an UTM-1 appliance is configured to run in bridge mode, Anti-Spam is supported providing that:

- The bridge interface has an IP address
- The bridge interface has a default gateway
Configuring Anti-Virus Protection for Mail

Configuring Mail Anti-Virus
The Mail Anti-Virus policy prevents use of email as a virus delivery mechanism.

To configure a mail Anti-Virus policy:
1. In SmartConsole, select Manage & Settings > Blades > Anti-Spam & Mail > and click Configure in SmartDashboard.
   SmartDashboard opens and shows the Anti-Spam & Mail tab.
2. From the navigation tree, select Traditional Anti-Virus > Security Gateway > Mail Protocols > Mail Anti-Virus.
3. Set the slider to Block.
4. Select tracking options for either all POP3 and SMTP mail, or just blocked mail. Tracking options include:
   • None (no logging)
   • Log
   • Popup alert
   • Mail alert
   • SNMP trap alert
   • Three custom user-defined scripts
5. Click Save and then close SmartDashboard.
6. From SmartConsole, install the Access Control policy.

Configuring Zero Hour Malware Protection
By proactively scanning the Internet, the Detection Center identifies massive virus outbreaks as soon as they occur. This Zero-Hour solution provides protection during the critical time it takes to discover a new virus outbreak and assign it a signature.

To configure zero hour malware protection:
1. In SmartConsole, select Manage & Settings > Blades > Anti-Spam & Mail > and click Configure in SmartDashboard.
   SmartDashboard opens and shows the Anti-Spam & Mail tab.
2. From the navigation tree, select Traditional Anti-Virus > Security Gateway > Mail Protocols > Zero Hour Malware Protection.
3. With the slider, select a Zero hour malware protection level:
   • Off
   • Monitor Only
   • Block
4. Select tracking options for blocked, SMTP and POP3 mail. Tracking options include:
   • None (no logging)
   • Log
   • Popup alert
   • Mail alert
• SNMP trap alert
• Three custom user-defined scripts
5. Click Save and then close SmartDashboard.
6. From SmartConsole, install the Access Control policy.

Configuring SMTP and POP3

SMTP and POP3 traffic can be scanned according to direction or by IPs.

To configure SMTP and POP3:
1. In SmartConsole, select Manage & Settings > Blades > Anti-Spam & Mail > and click Configure in SmartDashboard.

   SmartDashboard opens and shows the Anti-Spam & Mail tab.
2. From the navigation tree, select Traditional Anti-Virus > Security Gateway > Mail Protocols > SMTP or POP3.
3. Using the slider, select a protection level:
   • Off
   • Monitor Only - SMTP and HTTP are the only protocols that support this protection level
   • Block
4. Select to scan SMTP traffic By Mail Direction or By IPs
   a) When you scan by File Direction, select a scanning direction for:
      ▪ Incoming files
      ▪ Outgoing files
      ▪ Internal files through the gateway
   b) When you scan by IPs, create rules for the Rule Base to define the source and destination of the data to be scanned.
5. For SMTP and HTTP, select the Activate Proactive Detection [impacts performance] checkbox to enable file-based Traditional Anti-Virus detection. Clear the checkbox to enable stream mode detection. See Understanding Proactive and Stream Mode Detection for further information. FTP and POP3 are set to Proactive Detection mode automatically.
6. If Proactive Detection was configured, select the Activate Continuous Download checkbox to prevent client time-outs when large files are scanned.
   See Continuous Download for further information.
7. Click Save and then close SmartDashboard.
8. From SmartConsole, install the Access Control policy.

Configuring File Types

You can set an action to take place when a file of a certain type passes through the gateway. Certain file types can pass through the gateway without being scanned for viruses. For example, picture and video files are normally considered safe. Other formats can be considered safe because they are relatively hard to tamper with. Update the list as necessary.

To configure the file types:
1. In SmartConsole, select Manage & Settings > Blades > Anti-Spam & Mail > and click Configure in SmartDashboard.
SmartDashboard opens and shows the **Anti-Spam & Mail** tab.

2. From the navigation tree, select **Traditional Anti-Virus > Security Gateway > File Types**.
3. Configure the file types.
4. Optional: Click **Update** to update the list using a file.
5. Click **Save** and then close SmartDashboard.
6. From SmartConsole, install the Access Control policy.

### Configuring Settings

Define maximum sizes for scanned files and archives. Configure actions to take if the set limits are exceeded, or when a scan fails.

**To configure scan failure and scan settings:**

1. In SmartConsole, select **Manage & Settings > Blades > Anti-Spam & Mail** and click **Configure in SmartDashboard**.
   
   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.

2. From the navigation tree, select **Traditional Anti-Virus > Security Gateway > Settings**.
3. In the **Scan Failure** section, select the default behavior if there are problems with the scan.
4. In the **File Handling** section, select the maximum file size to scan and the default behavior if the file exceeds the size limit.
5. In the **Archive File Handling** section, select the maximum nesting level to scan, the compression ratio, and the default behavior if the file exceeds the limits or cannot be extracted.
6. Click **Save** and then close SmartDashboard.
7. From SmartConsole, install the Access Control policy.

### Configuring a Disclaimer

You can create your own custom disclaimer notice.

**To configure a disclaimer:**

1. In SmartConsole, select **Manage & Settings > Blades > Anti-Spam & Mail** and click **Configure in SmartDashboard**.
   
   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.

2. From the navigation tree, select **Advanced > Disclaimer**.
3. Select **Add disclaimer to email scanned by Anti-Virus and Anti-Spam engines**.
4. In the text box, type your disclaimer notice.
5. Click **Save** and then close SmartDashboard.
6. From SmartConsole, install the Access Control policy.

### Anti-Spam Logging and Monitoring

Anti-Spam logging and monitoring options are available in the **Logs & Monitor** view in SmartConsole.
Logs derived from Anti-Spam scanning are sent to Security Management Server, and show in the Logs & Monitor > Logs view. In the Logs & Monitor view, you can see detailed views (on page 102) and reports (on page 103) of the Anti-Spam activity, customize these views and reports, or generate new ones.
Troubleshooting

In This Section:

- Troubleshooting the Threat Extraction Blade..................................................166
- Troubleshooting Threat Emulation...................................................................168
- Troubleshooting IPS for a Security Gateway....................................................169

Troubleshooting the Threat Extraction Blade

This section covers common problems and solutions.

The Threat Extraction blade fails to extract threats from emails belonging to LDAP users

In Global Properties > User Directory, make sure that you have selected the Use User Directory for Security Gateways option.

Mails with threats extracted do not reach recipients

1. Make sure the gateway passed the MTA connectivity test during the First Time Configuration Wizard.
   a) Disable then enable the Threat Extraction blade.
   b) Complete the First Time Configuration Wizard again.
   c) Make sure the wizard passes the connectivity test.

2. Test the connection to the target MTA.
   a) Open a command prompt on the gateway.
   b) Telnet to port 25 of the designated Mail Transfer Agent.

Threat Extraction fails to extract threats from emails

1. Open SmartConsole > Gateway Properties > Mail Transfer Agent.
2. Make sure you selected Enable as Mail Transfer Agent.
3. Access the organizations mail relay. Configure the Threat Extraction gateway as the relay’s next hop.

Users have stopped receiving emails

1. On the gateway command line interface, run: scrub queues.
   If the queues are flooded with requests, the Threat Extraction load is too high for the gateway.
   a) Bypass the scrub daemon.
      Run: scrub bypass on.
   b) Ask affected users if they are now receiving their emails. If they are, reactivate Threat Extraction.
      To reactivate, run: scrub bypass off.

2. Make sure the queue is not full.
a) Run:
   /opt/postfix/usr/sbin/postqueue -c /opt/postfix/etc/postfix/ -p

b) If the queue is full, empty the queue.
   Run:
   /opt/postfix/usr/sbin/postsuper -c /opt/postfix/etc/postfix/ -d ALL
   Emptying the queue loses the emails

c) To prevent losing important emails, flush the queue. Flushing forcefully resends queued emails.
   Run:
   /opt/postfix/usr/sbin/postfix -c /opt/postfix/etc/postfix/ flush

3. If queues remain full, make sure that the MTA is not overloading the gateway with internal requests. The MTA should be scanning only emails from outside of the organization.

Users have no access to original attachments

Make sure users are able to access the UserCheck portal from the e-mail they get when an attachment is cleaned.
1. Click the link sent to users.
2. Make sure that the UserCheck Portal opens correctly.
3. If users are not able to access the UserCheck portal but see the Gaia portal instead, make sure that accessibility to the UserCheck portal is correctly configured.
   a) In SmartConsole, open Gateway Properties > UserCheck.
   b) Under Accessibility, click Edit.
   c) Make sure the correct option is selected according to the topology of the gateway.

4. Open CPView.
   Make sure the access to original attachments statistic is no longer zero.

Attachments are not scanned by Threat Extraction

The scanned attachment statistic in CPView fails to increment.

On the gateway:
1. Make sure that the disk or directories on the gateway are not full.
   a) Run df -h on the root directory of the disk
   b) Run df -h on: /var/log

2. Make sure directories used by Threat Extraction can be written to.
   Run:
   a) touch /tmp/scrub/test
   b) touch /var/log/jail/tmp/scrub/test
   c) touch $FWDIR/tmp/email_tmp/test
CPView shows Threat Extraction errors

In CPview > Software-blades > Threat-extraction > File statistics, the number for internal errors is high compared to the total number of emails.

1. Open the Logs & Monitor view.
2. In the query search bar, enter: blade: Threat Extraction.
3. Right-click the table heading and select Edit Profile.
4. Add Threat Extraction Activity to the Selected Fields.

If the ThreatSpect engine is overloaded or fails while inspecting an attachment, a log is generated. By default, attachments responsible for log errors are still sent to email recipients. To prevent these attachments being sent, set the engine’s fail-over mode to Block all connections.

1. Go to Manage & Settings > Blades > Threat Prevention > Advanced Settings.
2. In the Fail Mode section, select Block all connections (fail-close).

The Threat Extraction blade continues to scan, but attachments that generate internal system errors are prevented from reaching the recipient.

Corrupted attachments cannot be cleaned, and by default generate log entries in the Logs & Monitor view. Corrupted attachments are still sent to the email recipient. To prevent corrupted attachments from reaching the recipient:

1. In SmartConsole, open Threat Prevention > Profiles > Profile > Threat Extraction Settings >.
2. In the Threat Extraction Exceptions area, select Block for attachments.

Attachments look disordered after conversion to PDF

1. In Security Policies > Threat Prevention > policy, right-click the Action column and select Edit.
2. In Threat Extraction > File Types, select Process specific file types and click Configure.
   The File Types Configuration window opens.
3. For the pdf file type, set the extraction method to clean.

To check MTA connectivity on a Virtual System:

1. Open an ssh connection to the gateway.
2. Go to expert mode.
3. Run vsenv <VS #>
4. Run touch $FWDIR/conf/scrub_connectivity_results.txt
5. Run /etc/fw/scripts/scrub_cvsenvcheck_connectivity.sh <mail server IP> $FWDIR/conf/scrub_connectivity_results.txt
6. Check $FWDIR/conf/scrub_connectivity_results.txt and see the result

Troubleshooting Threat Emulation

Using MTA with ClusterXL

When you enable MTA with a ClusterXL deployment, make sure that the standby cluster member is also able to connect to one or more of the next hops. If not, it is possible that when there is a failover to the standby member, emails in the MTA do not go to their destination.
Configuring Postfix for MTA

The Check Point MTA uses Postfix, and you can add custom user-defined Postfix options [http://www.postfix.org/postconf.5.html](http://www.postfix.org/postconf.5.html).

**To add Postfix options:**

1. From the Security Gateway CLI, create the file `$FWDIR/conf/mta_postfix_options.cf`.
2. Edit the file and add the definitions.
3. Save the file.
4. Install the Threat Prevention policy.

Problems with Email Emulation

**Best Practice** - If you are blocking SMTP traffic with the Prevent action, we recommend that you enable MTA on the Security Gateway (on page 70). If you do not enable the MTA, it is possible that emails are dropped and do not reach the mail server.

Troubleshooting IPS for a Security Gateway

IPS includes the ability to temporarily stop protections on a Security Gateway set to Prevent from blocking traffic. This is useful when troubleshooting an issue with network traffic.

**To enable Detect-Only for Troubleshooting:**

1. In SmartConsole, click *Gateways & Servers* and double-click the Security Gateway.
   The gateway window opens and shows the *General Properties* page.
2. From the navigation tree, click *IPS*.
3. In the *Activation Mode* section, click *Detect Only*.
4. Click *OK*.
5. **Install Policy**.
   All protections set to Prevent allow traffic to pass, but continue to track threats according to the Track setting.
Appendix: Regular Expressions

In This Section:

Regular Expression Syntax ........................................................................................................... 170
Using Non-Printable Characters ..................................................................................................... 170
Using Character Types .................................................................................................................... 171
Using Regular Expressions in Custom Sites ..................................................................................... 171

Regular Expression Syntax

This table shows the Check Point implementation of standard regular expression metacharacters.

<table>
<thead>
<tr>
<th>Metacharacter</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>Backslash</td>
<td>escape metacharacters, non-printable characters, character types</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square Brackets</td>
<td>character class definition</td>
</tr>
<tr>
<td>( )</td>
<td>Parenthesis</td>
<td>sub-pattern, to use metacharacters on the enclosed string</td>
</tr>
<tr>
<td>{min[,max]}</td>
<td>Curly Brackets</td>
<td>min/max quantifier</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{n} - exactly n occurrences</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{n,m} - from n to m occurrences</td>
</tr>
<tr>
<td></td>
<td></td>
<td>{n,} - at least n occurrences</td>
</tr>
<tr>
<td>.</td>
<td>Dot</td>
<td>match any character</td>
</tr>
<tr>
<td>?</td>
<td>Question Mark</td>
<td>zero or one occurrences (equals {0,1})</td>
</tr>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>zero or more occurrences of preceding character</td>
</tr>
<tr>
<td>+</td>
<td>Plus Sign</td>
<td>one or more occurrences (equals {1,})</td>
</tr>
<tr>
<td></td>
<td>Vertical Bar</td>
<td>alternative</td>
</tr>
<tr>
<td>^</td>
<td>Circumflex</td>
<td>anchor pattern to beginning of buffer (usually a word)</td>
</tr>
<tr>
<td>$</td>
<td>Dollar</td>
<td>anchor pattern to end of buffer (usually a word)</td>
</tr>
<tr>
<td>-</td>
<td>hyphen</td>
<td>range in character class</td>
</tr>
</tbody>
</table>

Using Non-Printable Characters

To use non-printable characters in patterns, escape the reserved character set.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\a</td>
<td>alarm; the BEL character (hex code 07)</td>
</tr>
<tr>
<td>\cX</td>
<td>“control-X”, where X is any character</td>
</tr>
<tr>
<td>\e</td>
<td>escape (hex code 1B)</td>
</tr>
</tbody>
</table>
### Using Character Types

To specify types of characters in patterns, escape the reserved character.

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\d</td>
<td>any decimal digit [0-9]</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>

### Using Regular Expressions in Custom Sites

Select **URLs are defined as Regular Expression only** if the application or site URL is entered as a regular expression using the correct syntax.

The meaning of the asterisk (*) depends on its use.
- In regular expressions, the asterisk is a metacharacter for zero or more instances of the preceding character.
- Without regular expressions, the asterisk is a wildcard, for zero or more instances of any character.

For example, to block a domain that ends with “example.com” (such as www.example.com):

<table>
<thead>
<tr>
<th>Regular Expression</th>
<th>.*\example\co m</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wildcard</td>
<td>.*\example\co m</td>
</tr>
</tbody>
</table>

**Important!** If you use this string as a regular expression, policy install fails. The gateway cannot resolve the regular expression to a URL, because there is no preceding character to find.

---

**More examples of regular expressions:**

To match subdomains of mydomain.com:  

```
(^|\.)mydomain\com
```

To match domain and subdomains of mydomain.com:  

```
(^|\.)*mydomain\com
```