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.

Latest Documentation
The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=24834
To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.
For more about this release, see the R77.30 home page

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>05 January 2016</td>
<td>Updated Configuring the Threat Prevention Profile (on page 40)</td>
</tr>
<tr>
<td>25 October 2015</td>
<td>Removed user-defined object path limitation in Using Threat Prevention with HTTPS Traffic (on page 76) Updated System Specifications (on page 17)</td>
</tr>
<tr>
<td>08 July 2015</td>
<td>Updated Configuring a Cluster (on page 40)</td>
</tr>
<tr>
<td>06 May 2015</td>
<td>Updated for R77.30 Added Getting Started with the Threat Extraction Blade (on page 38) Added Using Anti-Bot and Anti-Virus with VSX (on page 121) Added Enhanced HTTPS Inspection Bypass (on page 86)</td>
</tr>
<tr>
<td>04 November 2014</td>
<td>Updated The Check Point ThreatCloud (on page 49)</td>
</tr>
<tr>
<td>14 August 2014</td>
<td>Malware DNS trap clarification (&quot;Configuring a Malware DNS Trap&quot; on page 71) Made corrections in Disabling a Protection on a Specified Server (on page 34) and added Configuring Whitelist Files (on page 106).</td>
</tr>
<tr>
<td>1 July 2014</td>
<td>Cover changed to be relevant for all R77 versions. Updated for R77.20: Threat Emulation support for VSX in System Specifications (on page 17), Inspection of links inside mail (&quot;Configuring Inspection of Links Inside Mail&quot; on page 72), Threat Indicators (&quot;Threat Indicators Settings&quot; on page 107). Added AV deep inspection option in Configuring Anti-Virus Settings (on page 68) - applies from R77.10. Updated information for the asterisk character in Regular Expression Syntax (on page 151)</td>
</tr>
<tr>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>29 December 2013</td>
<td>Updated these sections and general formatting:</td>
</tr>
<tr>
<td></td>
<td>• <em>Local or Remote Emulation</em> (on page 23)</td>
</tr>
<tr>
<td></td>
<td>• <em>Using Local or Remote Emulation</em> (on page 28)</td>
</tr>
<tr>
<td></td>
<td>• <em>Threat Prevention CLI Commands</em> (on page 122)</td>
</tr>
<tr>
<td>27 August 2013</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

**Feedback**

Check Point is engaged in a continuous effort to improve its documentation. Please help us by sending your comments

mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Threat Prevention R77

Versions Administration Guide.
**Contents**

Important Information ........................................................................................................... 4  
Terms ................................................................................................................................... 11  
The Check Point Threat Prevention Solution ......................................................................... 13  
  Using Threat Prevention Software Blades .......................................................................... 13  
  Analyzing Threats .............................................................................................................. 13  
  SmartDashboard Toolbar ................................................................................................. 14  
Introduction to Threat Prevention Software Blades .............................................................. 15  
  Threat Emulation .............................................................................................................. 15  
    The Need for Threat Emulation ...................................................................................... 15  
    Selecting the Correct Location ...................................................................................... 15  
    Selecting the Threat Emulation Deployment .................................................................. 16  
    Check Point ThreatCloud Network .............................................................................. 17  
    System Specifications .................................................................................................... 17  
    Threat Emulation License Requirements ..................................................................... 18  
  Anti-Bot ............................................................................................................................ 18  
    The Need for Anti-Bot .................................................................................................... 18  
    The Check Point Anti-Bot Solution .............................................................................. 19  
  Anti-Virus ......................................................................................................................... 20  
    The Need for Anti-Virus .................................................................................................. 20  
    The Check Point Anti-Virus Solution .......................................................................... 20  
  Anti-Bot and Anti-Virus Licensing and Contracts .............................................................. 21  
Getting Started with Threat Emulation .................................................................................. 22  
  Threat Emulation Analysis Locations .............................................................................. 22  
    ThreatCloud Emulation .................................................................................................. 22  
    Local or Remote Emulation ............................................................................................ 23  
    Optimizing File Emulation ............................................................................................ 25  
  Threat Emulation Deployments ......................................................................................... 25  
    Inline Deployments (Prevent and Ask) ......................................................................... 26  
    Monitor Deployments ..................................................................................................... 26  
    Deployments with a Mail Transfer Agent ..................................................................... 26  
  Preparing for Local or Remote Emulation ......................................................................... 26  
  Running the First Time Configuration Wizard ................................................................... 27  
    Using Cloud Emulation .................................................................................................. 27  
    Using Local or Remote Emulation ................................................................................ 28  
  Using an MTA ................................................................................................................... 29  
    Enabling MTA on the Security Gateway ....................................................................... 29  
    Configuring the Network to Use an MTA ..................................................................... 30  
    Deploying MTA in BCC Mode ....................................................................................... 30  
  Sample Workflow - Creating a Threat Emulation Profile .................................................. 31  
Getting Started with Anti-Bot .............................................................................................. 32  
  Enabling the Anti-Bot Software Blade .............................................................................. 32  
  Creating an Anti-Bot Policy .............................................................................................. 32  
  Creating Rules ................................................................................................................... 32  
  Installing the Policy .......................................................................................................... 34  
Getting Started with Anti-Virus ........................................................................................... 36  
  Enabling the Anti-Virus Software Blade .......................................................................... 36  
  Creating an Anti-Virus Policy ........................................................................................... 36
Troubleshooting Threat Emulation ........................................................................... 128
Using MTA with ClusterXL .................................................................................... 128
Configuring Postfix for MTA .................................................................................. 128
Problems with Email Emulation ............................................................................ 128

Using Anti-Spam and Mail ....................................................................................... 129
Introduction to Anti-Spam and Mail Security ......................................................... 129
Mail Security Overview .......................................................................................... 130
Anti-Spam ................................................................................................................ 130
Adaptive Continuous Download ............................................................................. 131
Configuring Anti-Spam ............................................................................................. 132
Configuring a Content Anti-Spam Policy ................................................................. 132
Configuring an IP Reputation Policy ....................................................................... 132
Configuring a Block List .......................................................................................... 133
Configuring Anti-Spam SMTP ............................................................................... 133
Configuring Anti-Spam POP3 ............................................................................... 133
Configuring Network Exceptions .......................................................................... 134
Configuring an Allow List ....................................................................................... 134
Selecting a Customized Server ............................................................................. 134
Anti-Spam on UTM-1 Edge Devices ....................................................................... 134
Bridge Mode and Anti-Spam .................................................................................. 134
Configuring Anti-Virus Protection for Mail ............................................................. 135
Configuring Mail Anti-Virus ................................................................................... 135
Configuring Zero Hour Malware Protection ........................................................... 135
Configuring SMTP and POP3 ................................................................................. 136
Configuring File Types ........................................................................................... 136
Configuring Settings ............................................................................................... 137
Configuring a Disclaimer ....................................................................................... 137
Anti-Spam Logging and Monitoring ....................................................................... 137
Reporting False Positives to Check Point ............................................................... 137
Anti-Spam Tracking and Reporting Options ........................................................... 137
SmartView Tracker ................................................................................................. 138
SmartView Monitor ................................................................................................ 138
SmartReporter ......................................................................................................... 138

Using Traditional Anti-Virus .................................................................................. 139
Managing Traditional Anti-Virus ............................................................................ 139
Enabling Traditional Anti-Virus .............................................................................. 139
Database Updates .................................................................................................... 140
Understanding Traditional Anti-Virus Scanning Options ...................................... 141
Definitions ............................................................................................................. 141
Comparing Scan by File Direction and by IPs ....................................................... 141
Scanning by File Direction: Selecting Data to Scan .......................................... 144
Understanding Proactive and Stream Mode Detection ......................................... 145
Continuous Download ........................................................................................... 146
File Type Recognition ............................................................................................. 146
Configuring Traditional Anti-Virus ......................................................................... 147
Configuring Mail Traditional Anti-Virus ................................................................ 147
Configuring Zero Hour Malware ........................................................................... 147
Configuring SMTP, POP3, FTP and HTTP ............................................................ 147
Configuring File Types ........................................................................................... 148
Configuring Security Gateway Settings .................................................................. 149
Logging and Monitoring ......................................................................................... 149
**Terms**

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

**Affinity**
The assignment of a specified process, Firewall instance, VSX Virtual System, interface or IRQ with one or more 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.

**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 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.

**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 through the use of 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 or appliance that inspects traffic and enforces Security Policies for connected network resources.

**Security Management Server**
The application that manages, stores, and distributes the security policy to Security Gateways.

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

**SmartDashboard**
A Check Point client used to create and manage the security policy.

**SmartView Tracker**
A Check Point SmartConsole used to track and give audit information on real-time traffic, status of Software Blades, connections, activities, and events.

**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 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 resources.

**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:

Using Threat Prevention Software Blades .......................................................... 13
Analyzing Threats .................................................................................................. 13
SmartDashboard Toolbar ....................................................................................... 14

Using Threat Prevention Software Blades

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 deal with modern malware:

- Threat Emulation - Stops unknown malware, targeted attacks, and zero-day attacks
- Anti-Virus - Pre-infection blocking of known viruses and file transfers
- Anti-Bot - Post-infection bot detection, prevention, and threat visibility

Each Software Blade gives unique network protections and they can be combined to supply a strong malware solution. Data from malicious attacks are shared between the Threat Prevention Software Blade and help to keep your network safe. For example, the signature from threat that is identified by Threat Emulation is added to the Anti-Virus database.

The Threat Prevention Software Blades use a separate policy installation to minimize risk and operational impact. They are also integrated with other Software Blades on the Security Gateway to detect and stop threats.

Analyzing Threats

SmartView Tracker and SmartEvent let you easily investigate infections and assess damages.

The infection statistics and logs show detailed information per incident or infected host and a selected time interval (last hour, day, week or month). They also show the scanned hosts, the number of infected files and the malware detected.

The malware activity views give you insight as to the originating regions of malware, their corresponding IPs and URLs, and outgoing emails that were scanned.

The Threat Wiki shows extensive malware information. It includes malware type, description, and all available details such as executables run and used protocols.
# SmartDashboard Toolbar

You can use the SmartDashboard toolbar to do these actions:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌐</td>
<td>Open the SmartDashboard menu. When instructed to select <strong>Manage &gt; Users and Administrators</strong>, click this button to open the Manage menu and then select the <strong>Users and Administrators</strong> option.</td>
</tr>
<tr>
<td>📁</td>
<td>Save current policy and all system objects.</td>
</tr>
<tr>
<td>📃</td>
<td>Open a policy package, which is a collection of Policies saved together with the same name.</td>
</tr>
<tr>
<td>🔄</td>
<td>Refresh policy from the Security Management Server.</td>
</tr>
<tr>
<td>📘</td>
<td>Open the Database Revision Control window.</td>
</tr>
<tr>
<td>🔧</td>
<td>Change global properties.</td>
</tr>
<tr>
<td>📂</td>
<td>Verify Rule Base consistency.</td>
</tr>
<tr>
<td>🔧</td>
<td>Install the policy on Security Gateways or VSX Gateways.</td>
</tr>
<tr>
<td>🦂</td>
<td>Open SmartConsole.</td>
</tr>
</tbody>
</table>
Introduction to Threat Prevention
Software Blades

In This Section:

Threat Emulation .................................................................15
Anti-Bot .............................................................................18
Anti-Virus ..........................................................................20
Anti-Bot and Anti-Virus Licensing and Contracts ..................21

Threat Emulation

The Need for Threat Emulation

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. Threat Emulation can protect your network against new malware, zero-day vulnerabilities and targeted attacks http://www.checkpoint.com/products/threat-emulation/index.html.

Threat Emulation gives networks the necessary protection against unknown threats in files that are downloaded from the Internet or attached to emails. 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
- Information about malicious files and malware is shared with Check Point ThreatCloud and helps to protect all ThreatCloud users

Selecting the Correct Location

Where is the file emulation run?

- Check Point ThreatCloud ("ThreatCloud Emulation" on page 22)
- Threat Emulation Private Cloud Appliance (Emulation appliance) ("Local or Remote Emulation" on page 23)

What are the available emulation actions that I can use with a Threat Emulation profile?

- Prevent - Files do not go to the destination computer until emulation is completed. If Threat Emulation discovers that a file contains malware, the malicious file does not enter the internal network.
network. Users can notice a delay when downloading a file, because they cannot download and open the file until the emulation is complete.

- **Detect** - The file is sent to the destination and to Threat Emulation. If Threat Emulation discovers that a file contains malware, the appropriate log action is done. Users receive all files without delay.

**Emulation location options:**

<table>
<thead>
<tr>
<th>Emulation action</th>
<th>ThreatCloud</th>
<th>Emulation Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>All actions</td>
<td>All actions</td>
<td>All actions</td>
</tr>
<tr>
<td>Emulation is run</td>
<td>Check Point</td>
<td>Emulation appliance in the internal network</td>
</tr>
<tr>
<td>ThreatCloud</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note** - For more about how to estimate the system requirements and amount of file emulations for a network, see sk93598 http://supportcontent.checkpoint.com/solutions?id=sk93598.

**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)** - 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. We recommend that you enable the MTA on the Security Gateway for Threat Emulation profiles that use the Prevent action for SMTP traffic.

- **A Threat Emulation deployment that uses an MTA optimizes emulation for profiles that use the Prevent action.**

*I want to use the Prevent action and be able to block malicious files, what are my deployment options ("Threat Emulation Deployments " on page 25)?*

- **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>

### Check Point ThreatCloud Network

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 receive protection updates with enriched threat intelligence.

Customers that participate in the ThreatCloud network can use the collected malware data to benefit from increased security and protection. The ThreatCloud can then distribute attack information, and turn zero-day attacks into known signatures that the Anti-Virus Software Blade can block.

When you send files to the ThreatCloud service for emulation, your network gets up-to-date threat information and operating system environments.

You can always change this default behavior by altering a setting in SmartDashboard.

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. Restart SmartDashboard.
4. Install the Policy

For full details and instructions, see sk94509


### System Specifications

These are the specifications for the Threat Emulation deployments:

- Threat Cloud - R77 (or higher) Security Gateways with Gaia or SecurePlatform (64 or 32-bit)
- R77.20 (or higher) VSX Gateways
- For Local or Remote emulation:
  - Maximum size of file to send to emulation is: 100,000 KB
  - Check Point Threat Emulation Private Cloud Appliance with R77 or higher on the Gaia operating system (64-bit only), and R77.20 or higher VSX Gateways (Remote emulation only)

Make sure that:

- Each Virtual System has access to the Remote gateway or to the cloud.
- Each Virtual System Gateway has access to the Internet for updates from the Check Point Download Center.
Note - This release does not support:

- Active/Standby Bridge Mode
- Virtual System Load Sharing Security Clusters with more than two members.
- MTA

Threat Emulation License Requirements

There are separate licenses for ThreatCloud and local emulation. Make sure that you have the correct Threat Emulation licenses for your network.

ThreatCloud Emulation Quota

If you configure Threat Emulation to send files to the Check Point ThreatCloud for emulation, the license is the ThreatCloud Emulation Quota. This quota is the maximum number of files that a company or organization can send for emulation. It is reset at the start of each month.

Emulation Appliance License and Contract

If you configure Threat Emulation to run emulation on an Emulation appliance, there is a license and a contract for the Software Blade.

- License for the emulation.
- Annual contract for the Emulation appliance updates (separate from the ThreatCloud Emulation Quota). Emulation is not done if this contract expires.

For Emulation appliance configurations, it is necessary to only have a license and contract for the appliance. Even though Threat Emulation is enabled on the Security Gateway, it does not require a Threat Emulation license or contract. If you want to be able to send files to the ThreatCloud, it is necessary to have a ThreatCloud Emulation Quota.

Anti-Bot

The Need for Anti-Bot

There are two emerging trends in today's threat landscape:

- A profit-driven cybercrime industry that uses different tools to meet its goals. This industry includes cyber-criminals, malware operators, tool providers, coders, and affiliate programs. Their "products" can be easily ordered online from numerous sites (for example, do-it-yourself malware kits, spam sending, data theft, and denial of service attacks) and organizations are finding it difficult to fight off these attacks.

- Ideological and state driven attacks that target people or organizations to promote a political cause or carry out a cyber-warfare campaign.

Both of these trends are driven by bot attacks.

A *bot* is malicious software that can invade your computer. There are many infection methods. These include opening attachments that exploit a vulnerability and accessing a web site that results in a malicious download.
When a bot infects a computer, it:

- Takes control over the computer and neutralizes its Anti-Virus defenses. Bots are difficult to detect since they hide within your computer and change the way they appear to Anti-Virus software.
- Connects to a Command and Control (C&C) center for instructions from cyber criminals. The cyber criminals, or bot herders, can remotely control it and instruct it to execute illegal activities without your knowledge. These activities include:
  - Data theft (personal, financial, intellectual property, organizational)
  - Sending SPAM
  - Attacking resources (Denial of Service Attacks)
  - Bandwidth consumption that affects productivity

In many cases, a single bot can create multiple threats. Bots are often used as tools in attacks known as Advanced Persistent Threats (APTs) where cyber criminals pinpoint individuals or organizations for attack. A botnet is a collection of compromised computers.

Check Point's Anti-Bot Software Blade detects and prevents these bot threats.

The Check Point Anti-Bot Solution

The Anti-Bot Software Blade:

- Identifies bot infected machines in the organization by analyzing network traffic using the multi-layered ThreatSpect engine.
- Uses the ThreatCloud repository to receive updates and queries it for classification of unidentified IP, URL, and DNS resources.
- Prevents damage by blocking bot communication to C&C sites and makes sure that no sensitive information is stolen or sent out of the organization.
- Gives the organization threat visibility using different views and reports that help assess damages and decide on next steps.

Identifying Bot 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.

Check Point uses the ThreatSpect engine and ThreatCloud repository to find bots based on these procedures.
**ThreatSpect engine and ThreatCloud repository**

The ThreatSpect engine is a unique multi-tiered engine that analyzes network traffic and correlates information across multiple layers to find bots and other malware. It combines information on remote operator hideouts, unique botnet traffic patterns and behavior to identify thousands of different botnet families and outbreak types.

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.

The Security Gateway gets automatic binary signature and reputation updates from the ThreatCloud repository. It can query the cloud for new, unclassified IP/URL/DNS resources that it finds.

The layers of the ThreatSpect engine:

- **Reputation** - Analyzes the reputation of URLs, IP addresses and external domains that computers in the organization access. The engine searches for known or suspicious activity, such as a C&C.
- **Signatures** - Detects threats by identifying unique patterns in files or in the network.
- **Suspicious Mail Outbreaks** - Detects infected machines in the organization based on analysis of outgoing mail traffic.
- **Behavioral Patterns** - Detects unique patterns that indicate the presence of a bot. For example, how a C&C communicates with a bot-infected machine.

**Preventing Bot Damage**

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**

**The Need for 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. It also gives pre-infection protection from malware contained these files.

**The Check Point Anti-Virus Solution**

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.

Anti-Bot and Anti-Virus Licensing and Contracts

Make sure that you have a valid Security Gateway license and Anti-Bot and/or Anti-Virus contracts. For clusters, make sure you have a contract and license for each cluster member.

New and upgraded installations automatically receive a 30 day trial license and updates. Contact your Check Point representative to get full licenses and contracts.

The Anti-Bot blade and/or Anti-Virus blades do not work if you do not have a valid contract. When contracts are about to expire or have already expired, warnings show in these places:

• The Messages and Actions section of the Overview pane of the Threat Prevention tab.
• The Check Point User Center, when you log in to your account.
Getting Started with Threat Emulation

In This Section:

- Threat Emulation Analysis Locations ................................................................. 22
- Threat Emulation Deployments ........................................................................... 25
- Preparing for Local or Remote Emulation ......................................................... 26
- Running the First Time Configuration Wizard ...................................................... 27
- Using an MTA ....................................................................................................... 29
- Sample Workflow - Creating a Threat Emulation Profile ................................ 31

Threat Emulation Analysis Locations

You can choose a location for the emulation analysis that best meets the requirements of your company. Run the file emulation in the ThreatCloud or on a Threat Emulation Private Cloud Appliance (Emulation appliance) in the internal network.

- **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.

- **Internal network** - You can use an Emulation appliance to run emulation on the files.

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>Computers and servers in the internal network</td>
</tr>
<tr>
<td>4</td>
<td>Check Point ThreatCloud servers</td>
</tr>
</tbody>
</table>

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.
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.
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.

Threat Emulation Deployments

You can use inline or monitor deployments for file emulation.

**Inline** - Use **Prevent** and **Ask** actions to block traffic before it goes to the internal computer. You can configure how Threat Emulation handles connections while it finishes the emulation of a file ("Handling Connections During Emulation" on page 115):

- **Background** - The traffic is allowed to enter the internal network
- **Hold** - The traffic is blocked and does not enter the internal network until after emulation is finished
Monitor - Use a SPAN or TAP configuration to duplicate network traffic. The files are then sent directly to Threat Emulation and the computer in the internal network. If Threat Emulation discovers that a file contains malware, the applicable log action is done. Monitor deployments support only the Detect action.

Inline Deployments (Prevent and Ask)

Use the Prevent or Ask UserCheck action to quarantine a malicious file ("Threat Prevention and UserCheck" on page 61).

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

Deployments with a Mail Transfer Agent

If you use the Prevent action to block traffic, we recommend that you enable the Security Gateway as an MTA (Mail Transfer Agent) for SMTP traffic. You can use the MTA to help manage the emulation of emails and attachments ("Using an MTA" on page 29).

Preparing for Local or Remote Emulation

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

1. Open SmartDashboard.
2. Create the network object for the Emulation appliance.
3. If you are running emulation on HTTPS traffic, configure the settings for HTTPS Inspection ("Using Threat Prevention with HTTPS Traffic" on page 76).
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.
Running the First Time Configuration Wizard

Use the First Time Configuration Wizard in SmartDashboard to enable Threat Emulation in the network. Configure the Security Gateway or Emulation appliance for your deployment.

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.

Note - For ThreatCloud emulation, it is necessary that the Security Gateway can connect to the Internet. We recommend that you make sure that the DNS and proxy settings are configured correctly in Global Properties.

To enable ThreatCloud emulation:

1. Double-click the perimeter 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. Select ThreatCloud Emulation Service.
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 the policy on the Security Gateway.
Using Local or Remote Emulation

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

**Note** - Make sure that you prepare the network for the Emulation appliance before you run the First Time Configuration Wizard (“Preparing for Local or Remote Emulation” on page 26).

To enable an Emulation appliance for Local and Remote emulation:

1. Double-click the Emulation appliance.
   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.
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 policy on the Emulation appliance.

To enable Threat Emulation on the Security Gateway for Remote emulation:

1. 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 Emulation appliance.
   b) From the drop-down menu, select the 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.
Using an MTA

You can enable the Security Gateway as an MTA (Mail Transfer Agent) to manage the emulation of SMTP traffic. It is possible that during file emulation, the email server cannot keep the connection open for the time that is necessary for full emulation. When this happens, there is a timeout for the email. A Threat Emulation deployment with an MTA avoids this problem, the MTA completes and closes the connection with the source email server and then sends the file for emulation. After the emulation is complete, the MTA sends the email to the mail server in the internal network.

- For topologies that use TLS between the Security Gateway and the mail server, Threat Emulation must use an MTA to decrypt emails for emulation.
- When Threat Emulation identifies that an email attachment is malicious, the MTA removes the attachment and sends the safe email.
- We recommend that you use an MTA for Threat Emulation profile settings that block SMTP traffic. Without an MTA, it is possible that safe emails are dropped and do not reach the computers in the internal network.

To use the Security Gateway as an MTA:
2. Configure the network to forward emails to the MTA ("Configuring the Network to Use an MTA" on page 30).

Enabling MTA on the Security Gateway

For a topology that uses TLS between the Security Gateway and the mail server, you must import the mail server certificate to the Security Gateway.

To enable the Security Gateway as an MTA:
1. Double-click the Security Gateway and from the navigation tree select Mail Transfer Agent. The Mail Transfer Agent page opens.
2. Select Enable as a Mail Transfer Agent.
3. In the Mail Forwarding section, add one or more rules.
   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 send all traffic.
   d) Click OK.
   e) Click the Next Hop cell and select the node object that is the mail server for this rule.
      You can also configure the MTA to only run emulation and not forward emails to the mail server ("Deploying MTA in BCC Mode" on page 30).
4. Optional: Select Sign scanned emails and enter the message to add to emails when emulation is finished.
5. 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**.

6. **Optional:** In the **Advanced Settings** section, click **Configure Settings** and configure the MTA interface and email settings ("Configuring MTA Advanced Settings" on page 116).

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

**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 ("Disabling the MTA" on page 117), 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 BCC Mode**

You can use the Check Point MTA to only monitor SMTP traffic. Configure the MTA to send emails only for emulation, 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. Double-click the Security Gateway and from the navigation tree select **Mail Transfer Agent**.
   The **Mail Transfer Agent** page opens.
2. Make sure that all the **Mail Forwarding** rules are deleted.
3. Click the add rule button.
4. Click the Next Hop cell and click New.
   The Host Node window opens.
5. Configure these settings:
   • Name - For example, No_Forward
   • IPv4 Address - Enter 0.0.0.0
6. Click OK.
   The Host Node window closes, and the server object is added to the Next Hop cell.
7. Click OK and then install the policy.

Sample Workflow - Creating a Threat Emulation Profile

This is a sample workflow to create a Threat Prevention profile ("Creating Profiles" on page 66) that includes Threat Emulation. To run emulation on HTTPS traffic, enable and configure HTTPS inspection ("Using Threat Prevention with HTTPS Traffic" on page 76).

To create a Threat Prevention profile for Threat Emulation:
1. From Threat Prevention >Profiles, click New.
2. Select the Threat Prevention Software Blades for the profile.
3. Configure the Protection Activation settings for the traffic.
4. From the Threat Emulation Settings page, set the Prevent and Ask UserCheck settings.
5. Configure the Threat Emulation Protected Scope for this profile, and define how traffic from external and internal networks is sent for emulation.
6. Select one or more protocols for this profile.
   The Software Blade runs emulation only for files and traffic that match the selected protocols.
7. Configure the file types for this profile.
   The Software Blade runs emulation only for files that match the selected file types.
8. Save the profile.
Getting Started with Anti-Bot

In This Section:

- Enabling the Anti-Bot Software Blade.................................................................32
- Creating an Anti-Bot Policy......................................................................................32

Enabling the Anti-Bot Software Blade

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

To enable the Anti-Bot Software Blade:

1. In SmartDashboard, right-click the gateway object and select Edit. The Gateway Properties window opens.
3. Select one of the activation mode options:
   - 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 the Threat Prevention policy.

Creating an Anti-Bot Policy

Create and manage the policy for the Anti-Bot Software Blade in the Threat Prevention tab of SmartDashboard. The policy shows the profiles set for network objects or locations defined as a protected scope.

- The Overview pane shows a high-level summary of your Anti-Bot activity and traffic.
- The Policy pane shows the rules and exceptions for the Anti-Bot policy. Click the Add Rule button to get started.
- To learn about bots and protections, look through the Threat Wiki.

Creating Rules

Here are examples of how to create different types of Anti-Bot rules.
**Blocking Bots**

*Scenario: I want to block bots in my organization. How can I do this?*

**To block bots in your organization:**

1. In the Gateway Properties page, select the **Anti-Bot Software Blade**. The First Time Activation window opens.
2. Select **According to the Anti-Bot and Anti-Virus policy** and click **OK**.
3. Select **Threat Prevention > Policy**.
4. Click **Add Rule**.
   - A new rule is added to the Threat Prevention policy. The Software Blade applies the first rule that matches the traffic.
5. 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. In this example, the Any network object is used.
   - **Action** - The Profile that contains the protection settings you want ("Profiles Pane" on page 65). The default profile is **Recommended_Profile**.
   - **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. In SmartView Tracker, you will then be able to view the actual packets.
   - **Install On** - Keep it as All or choose specified gateways to install the rule on.
6. Install the Threat Prevention policy.

**Monitoring Bot Activity**

*Scenario: I want to monitor bot activity in my organization without blocking traffic at all. How can I do this?*

**To monitor all bot activity:**

1. In the Threat Prevention tab of SmartDashboard, open the **Policy** pane.
2. Click one of the **Add Rule** toolbar buttons to add the rule in the position that you choose in the Rule Base. The first rule matched is applied.
3. Give the rule a name, such as **Monitor Bot Activity**.
4. In **Protected Scope**, do not change from Any. The rule applies to all traffic in the organization.
5. Right-click in the **Action** cell and select **New Profile**.
6. In the **New Profile** window, set all confidence level settings to **Detect**.
7. Set **Performance Impact** to **Medium or lower**.
   - This profile will detect attacks with low, medium or high confidence and have a medium or lower performance impact.
8. Name the profile.
9. Click **OK**.
### Disabling a Protection on a Specified Server

**Scenario:** The protection Backdoor.Win32.Agent.AH detects malware on a server (Server_1). How can I disable this protection for this server only?

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

1. In the Threat Prevention tab of SmartDashboard, open the Policy pane.
2. Click the rule that contains the scope of Server_1.
3. Click the Add Exception toolbar button to add the exception under the rule. The first exception matched is applied.
4. Make a rule exception that includes these components:
   - **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/File/Indicator** - Click + in the cell to open the Add Objects window.
5. Select items to exclude:
   - **Protection** - Predefined malware signature
   - **Site** - Web site, URL, or category of sites
   - **File** - Filenames
     
     **Note** - To add EICAR files as exceptions, you must add them as Whitelist Files (“Configuring Whitelist Files” on page 106). Adding EICAR files through Exceptions in Policy rules will still get them blocked.
6. Click OK.
7. In the rule, leave defaults for **Action** (Detect), **Track** (Log), and **Install On** (All).

### Installing the Policy

The Anti-Bot, Threat Emulation and Anti-Virus Software Blades have a dedicated policy. You can install this policy installation separately from the policy installation of the other Software Blades.

You can update the Anti-Bot, Threat Emulation and Anti-Virus Rule Base to give immediate coverage for new malware threats. Install only the Threat Prevention policy to minimize the impact on the Security Gateways.

**To install the Anti-Bot and Anti-Virus policy:**

1. From the Threat Prevention tab > Policy pane, click Install Policy.
2. Select the relevant options:
   - **Install Threat Prevention Policy on all gateways** - Installs the policy on all Security Gateways that have Anti-Bot, Threat Emulation, and Anti-Virus enabled.
• **Install Threat Prevention Policy on selected gateways** - Select the applicable Security Gateways.

• **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.

3. Click **OK**.
Getting Started with Anti-Virus

**In This Section:**
- Enabling the Anti-Virus Software Blade ......................................................... 36
- Creating an Anti-Virus Policy ............................................................................. 36
- Blocking Viruses .............................................................................................. 37

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 SmartDashboard, right-click the gateway object and select **Edit**. The **Gateway Properties** window opens.
2. In **Network Security** tab, select **Anti-Virus**. 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 the Threat Prevention policy.

Creating an Anti-Virus Policy

Create and manage the policy for the Anti-Virus Software Blade in the Threat Prevention tab of SmartDashboard. The policy shows the profiles set for network objects or locations defined as a protected scope.

- The **Overview** pane shows a high-level summary of your Anti-Virus activity and traffic.
- The **Policy** pane shows the rules and exceptions for the Anti-Virus policy. Click the **Add Rule** button to get started.
- To learn about malware and protections, look through the Threat Wiki.

You can use Anti-Virus rules to disable a specified malware protection ("Disabling a Protection on a Specified Server" on page 34).

After you create and configure the rules, install the policy on the specified Security Gateways (see "Installing the Policy" on page 34).
Blocking Viruses

Scenario: I want to block viruses and malware in my organization. How can I do this?

To block viruses in your organization:

1. In the Gateway Properties page, select the Anti-Virus Software Blade.
   The First Time Activation window opens.
2. Select According to the Anti-Bot and Anti-Virus policy and click OK.
3. Select Threat Prevention >Policy.
4. Click Add Rule.
   A new rule is added to the Threat Prevention policy. The Software Blade applies the first rule that matches the traffic.
5. Make a rule that includes these components:
   - **Name** - Give the rule a name, such as Block Virus Activity.
   - **Protected Scope** - Add the network objects you want to protect. In this example, the Any network object is used.
   - **Action** - Select the Profile with the protection settings you want ("Profiles Pane" on page 65). The default profile is Recommended Profile.
   - **Track** - Select the type of log to get when malware is detected. In this example, keep Log and also select Packet Capture, to capture the packets of malicious activity. In SmartView Tracker, you can see the captured packets.
   - **Install On** - Keep it as All, or select gateways to install the rule on.
6. Install the Threat Prevention policy.
Getting Started with the Threat Extraction Blade

In This Section:

- Enabling the Threat Extraction Blade
- Configuring the Threat Extraction Blade
- Threat Extraction Statistics
- Using the Gateway CLI
- Troubleshooting the Threat Extraction Blade

Important: Threat Extraction is supported only on R77.30 and higher.

Before you enable the Threat Extraction blade, you must deploy the gateway as a Mail Transfer Agent ("Enabling MTA on the Security Gateway" on page 29).

The Threat Extraction blade extracts potentially malicious content from files before they enter the corporate network. To remove possible threats, the Threat Extraction blade can create a simpler version of the file in PDF format.

Microsoft Office Suite Applications support many features that can pose a threat to the corporate network. For example:

- 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
- User names

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
- Lists of user names
Enabling the Threat Extraction Blade

**Important:** Before enabling the Threat Extraction blade, make sure the R77.30 Add-on is installed on the Security Management Server. For more about the add-on, see the *R77.30 Release Notes*.

**To enable the Threat Extraction Blade:**

1. In SmartDashboard, right-click the R77.30 gateway object and select *Edit*. The *Gateway Properties* window opens.
2. On the *General Properties > Network Security* tab, select:
   - *Firewall*
   - *Threat Extraction*
   The *Threat Extraction First Time Activation Wizard* opens.
3. Enable the gateway as a *Mail Transfer Agent* (MTA).
   From the drop-down box, select a mail server for forwarded emails.
4. Click *Next*.
5. Click *Finish*.
   **Note:** In a ClusterXL HA 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 *SmartDashboard > Global Properties*.
3. Click *OK*.

**Configuring the Threat Extraction Blade**

Threat Extraction settings are configured:

- On the Security Gateway object or cluster object
- In Threat Prevention Profiles
- On the Threat Prevention tab > Advanced > Engine Settings page

**Configuring the Security Gateway**

1. Open SmartDashboard.
2. Open the *gateway properties > Threat Extraction* page.
3. Set the *Activation Mode* to *Active*.
4. Allocate disk space resources.
5. Click *OK*. 
Configuring a Cluster

1. Open SmartDashboard.
2. Open the ClusterXL and VRRP page.
3. Select High Availability.
4. In the Upon cluster Member recovery section, select Switch to higher priority Cluster Member.
5. On the Cluster Members page, make sure the primary member (the member at the top of the list that automatically becomes the active server) has strong memory and CPU resources.
6. Enable the Threat Extraction Blade:
   a) On the General Properties > Network Security tab, select:
      - Firewall
      - Threat Extraction
      The Threat Extraction First Time Activation Wizard opens.
   b) Enable the gateway as a Mail Transfer Agent (MTA).
   c) From the drop-down box, select a mail server for forwarded emails.
   d) Click Next.
   e) Click Finish.
7. In the Cluster Properties window, open Other > Threat Extraction.
8. Set the Activation Mode to Active.
9. Allocate disk space resources.
10. Click OK.
11. Install policy.

Configuring the Threat Prevention Profile

1. Open SmartDashboard.
2. On the Threat Prevention tab, open Profiles.
3. Right-click a profile and select Edit.
   The profile's properties window opens.
5. On the Threat Extraction Settings page, configure:
   UserCheck Messages
   • 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
Protocols

- **Mail (SMTP)**
  
  Click **Configure** to set the maximum MIME nesting level for emails that contained nested MIME content.

Extraction Method

- **Extract files from potential malicious parts**
  
  Click **Configure** to select which malicious parts the blade extracts, for example macros or JavaScript.

- **Convert to PDF**
  
  Converts the file to PDF, and keeps text and formatting.

**Note** - If you use PDFs in Right-to-Left languages or Asian fonts, we recommend that you DO NOT select the **Convert to PDF** option. Otherwise, the formatting and content in the PDF can be significantly changed. Select the **Extract files from potential malicious parts** option to make sure that these files are processed correctly.

Extraction Settings

- **Process all files**
- **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 supported file types**
- **Process specific file types**
  
  Click **Configure** to select file types.

6. On the **Exclude/Include Users** page, configure these settings:

- **Scan all mail**
  
  Click **Exceptions** to not include specified users, groups, recipients or senders.

- **Scan mail only for specific users or groups**
  
  Click **Configure** to select specified User Groups, Recipients or Senders.

  **Note:**

  A **user** is an object that can contain an email address with other details.
  
  A **group** is an AD group or LDAP group of users
  
  A **recipient** is an email address only.

Important: In **Global Properties > User Directory**, make sure that you have selected the **Use User Directory for Security Gateways** option.

7. On the **Advanced** page, configure these settings:

- **Logging**
  
  - Log only those files from which threats were extracted
  
  - Log every file
Threat Extraction Exceptions

- **Corrupted files**
  Block or Allow corrupted files attached to the email. 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 corrupt attachment and sends the recipient a text describing how the attachment 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 corrupt file attachment.

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

  *Block* removes the encrypted attachment and sends the recipient a text file describing how the attachment 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 attachment.

- **Signed emails**
  Allow or Clean signed emails.

  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. 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.

8. Click **OK**.

Configuring Advanced Engine Settings for Threat Extraction

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

**To configure file type support:**

1. Open SmartDashboard.
2. On the **Threat Prevention** tab, open **Advanced > Engine Settings**.
3. In the **Threat Extraction Settings** area, click **Configure file type support**.
   - The **File Types Support** window opens.
4. From the list select which file types the Threat Extraction blade supports.
5. Click **OK**.
To configure mail signatures:
1. Open SmartDashboard.
2. On the Threat Prevention tab, open Advanced > Engine Settings.
3. In the Threat Extraction Settings area, 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 mail that has 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
     Predefined field codes can be inserted 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 recipient the file. You can also find the ID in the logs.
   4. Click OK.

Threat Extraction Statistics
You can see Threat Extraction statistics in SmartDashboard, and by running a number of commands on the CLI.

In SmartDashboard:
1. Open Threat Prevention tab > Overview.
2. Scroll to Latest Malware Activity.
3. Click Extracted Files.

On 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 R77.30 gateway has a Threat Extraction menu to:
- Control debug messages
- Get information on queues
- Send the initial email attachments to recipients
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. Using this command helps you understand the queue status and load on the mail transfer agent (MTA) and the scrubd daemon. The command shows:</td>
</tr>
<tr>
<td></td>
<td>• Number of pending requests from the MTA to the scrubd daemon</td>
</tr>
<tr>
<td></td>
<td>• Maximum number pending requests from the MTA to the scrubd daemon</td>
</tr>
<tr>
<td></td>
<td>• Current number of pending request from scrubd to scrub_cp_file_convert</td>
</tr>
<tr>
<td></td>
<td>• Maximum number of pending requests from scrubd to scrub_cp_file_convert</td>
</tr>
<tr>
<td>send_orig_email</td>
<td>Sends original email to recipients. To send the original email get:</td>
</tr>
<tr>
<td></td>
<td>• The reference number - Click on link in the email received by the user.</td>
</tr>
<tr>
<td></td>
<td>• The email ID - Found in the SmartView Tracker logs or debug logs.</td>
</tr>
<tr>
<td>bypass</td>
<td>Bypasses all files. Use this command to debug issues with the scrub (Threat Extraction) daemon. When you set bypass to active, requests from the mail transfer agent (MTA) to the scrub daemon are not handled. Threat Extraction is suspended. No files are cleaned.</td>
</tr>
</tbody>
</table>

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 SmartDashboard > 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 SmartDashboard, 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 SmartView Tracker or SmartLog.
2. Select the Threat Extraction Blade.
3. Add the column for the Threat Extraction Activity and look for errors.

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. In SmartDashboard, open Threat Prevention > Advanced > Engine Settings.
2. Under Fail Mode, 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 SmartView Tracker and SmartLog. Corrupted attachments are still sent to the email recipient. To prevent corrupted attachments from reaching the recipient:

1. In SmartDashboard, 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**

2. In the File Types area, 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.
Managing Threat Prevention

In This Section:
- The Threat Prevention Overview Pane ................................................................. 47
- The Check Point ThreatCloud .............................................................................. 49
- The ThreatCloud Repository ............................................................................... 50
- Exception Groups Pane ...................................................................................... 52
- Gateways Pane ...................................................................................................... 54
- Protections Browser .............................................................................................. 55
- The Policy Rule Base ............................................................................................ 56
- Threat Prevention and UserCheck ........................................................................ 61
- Profiles Pane .......................................................................................................... 65
- Sites Pane .............................................................................................................. 74

The Threat Prevention Overview Pane

In the Threat Prevention Overview page, you can quickly see the gateways in your organization that are enforcing Threat Prevention Software Blades and malware details. Use the windows for the most urgent or commonly-used management actions.

To customize windows you see in the Overview pane:
1. In the Overview pane, click Customize.
2. Select or clear the windows to show or hide them.
3. To restore the original view, click Reset.
4. Click OK.

My Organization

The My Organization window shows the Threat Prevention Software Blades that are enabled on the Security Gateways.

- Click Security Gateways to open the Gateways window in the Threat Prevention tab
- Click Add Gateway to open the Gateway Properties window of a Security Gateway or to create a new one

Messages and Action Items

The Messages and Action Items window includes:
- A direct link to Check Point for reporting malicious files that were not identified as such.
- A search field that lets you enter a malware name to get a detailed description of the malware and severity, family name, and type details. The system queries the Threat Wiki for this information.
- Shows if a new Anti-Bot and Anti-Virus update package is available.
- Shows if Security Gateways require renewed licenses and/or contracts.
Statistics

The **Statistics** window shows up-to-the-minute statistics in timeline wheels for one of these malware threats:

- **Infection** - The Anti-Bot Software Blade gives protection against bot attacks.
- **Viruses** - The Anti-Virus Software Blade gives protection against known malicious software and code.
- **Advanced Threats** - The Threat Emulation Software Blade identifies and gives protection against new malicious software and code.

This window also shows statistics for:

- Incidents - Viruses or bots detected by the system.
- Detected hosts - Hosts that have been compromised with traffic containing a virus or bot. The number of detected hosts shown is related to the Protected Scope values (the network objects you want to protect) in the policy. For example, if the protected scope of a rule refers to the internal network, the number of detected hosts in the time wheels will be from the internal network.

The timeline wheels are grouped according to:

- Selected time interval - hour, day, week or month
- Severity - color-coded according to critical, high, medium and low

When you hover over a timeline wheel you get drilled-down information for the selected time interval. For example, if your selected time interval is **week**, you will see 7 timeline wheels for each day. When you hover over a wheel, you will see the breakdown of the number of incidents or detected hosts according to each severity.

This window also has links to open **SmartView Tracker** to see Threat Prevention logs and **SmartEvent** to see traffic graphs and analysis.

The bottom part of the window shows a time-line of the selected time interval.

**To show statistics by incidents or detected hosts:**

1. In the **Statistics** window, select the time interval from the **In the last** list.
2. Select whether to show incidents or detected hosts from the **by** list.
3. To refresh the list, click the refresh icon.

Malware Activity

The **Latest Malware Activity** window shows you the originating regions of malware, their corresponding IP addresses and URLs, and outgoing emails that were scanned.

- **Attack Map** - Pinpoints regions in the world that are attacking your organization and the corresponding number of incidents. This information comes from aggregated data on suspicious URLs and IPs.
- **Attacker IPs/URLs** - Shows details for the pinpointed regions in the Attack Map. These details include the specified URLs or IP addresses, the number of attempts and the severity.
- **Suspicious Email** - Shows the number of outgoing emails scanned from when the Anti-Bot and Anti-Virus Software Blades were activated. This window does not show the results of emails scanned by Threat Emulation.
RSS Feeds
Shows RSS feeds with malware related information. When you click a link, it opens the Check Point Threat Wiki.

The Check Point ThreatCloud
To continuously improve our Threat Prevention products, Security Gateways can automatically send anonymous information about feature usage, infection details, and end-user product customization to the Check Point ThreatCloud. The Security Gateway does not collect or send any personal data.

Participating 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. Your participation in this network allows you to contribute data to Check Point for security research. This research aims to improve coverage, quality, and accuracy of security services and obtain valuable information for organizations.

Data 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" />
```

The above 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 above data does not contain any confidential information or internal resource information. The source IP address is obscured. Information sent to the Check Point Lab is stored in an aggregated form.

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.
   c) To disable the Security Gateway to share Anti-Bot and Anti-Virus information with the ThreatCloud, clear Share anonymous attack information with Check Point ThreatCloud.
3. Configure the settings for the Threat Emulation Software Blade.
   **Note:** These settings are not relevant when you are using the ThreatCloud emulation service, the files and information are 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**.

c) Select **Share malicious files with Check Point** to send malware files that the Threat Prevention Software Blade identifies to the ThreatCloud.

d) To disable the Security Gateway to share Threat Emulation information with the ThreatCloud, clear **Share anonymous attack information with Check Point ThreatCloud**.

4. Click **OK**.

---

### The ThreatCloud Repository

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 ("Updating the Malware Database" on page 51).
- 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:

- **SmartDashboard** - From the Anti-Bot and Anti-Virus Rule Base in SmartDashboard, click the plus sign in the **Protection** column, and the Protection viewer opens. From there you can add specific malwares to rule exceptions when necessary.
- **Threat Wiki** - A tool to see the entire Malware database. Open it from the Threat Wiki pane in the Threat Prevention tab or from the Check Point website.

### Using the Threat Wiki

The Threat Wiki is an easy to use tool that lets you search and filter the ThreatCloud repository to find more information about identified malware.

- Learn about malware.
- Filter by category, tag, or malware family.
- Search for a malware.

You can access the Threat Wiki from:

- The Threat Prevention tab
- The Check Point website
• SmartEvent
  • Right-click an event and select Go to Threat Wiki.
  • Click the malware protection link in the event log.
  • Select Go to Threat Wiki from the Anti-Virus or Anti-Bot tab in the event log.
• SmartView Tracker - Click the malware protection link in the Protection Name field of a log record.

Updating the Malware Database
The Malware database automatically updates regularly to make sure that you have the most current data and newly added signatures and URL reputations in your Anti-Bot and Anti-Virus policy.
The Malware database only updates if you have a valid Anti-Bot, Threat Emulation and/or Anti-Virus contract.
By default, updates run on the Security Gateway every two hours. You can change the update schedule or choose to manually update the Security Gateway. The updates are stored in a few files on each Security Gateway.

Connecting to the Internet for Updates
The Security Gateway connects to the internet to get the Malware database updates. To make sure that it can get the updates successfully:
• Make sure that there is a DNS server configured.
• Make sure a proxy is configured for each gateway, if necessary.

To configure a proxy:
1. The Advanced > Updates pane shows if the Security Gateway uses a proxy to connect to the internet or not.
2. Click Configure Proxy and select a gateway from the list.
3. Click Edit and configure the proxy for the gateway.
4. Click OK.

Scheduling Updates
You can change the default automatic scheduling. If you have Security Gateways in different time zones, they will not be synchronized when one updates and the other did not yet update.

To change the update schedule:
1. Select Threat Prevention > Advanced > Updates.
   The Updates page opens.
2. Make sure that Update malware database is selected.
3. Next to the Update malware Database option, click Schedule.
   The Scheduled Event Properties window for the Anti-Bot and Anti-Virus database opens.
4. 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.
5. Click **OK** and then install the Threat Prevention policy.

**Exception Groups Pane**

The **Exceptions Groups** pane lets you define exception groups. When necessary, you can create exception groups to use in the Rule Base. An exception group contains one or more defined exceptions. This option facilitates ease-of-use so you do not have to manually define exceptions in multiple rules for commonly required exceptions. You can choose to which rules you want to add exception groups. This means they can be added to some rules and not to others, depending on necessity.

The pane shows a list of exception groups that have been created, what rules are using them, and any comments associated 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 Global Exceptions 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 will 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 adding 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 the Threat Prevention tab, select Exception Groups.
2. Click New.
3. From the New Exception Group window, enter:
   - Name - Mandatory, cannot contain spaces or symbols
   - Color - Optional color for SmartDashboard object mapping
   - Comment - Optional free text
4. Click OK.

Adding Exceptions to Exception Groups

To use exception groups, you must add exception rules to them. For details on the columns, see Parts of the Rules (on page 58).

To add exceptions to an exception group:
1. In the Threat Prevention tab, select Exception Groups.
2. From the tree, select the group to which you want to add exceptions.
   A pane opens showing the exception group name.
3. Use the Add Top and Add Bottom icons to add exceptions.

Adding Exception Groups to the Rule Base

To add an exception group to the Rule Base:
1. In the Policy pane, select the rule to which you want to add an exception group.
2. Click Add Exception > Add Exception Group.
3. Select the Above, Below, or Bottom option according to where you want to place the exception group.
   The Add Exception Group to rule window opens.
4. Select the group from the list and click OK.
   The exception group is added to the Threat Prevention policy.
5. Click Install Policy to install the Anti-Bot, Threat Emulation, and Anti-Virus policy (see "Installing the Policy" on page 34).
Creating Exceptions from Logs or Events

In some cases, after evaluating a log in SmartView Tracker or an event in SmartEvent, it may be necessary to update a rule exception in the SmartDashboard Rule Base. You can do this directly from within SmartView Tracker or SmartEvent. You can apply the exceptions to a specified rule or apply the exception to all rules that shows under Global Exceptions.

To update a rule exception or global exception:

1. Right-click a SmartView Tracker log entry or a SmartEvent event.
2. Select Add Exception to the Rule.
   SmartDashboard opens and shows an Add Exception window in the Threat Prevention Rule Base. These details are shown:
   - **Protection** - The name of the protection. Details are taken from the ThreatCloud repository or, if there is no connectivity, from the log.
   - **Scope** - The scope is taken from the log. If there is no related host object, an object is created automatically after you click OK. Click the plus sign to add additional objects.
   - **Install On** - Shows All by default. You can use the plus sign to add gateways.
3. Select an Exception Scope option:
   - **Apply Exception to rule number X** - If you want the exception to apply only to the related rule.
   - **Apply Exception to all rules** - If you want the exception to apply to all rules. The exception is added to the Exception Groups >Global Exceptions pane.
4. Click OK.
   The exception is added to the Rule Base. The **Action** is set to Detect by default. Change if necessary.
5. Click Install Policy to install the Anti-Bot, Threat Emulation, and Anti-Virus policy (see "Installing the Policy" on page 34).

Gateways Pane

The Gateways page lists the Security Gateways that use one or more of these Software Blades: Anti-Bot, Threat Emulation, and Anti-Virus. The left pane shows the Security Gateways that use these Software Blades, the right pane shows the Threat Prevention details for the selected Security Gateway. Threat Emulation is supported only on Security Gateways and Emulation appliance in the internal network.

<table>
<thead>
<tr>
<th>Option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add a Security Gateway or create a new Security Gateway</td>
</tr>
<tr>
<td>Edit</td>
<td>Modify an existing Security Gateway</td>
</tr>
<tr>
<td>Remove</td>
<td>Disable the Threat Prevention Software Blades on the selected Gateway</td>
</tr>
<tr>
<td>Actions &gt;Update</td>
<td>Connect to the ThreatCloud to download new operating system images</td>
</tr>
</tbody>
</table>
Option | Meaning
---|---
Search | Search for a Security Gateway

The left pane shows the name, IPv4 and IPv6 address for each Security Gateway. These columns also show the following information about the Security Gateways:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Bot</td>
<td>If Anti-Bot is enabled</td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>If Anti-Virus is enabled</td>
</tr>
<tr>
<td>Threat Emulation</td>
<td>If Threat Emulation is enabled</td>
</tr>
<tr>
<td>Update Status</td>
<td>If the Malware database is up to date on the Security Gateway or if an update is necessary</td>
</tr>
</tbody>
</table>

The right pane shows the details for the Threat Prevention Software Blades that are enabled on the Security Gateway.

## Protections Browser

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

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>Shows the name of the protection type. A description of the protection type is shown in the bottom section of the pane. The Malicious Activity and Unusual Activity protections contain lists of protections. Click the plus sign to see them.</td>
</tr>
<tr>
<td>Blade</td>
<td>Shows if the protection type belongs to the Anti-Bot, Threat Emulation or Anti-Virus Software Blade.</td>
</tr>
<tr>
<td>Engine</td>
<td>Shows the layer of the ThreatSpect engine that handles the protection type.</td>
</tr>
<tr>
<td>Known Today</td>
<td>Shows the number of known protections.</td>
</tr>
<tr>
<td>Performance Impact</td>
<td>Shows how much the group of protections affects the performance of the Security Gateway. If possible, shows an exact figure.</td>
</tr>
<tr>
<td>&lt;Profile Name&gt;</td>
<td>Shows the activation setting of the protection type for each defined profile. The values shown here are calculated based on the settings of the confidence levels in the profile and the specified protections that match that confidence level. You can right-click the activation setting and select a different setting if required. This overrides the setting in the original profile.</td>
</tr>
</tbody>
</table>
Searching Protections

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

**To filter by protection name:**
- In the search box, enter your search text.
  - The list filters as you type and the results are highlighted in yellow.

Sorting Protections

You can sort the Protection, Blade, Engine, Known Today columns in the Protections list.

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

The Policy Rule Base

The Threat Prevention policy determines how the system inspects connections for bots and viruses. The primary component of the policy is the Rule Base. The rules use the Malware database and network objects.

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

There are no implied rules in the Rule Base. All traffic is allowed unless it is explicitly blocked.

For examples of how to create different types of rules, see the applicable section for the Threat Prevention Software Blade:
- Anti-Bot ("Creating Rules" on page 32)
- Threat Emulation ("Sample Workflow - Creating a Threat Emulation Profile" on page 31)
- Anti-Virus

Predefined Rule

When you enable a Threat Prevention Software Blade, 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 58) value equals any) is inspected for all protections according to the recommended profile ("Profiles Pane" on page 65). 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 **Recommended Profile**) is that:
- All protections that can identify an attack with a high or medium confidence level and have a medium or lower performance impact are set to **Prevent** mode.
- All protections that can identify an attack with a low confidence level and have a medium or lower performance impact are set to **Detect** mode.

You can see logs related to Threat Prevention traffic in SmartView Tracker and SmartEvent. Use the data there to better understand the use of Threat Prevention Software Blades in your environment and create an effective Rule Base. From SmartEvent, you have an option to directly update the Rule Base.
You can add more rules that prevent or detect specified protections or have different tracking settings.

**Exception Rules**

When necessary, you can add an **exception** directly to a rule. An exception lets you set a protection or protections to either detect or prevent for a specified protected scope. For example, if you want to prevent specified protections for a specific user in a rule with a profile that only detects protections. Another example, if you want to detect all protections in an R and D lab network in a rule with a prevent profile.

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.

<table>
<thead>
<tr>
<th>No</th>
<th>Name</th>
<th>Protected Scope</th>
<th>Protection</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Prevent_Profile</td>
<td>Any</td>
<td>n/a</td>
<td>Prevent_Profile</td>
<td>Log</td>
<td>All</td>
</tr>
<tr>
<td>E-1.1</td>
<td>Corporate_rnd_net</td>
<td>Adware.Win32.Agent.AX</td>
<td>Detect</td>
<td>Log</td>
<td></td>
<td>All</td>
</tr>
<tr>
<td>2</td>
<td>Detect_Profile</td>
<td>Any</td>
<td>n/a</td>
<td>Detect_Profile</td>
<td>Log</td>
<td>All</td>
</tr>
<tr>
<td>E-2.1</td>
<td>Joan_Adams_Role</td>
<td>Trojan-Downloader.Win32.Worm.Win32_Soglued</td>
<td>Prevent</td>
<td>Log</td>
<td></td>
<td>All</td>
</tr>
</tbody>
</table>

**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. Click **Install Policy** to install the Anti-Bot, Threat Emulation, and Anti-Virus policy (see "Installing the Policy" on page 34).

**Copying an Exception to an Exception Group**

You can copy an exception you have created to be a part of an existing exception group or multiple groups. If necessary, you can create a new group with this option.
To copy an exception to an exception group:
1. In the Policy pane, select the exception rule in the Rule Base.
2. Select Actions > Copy to Group.
   The Select Exception Group window opens.
3. Select the group or groups from the list or click New Group to create a new group.
4. Click OK.

Converting Exceptions into an Exception Group
You can select multiple exceptions in the Rule Base and create an exception group. The exceptions can be from different rules. When you convert exceptions into a group, they are removed from the Rule Base as individual exceptions and exist only as a group.

To create an exception group from multiple exceptions:
1. In the Policy pane, select the exception rules in the Rule Base.
2. Select Actions > Convert to Group.
   The New Exception Group window opens.
3. Enter a name and comment (optional).
4. Click OK.

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 58) 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
Anti-Bot, Threat Emulation, and Anti-Virus 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 Recommended 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 column shows the Anti-Bot, Threat Emulation, and Anti-Virus protections that you choose to include.

- 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. Put your mouse in the Protection column and click the plus sign to open the Protection viewer. For each protection, the viewer shows a short description, malware family, type and severity level.
2. To add a protection to the exception, click the checkbox in the Available list.
3. To see the details of an item without adding it to the rule, click the name of the Available item.
4. To see all malwares in a risk level, select the level from the Risk field in the toolbar.
5. Click OK.

**To search for a malware in the Protection viewer:**

1. Put your mouse in the Protection column and click the plus sign to open the Protection viewer.
2. Enter the malware name in the search box. The results show in the Available list.

**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 ("Profiles Pane" on page 65).
- 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.

**Track**

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

- **Alert** - Logs the event and executes a command, such as show a popup window, send an email alert, or run a user-defined script as defined in Policy > Global Properties > Log and Alert > Alerts.
- **Log** - Records event details in SmartView Tracker. This option is useful for getting general information on network traffic.
- **None** - Does not record the event.
• **Packet capture** - Allows the packets relevant to the connection to be captured for analysis at a later time. The packet capture can be viewed from the event in SmartView Tracker ("Viewing Packet Capture Data" on page 103). This can be configured only for rules (not rule exceptions). To configure packet capture, select any tracking action other than None and then select **Packet capture**.

**Install On**

Choose which gateways the rule will be installed on. The default is All (all gateways that have Anti-Bot, Threat Emulation, and Anti-Virus 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.

**Threat Prevention and UserCheck**

For more about using UserCheck objects and settings, see the UserCheck chapters in the *R77 Data Loss Prevention Administration Guide* [http://supportcontent.checkpoint.com/documentation_download?ID=24852]. 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 and until the user verifies that it should be sent. The user decides whether the file or traffic should be allowed or not. The decision itself is logged in SmartView Tracker under the User Actions category.</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 in SmartView Tracker and is available for your review and analysis in SmartReporter and SmartEvent.</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>Company Policy Software Blade Ask</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>Cancel Page Anti-Malware</td>
<td>Cancel</td>
<td>Shows after a user gets an Inform or Ask message and clicks Cancel.</td>
</tr>
</tbody>
</table>

**Ask** and **Inform** pages include a **Cancel** button that users can click to cancel the request.

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

### Configuring the Security Gateway for UserCheck

Enable or disable UserCheck directly on the Security Gateway. The **Gateways** page in the Software Blade tab shows the Security Gateways that use that Software Blade. Make sure the UserCheck is enabled on each Security Gateway in the network. 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.

When you configure the Main URL of the UserCheck portal, if it is set to an external interface, the **Accessibility** option must be set to one of these:

- **Through all interfaces**
- **According to the firewall Policy**

If users connect to the Security Gateway remotely, make sure that the Security Gateway internal interface (in the **Topology** page) is the same as the Main URL for the UserCheck portal.

If you are using internal encrypted traffic, add a new rule to the Firewall Rule Base. This is a sample rule:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Security Gateway on which UserCheck client is enabled</td>
<td>Any Traffic</td>
<td>UserCheck</td>
<td>Accept</td>
</tr>
</tbody>
</table>

**Note** - When you enable UserCheck on an IP appliance, make sure to set the Voyager management application port to a port other than 443 or 80.

### To configure UserCheck on a Security Gateway:

1. From the **Network Objects** tree, double-click to Security Gateway. The **Gateway Properties** window opens.
2. From the navigation tree, click UserCheck. The **UserCheck** page opens.
3. Select **Enable UserCheck**.
4. Enter the settings for the UserCheck portal:
   a) In the **Main URL** field, enter the primary URL for the web portal that shows the UserCheck notifications.

   **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.

   b) In **IP Address**, enter the IP address for the portal.

   c) **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.

5. In the **Certificate** area, click **Import** to import a certificate that the portal uses to authenticate to the 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.

6. In the **Accessibility** area, 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. 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.

7. Click **OK**.

8. Install the Policy.

Creating Threat Prevention UserCheck Objects

Create a UserCheck Interaction object from the UserCheck page or Threat Prevention Software Blade profile **Settings**. You can create these objects for Threat Prevention profiles:

- **Block** - Message that is shown for traffic that matches the Prevent action
- **Ask** - Message that is shown for traffic that matches the Ask action

You can write the UserCheck message with formatting buttons, like Bold and bullets, or directly enter HTML code.

To change text input modes:

Right-click a text field and select the option:

- **Switch to Text Mode** - Enter HTML code
- **Switch to HTML Mode** - Enter text with formatting buttons and options
This procedure shows how to create an object from the UserCheck page in the Threat Prevention tab.

**To create a new Threat Prevention UserCheck object:**

1. From the Threat Prevention tab, click UserCheck.
   
   The UserCheck page opens and shows the UserCheck objects for Threat Prevention rules.

2. Click New > New Block or New Ask.
   
   The UserCheck Interaction window opens.

3. Enter a Name.

4. Optional: Click Language and select one or more languages for the message.
   
   The default language for messages is English.

5. Enter the text for the message.
   
   - Title
   - Subtitle
   - Field - Dynamic text such as: Original URL, Source IP address, and so on
   - User Input - Such as: Confirm check box, Report Wrong Category and so on

6. Optional: Click Add logo to add a graphic to the message.
   
   The size of the graphic must be 176 x 52 pixels.

7. Click Preview in browser to see the message in the default Internet browser.

8. You can also configure one or more of these options for UserCheck messages:
   
   - Using a Fallback Action (on page 64)
   - Redirecting to an External Portal (on page 64)
   - Configuring User Interaction (on page 65)

9. Click OK.

**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:

- **Block** - The connection or traffic is blocked and does not enter the internal network
- **Allow** - The connection or traffic is allowed to enter the internal network

**To configure a fallback action for an Ask object:**

1. From the navigation tree, click Fallback Action.
2. Select to Block or Allow 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 Redirect to External Portal.
2. Select 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 **Conditions**.
2. 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.

**Profiles Pane**

The Profiles pane lets you configure profiles. These profiles are used in enforcing rules in the Rule Base.

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>Edit</td>
<td>Modifies an existing profile.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes a profile.</td>
</tr>
<tr>
<td>Search</td>
<td>Search for a profile.</td>
</tr>
<tr>
<td>Actions &gt;Clone</td>
<td>Creates a copy of an existing profile.</td>
</tr>
<tr>
<td>Actions &gt;Where Used</td>
<td>Shows you reference information for the profile.</td>
</tr>
<tr>
<td>Actions &gt;Last Modified</td>
<td>Shows who last modified the selected profile, when and on which client.</td>
</tr>
</tbody>
</table>

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
- **Anti-Bot Settings**
• Anti-Virus Settings
• Threat Emulation Settings
• Indicators 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.

**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.

**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

The system comes with a *Recommended_PROFILE*. It is defined with these parameters and is used in the predefined rule:

• All protections that can identify an attack with a high or medium confidence level and have a medium or lower performance impact are set to **Prevent** mode.
• All protections that can identify an attack with a low confidence level and have a medium or lower performance impact are set to **Detect** mode.

**Creating Profiles**

When you create a profile, you create a new SmartDashboard object. Protections that match one of the confidence levels can be set to **prevent**, **detect** or **inactive** to allow the profile to focus on identifying certain attacks. The profiles can then be used in the Rule Base.

When HTTPS inspection is enabled on the Security Gateway, Threat Emulation and Anti-Virus can analyze the applicable HTTPS traffic.
To create a Threat Prevention profile:
1. In the Threat Prevention tab, select Profiles.
2. Click New.
3. From the New Profile window, configure:
   - General Properties
   - Anti-Bot Settings
   - Anti-Virus Settings
   - Threat Emulation Settings
   - Malware DNS Trap
4. Click OK.
5. Install the Threat Prevention policy.

General Properties
Set the general properties of the profile:
- **Name** - Mandatory, cannot contain spaces or symbols
- **Color** - Optional color for SmartDashboard object mapping
- **Comment** - Optional free text
- **Blade Activation** - Select the Software Blades that this profile defines

Protection Activation
- **High Confidence, Medium Confidence, and Low Confidence** - The default action that Threat Prevention protections do when they are enabled
  - **Ask** - Traffic is blocked until the user confirms that it is allowed
  - **Prevent** - Protections block traffic matching the protection type's definitions
  - **Detect** - Protections allow and track traffic matching the protection type's definitions
  - **Inactive** - Protections are deactivated
- **Performance Impact** - Set the Security Gateway performance impact level when these protections are active

Configuring Anti-Bot Settings

To configure the Anti-Bot settings for a profile:
1. Configure the UserCheck settings:
   - **Prevent** - Select the UserCheck message that opens for a Prevent action.
   - **Ask** - Select the UserCheck message that opens for an Ask action.
2. Configure the Suspicious Mail Detection setting:
   - **Inspect first X (KB) of email messages** - Set the kilobytes for each email that the ThreatSpect engine inspects to check for bot activity.
   - **Note** - The Suspicious Mail Detection feature requires an Anti-Spam license.
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 SmartDashboard) 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 SmartDashboard, double-click the applicable Security Gateway object.
2. In the gateway Properties window, select Topology and then double-click a DMZ interface.
3. In the Interface Properties window, select the Interface leads to DMZ option.

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

You can configure the Anti-Virus profile to enable archive scanning. The Anti-Virus engine unpacks archives and applies proactive heuristics. If you use this feature, it can have an impact on network performance.

Note - The MIME Nesting settings are the same for Anti-Virus and Threat Emulation.

To configure the Anti-Virus settings for a profile:

1. On the Threat Prevention tab, select Profiles and double-click the applicable Profile.
2. Select the UserCheck Messages options:
   - Prevent - Select the UserCheck message that opens for a Prevent action.
   - Ask - Select the UserCheck message that opens for an Ask action.
3. In the Protected Scope section, select an interface type and traffic direction option:
   - 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.
4. Select the applicable Protocols that Anti-Virus scans.
5. Optional: Configure how Anti-Virus inspects SMTP traffic.
   a) Click Configure.
      The Threat Prevention Mail Configuration window opens.
   b) Configure the MIME nesting settings.
      - Maximum MIME nesting is X levels - For emails that contain nested MIME content, set the maximum number of levels that the ThreatSpect engine scans in the email.
      - When nesting level is exceeded block/allow file - If there are more nested levels of MIME content than the configured amount, select to Block or Allow the email file.
6. Select 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
     Click Configure, and in the window that opens, for each file type, select one of the actions:
     - Inspect
     - Deep Scan
     - Bypass
     - Block
     Click OK to exit the File Types Configuration window.

7. Click OK.

8. Click Install Policy.

To enable Archive Scanning:
1. Select Enable Archiving scanning (impacts performance)
2. Click Configure.
3. Set the amount in seconds to Stop processing archive after X seconds. The default is 30 seconds.
4. Set to block or allow the file When maximum time is exceeded. The default is allow.
5. Click OK.
6. Click Install Policy.

Configuring Threat Emulation 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 SmartDashboard) 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 SmartDashboard, double-click the applicable Security Gateway object.
2. In the gateway Properties window, select Topology and then double-click a DMZ interface.
3. In the Interface Properties window, select the Interface leads to DMZ option.

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.

Note - The MIME Nesting settings are the same for Anti-Virus and Threat Emulation.

To configure the Threat Emulation settings for a profile:
1. On the Threat Prevention tab, select Profiles and double-click the applicable Profile.
2. Configure the settings for UserCheck Messages:
   - Prevent - Select the UserCheck message that opens for a Prevent action
- **Ask** - Select the UserCheck message that opens for an **Ask** action

3. In the **Protected Scope** section, select an interface type and traffic direction option:
   - **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.

4. Select the applicable **Protocols** to be emulated.

5. Configure how Threat Emulation does emulation for SMTP traffic.
   a) Click **Configure**.
      The **Threat Prevention Mail Configuration** window opens.
   b) Configure the **MIME Nesting** settings.
      - **Maximum MIME nesting is X levels** - For emails that contain nested MIME content, set the maximum number of levels that the ThreatSpect engine scans in the email.
      - **When nesting level is exceeded block/allow file** - If there are more nested levels of MIME content than the configured amount, select to **Block** or **Allow** the email file.

6. Select the **File Types** to be emulated.

**Configuring the Virtual Environment (Profile)**

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.

The **Environments** section lets you select operating system images for emulation. 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:
- Check Point automatically updates images and adds new ones
- Select the images that are closest to the operating systems for the computers in your organization

**To configure the virtual environment settings for the profile:**

1. From the navigation tree, select **Threat Emulation Settings > Emulation Environment**.
   The **Emulation Environment** page opens.

2. Set the **Analysis Location** setting:
   - 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
3. Set the **Environments** setting:
   - To use the emulation environments recommended by Check Point security analysts, click **Use Check Point recommended emulation environments**
   - To select one or more images that are used for emulation, click **Use the following emulation environments**

**Excluding Emails**

You can enter email addresses that are not included in Threat Emulation protection. SMTP traffic that is sent to or from these addresses is not sent for emulation.

You can also use a wildcard character to exclude more than one email address from a domain.

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 Emulation:**
1. Select **Threat Prevention >Profiles**.
   The **Profiles** pane opens.
2. Right-click the profile and select **Edit**.
   The **General Properties** page of the profile window opens.
3. From the navigation tree, select **Threat Emulation Settings >Excluded Mail Addresses**.
4. In the **Do not scan mails to the following recipients** section, you can enter one or more emails.
   Emails and attachments that are sent to these addresses are not sent for emulation.
5. In the **Do not scan mails from the following senders** section, you can enter one or more emails.
   Emails and attachments that are received from these addresses are not sent for emulation.

**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 then detect compromised clients by checking logs with connection attempts to the false IP address.

At the Security Gateway level, you can configure to use the settings defined for the profiles or a specified IP address that is used by all profiles used on the specific gateway.
To set the Malware DNS Trap parameters for the profile:

- **Activate DNS Trap** - Select to use a Malware DNS Trap to identify compromised clients attempting to access known malicious domains and select which IP address to use:
  - **User-defined trap IP** - Select and enter a user-defined DNS trap IP address
  - **Internal DNS Servers** - Select or add a new internal DNS server to identify the origin of malicious DNS requests

Use these options to work with the internal DNS server list:

- **Add or Edit** - Click to add or edit an internal DNS server to identify the origin of malicious DNS requests.
- **Remove** - Select a DNS server in the list and click Remove to remove it from the list.
- **Search** - Enter the name of a DNS server to search for in the list. Results are shown highlighted.

To set the Malware DNS Trap parameters per gateway:

1. In SmartDashboard, right-click the gateway object and select **Edit**.
2. From the navigation tree, select **Anti-Bot and Anti-Virus**.
3. In the DNS Redirect Mode section, choose one of the options:
   - **According to profile settings** - Use the Malware DNS Trap IP address configured for each profile.
   - **Specific IP** - Configure an IP address to be used by all profiles used by this Security Gateway.
4. Click **OK**.

Configuring Inspection of Links Inside Mail

**Inspection of Links Inside Mail** scans URL links in the body of email messages, subject, or .txt attachments, and checks them against the URL reputation database. The email messages that contain malicious URL links are blocked.

**Inspection of Links Inside Mail** is on by default, and scans incoming mail with Anti-Virus Software Blade and outgoing mail with Anti-Bot Software Blade.

To turn **Inspection of Links Inside Mail** off:

1. From the navigation tree in the **Threat Prevention** tab, select **Protections**.
   - The **Protections** page opens.
2. Right-click on **Anti-Bot** or **Anti-Virus** for **Links Inside Mail**, and select **Inactive on All Profiles**.
   - **Note** - for each Software Blade - **Anti-Bot** and **Anti-Virus**, you must turn the **Links Inside Mail** separately.

To turn **Inspection of Links Inside Mail** on:

1. From the navigation tree in the **Threat Prevention** tab, select **Protections**.
   - The **Protections** page opens.
2. Right-click on **Anti-Bot** or **Anti-Virus** for **Links Inside Mail**, and select one of these -
   - **Prevent on All Profiles**
   - **Detect on All Profiles**
To configure Link Inspection Inside Mail:
1. From the navigation tree in the Threat Prevention tab, select Profiles.
   The Profiles page opens.
2. Select a profile.
3. Click Edit.
4. In the window that opens, select Advanced > Links inside mail.
   The Links inside mail page opens.
5. Configure the Inspect first settings.
   - Inspect first <number>(KB) of email messages
   - Inspect first <number>URLs in email messages
6. Click OK.

Copying Profiles
You can create a copy of a selected profile and then make necessary changes.

To copy a profile:
1. In the Threat Prevention tab, select Profiles.
2. Select the profile you want to copy.
3. Click Actions > Clone.
   The Name field shows the name of the copied profile plus _copy. Rename the profile.
4. Configure:
   - General Properties
   - Anti-Bot Settings
   - Anti-Virus Settings
   - Threat Emulation Settings
   - Malware DNS Trap
5. Click OK.

Deleting Profiles
You can delete a profile (except for the Recommended_Profile profile). But do this carefully, as it can affect Security Gateways, other profiles or SmartDashboard objects.

To delete a profile:
1. In the Threat Prevention tab, select Profiles.
2. Select the profile you want to delete and click X.
   This message is shown: Are you sure you want to delete object <Name of object>?
3. Click Yes.
   If the profile contains references to/from other objects you cannot , another message is shown:
   <profile_name> is used by another object and cannot be deleted.
4. Click Where Used.
   The Object References window opens.
5. For each object that references the profile, there is a value in the Is Removable? column. If the value is Yes, you can safely delete the profile. If not, find the relationship before you decide to delete this profile.

Sites Pane

The Sites pane shows custom sites, categories and groups that you defined. Select an object in the list and click Edit to change its properties. You can use the toolbar buttons to create, look for, and delete objects.

Creating Threat Prevention Sites

You can create a custom site to use in the Threat Prevention Policy. You can enter the URLs manually or use a CSV (comma separated values) file to add many URLs at one time from an external source.

The .csv file syntax is one URL for each line in the text file. When you use the .csv file option, the URLs are imported when you click Finish. If it is necessary to edit the URLs, click the Applications/Site object in the list and click Edit.

To create a site:

1. In the Sites pane, click New > Site.
   The Create a New Site wizard opens.
2. Enter a name for the site.
3. Select one of the options:
   - Sites URLs - To manually enter a URL.
   - Sites URLs from a file (.csv) - To upload a CSV file with URLs.
4. Click Next.
5. Add the URLs to the Site object:
   - Site URLs window - Enter a URL and click Add.
     If you used a regular expression in the URL, click URLs are defined with regular expressions.
     Note - Select the URLs are defined as Regular Expression checkbox only if the application or site URL is entered as a regular expression using the correct syntax ("Regular Expression Syntax" on page 151).
   - Upload a Sites file window - Browse to the CSV file and upload it.
6. Click Next.
   The Finished window opens.
7. Click Finish.
   You can use this custom site in the Threat Prevention Policy.
Creating Threat Prevention Site Groups

You can create a group of sites to use in the Threat Prevention Policy. The group members can include categories, applications and widgets from the Application Database and also custom applications, sites and categories.

To create an application or site group:

1. In the Sites pane, click New >Sites Group. 
   The Applications/sites group window opens.
2. Enter a Name for the group.
3. Click Add.
   The Application viewer opens.
4. Select the categories, applications, widgets, and custom items to add as members to the group.
5. Click OK.
   The selected items are shown in the list of Group members.
6. Click OK.
   The Site Group object is created.
Using Threat Prevention with HTTPS Traffic

In This Section:

HTTPS Inspection ................................................................. 76
HTTP Inspection on Non-Standard Ports .................................. 95

You can use the HTTPS Inspection feature to unencrypt traffic and let Threat Prevention Software Blades give protections against advanced threats, bots, and other malware.

HTTPS Inspection

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

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

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

There are two types of HTTPS inspection:

- **Inbound HTTPS inspection** - To protect internal servers from malicious requests originating from the internet or an external network.
- **Outbound HTTPS inspection** - To protect an organization from malicious traffic being sent by an internal client to a destination outside of the organization.

The Security Gateway acts as an intermediary between the client computer and the secure web site. The Security Gateway behaves as the client with the server and as the server with the client using certificates.

To optimize performance, inbound HTTPS traffic is inspected only if the policy has rules for HTTPS. For example, if the IPS profile does not have HTTP/HTTPS-related protections activated, HTTPS Inspection is not started.

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

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

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

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

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

Configuring Outbound HTTPS Inspection

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

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

You must enable HTTPS inspection on each Security Gateway. From **Security Gateway >HTTPS Inspection >Step 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 as it also used by other Security Management Servers that import the CA certificate to decrypt the file.

After you create an outbound CA certificate, you must export it so it can be distributed to clients. If you do not deploy the generated outbound CA certificate on clients, users will receive SSL error messages in their browsers when connecting to HTTPS sites. You can configure a troubleshooting option that logs such connections ("Troubleshooting" on page 90).

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

**To create an outbound CA certificate:**

1. In SmartDashboard, right-click the Security Gateway object and select **Edit**. The **Gateway Properties** window opens.
2. In the navigation tree, select **HTTPS Inspection**.
3. In the HTTPS Inspection page, click **Create**.
4. Enter the necessary information:
   - **Issued by (DN)** - Enter the domain name of your organization.
   - **Private key password** - Enter the password that is used to encrypt the private key of the CA certificate.
   - **Retype private key password** - Retype the password.
   - **Valid from** - Select the date range for which the CA certificate is valid.
5. Click **OK**.
6. Export and deploy the CA certificate ("Exporting and Deploying the Generated CA" on page 79).

**Exporting a Certificate from the Security Management Server**

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

**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 do standard updates, the generated CA will be in the CA list and they will not receive browser certificate warnings.

To distribute a certificate with a GPO:

1. From the HTTPS Inspection window of the Security Gateway, click Export certificate.
   Or
   From the HTTPS Inspection >Gateways pane in a supported blade, click Export.
2. Save the CA certificate file.
3. Use the Group Policy Management Console ("Deploying Certificates by Using Group Policy" on page 79) 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 by using Active Directory Domain Services and a Group Policy object (GPO). A GPO can contain multiple configuration options, and is applied to all computers that are within the scope of the GPO.

Membership in the local Administrators group, or equivalent, is necessary to complete this procedure.

To deploy a certificate using Group Policy:

1. Open the Group Policy Management Console.
2. Find an existing GPO or create a new GPO to contain the certificate settings. Make sure the GPO is associated with the domain, site, or organization unit whose users you want affected by the policy.
3. Right-click the GPO and select Edit.
   The Group Policy Management Editor opens and shows the current contents of the policy object.

5. Click **Action > Import.**

6. Do the instructions in the **Certificate Import Wizard** to find and import the certificate you exported from SmartDashboard.

7. In the navigation pane, click **Trusted Root Certification Authorities** and repeat steps 5-6 to install a copy of the certificate to that store.

### 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.

**Note** - It is recommended that you 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. This password is only used 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 ("Exporting a Certificate from the Security Management Server" on page 78).

2. In SmartDashboard, right-click a Security Gateway object, select **Edit > HTTPS Inspection > Import**

   Or

   From the **HTTPS Inspection > Gateways** pane of a supported blade, click the arrow next to Create Certificate and select **Import certificate from file**.
   
   The Import Outbound Certificate window opens.


4. Enter the **private key password**.

5. Click **OK**.

6. If the CA certificate was created on another Security Management Server, deploy it to clients ("Exporting and Deploying the Generated CA" on page 79).

### Configuring Inbound HTTPS Inspection

**To enable inbound HTTPS traffic inspection:**

1. Set the Security Gateway for HTTPS Inspection. From **Security Gateway > HTTPS Inspection > Step 3**, select **Enable HTTPS Inspection**.

2. Import server certificates for servers behind the organization Security Gateways ("Server Certificates" on page 81).
3. Generate an HTTPS inspection policy. Define relevant rules in the HTTPS inspection Rule Base ("The HTTPS Inspection Policy" on page 82).
4. Configure the relevant server certificate in the HTTPS inspection Rule Base ("Certificate" on page 85).

**Server Certificates**

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 seamless HTTPS inspection, the Security Gateway must use the original server certificate and private key.

To enable inbound HTTPS inspection:

1. Add the server certificates to the Security Gateway. This creates a server certificate object ("Adding a Server Certificate" on page 81).
2. Add the server certificate object to the Certificate column in the HTTPS Inspection Policy, to enforce it in rules ("Certificate" on page 85).

The Server Certificates window in SmartDashboard has these options:

- **Add** - Import a new server certificate. Enter a name for the server certificate, optional comment and import the P12 certificate file.
- **Delete** - Delete a previously added server certificate. This option does not delete the server certificate option. It only removes it from the Server Certificate list.
- **Search** - Enter a key word to search for a server certificate in the list.

**Adding a Server Certificate**

When you import a server certificate, enter the same password that was entered to protect the private key of the certificate on the server. The Security Gateway uses this certificate and the private key for SSL connections to the internal servers.

After you import a server certificate (with a P12 file extension) to the Security Gateway, make sure you add the object to the HTTPS Inspection Policy.

Do this procedure for all servers that receive connection requests from clients outside of the organization.

**To add a server certificate:**

1. In SmartDashboard, open HTTPS Inspection >Server Certificates.
2. Click Add.
   
   The Import Certificate window opens.
3. Enter a Certificate name and a Description (optional).
5. Enter the Private key password.
6. Click OK.

The Successful Import window opens the first time you import a server certificate. It shows you where to add the object in the HTTPS Inspection Rule Base. Click Don't show this again if you do not want to see the window each time you import a server certificate and Close.
The HTTPS Inspection Policy

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

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

- Application Control
- URL Filtering
- IPS
- DLP
- Threat Prevention

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

To access the HTTPS inspection Rule Base:

In SmartDashboard, open the Policy page from the specified blade tab:

- For Application Control and URL Filtering, Anti-Bot, Anti-Virus, and IPS - Select Advanced > HTTPS Inspection > Policy.
- For DLP - Select Additional Settings > HTTPS Inspection > Policy.

Predefined Rule

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

Parts of the Rule

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

Number (No.)

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

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

Name

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

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

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

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

Put your mouse in the column and a plus sign shows. Click the plus sign to open the list of network objects and select one or multiple sources. The source can be an Access Role object, which you can define when Identity Awareness is enabled.

**Destination**

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

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

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

**Services**

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

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

**Site Category**

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

⚠️ **Important** -

- A valid URL Filtering blade contract and license are necessary on the relevant Security Gateways to use the Site Category column.
- To perform categorization correctly, a single connection to a site must be inspected in some cases regardless of the HTTPS inspection policy. This maps the IP address of a site to the relevant domain name.

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

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

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

- To filter the Available list by categories or custom-defined sites, click the specified button in the toolbar of the viewer. The Available list opens in the left column and then you can add items to the rule.
To add a category object to the rule, click the checkbox in the Available list.

To see the details of category without adding it to the rule, click the name of the item in the Available list.

You can only select a category to add to the rule from the Available list.

If a category is already in a rule, it will not show in the Category viewer.

If you know the name of a category, you can search for it. The results will show in the Available list.

You can add a new host site with the New button.

**Adding a New Host Site**

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

To create a new host site:

1. Click the plus icon in the Site Category column.
2. In the Category viewer, select **New**.
   The **Hosts/Sites** window opens.
3. Enter a name for the host site.
4. Set a color for the host site icon (optional).
5. Enter a comment for the host site (optional).
6. In **Hosts List**, enter a valid URL and click **Add**.
7. If you used a regular expression ("Regular Expression Syntax" on page 151) in the URL, click **Hosts are defined as regular expressions**.
8. Click **OK**.
   The new host site is added to the **Selected** list and can be added to the Rule Base.

**Action**

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

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

**Track**

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

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

**Blade**

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

- Anti-Bot
- Anti-Virus
- Application Control
- Data Loss Prevention
- IPS
- URL Filtering

⚠️ **Important** - The blade options you see are based on the blade contracts and licenses in your organization.

**Install On**

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

**Certificate**

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

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

**Bypassing HTTPS Inspection 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 the HTTPS Inspection >Policy pane, select **Bypass HTTPS Inspection of traffic to well known software update services (list is dynamically updated)**. This option is selected by default.
2. Click **list** to see the list of approved domain names.

**Enhanced HTTPS Inspection Bypass**

Enhanced HTTPS Inspection Bypass lets the gateway bypass traffic to servers that require client certificate authentication and bypass non-browser applications.

This feature is supported on R77.30 and higher gateways.

To enable enhanced HTTPS inspection:

1. In the $FWDIR/boot/modules/fwkern.conf file on the gateway, add:
   ```
   enhanced_ssl_inspection=1
   ```
2. Reboot.

You can configure this feature without changing the configuration file, but it does not survive reboot:

In **expert mode**, run:
```bash
fw ctl set int enhanced_ssl_inspection 1
```

**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. You can also search, add and remove Security Gateways from here.

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

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

If the Security Management Server managing 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 ("Exporting a Certificate from the Security Management Server" on page 78) 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 to be installed. The notification in SmartDashboard shows as a pop-up notification or in the **Trusted CAs** window in the Automatic Updates section. After you install the update, make sure to install the policy. You can choose to disable the automatic update option and manually update the Trusted CA list.
If the Security Gateway receives a non-trusted server certificate from a site, by default the user gets a self-signed certificate and not the generated certificate. A page notifies the user that there is a problem with the website security certificate, but lets the user continue to the website.

You can change the default setting to block untrusted server certificates ("Server Validation" on page 88).


**Automatically Updating the Trusted CA List and Certificate Blacklist**

Updates for the trusted CA list and Certificate Blacklist ("Certificate Blacklisting" on page 89) will be published from time to time on the Check Point web site. They are automatically downloaded to the Security Management Server by default. When you are sent a notification that there is an update available, install it and do the procedure. The first notification is shown in a popup balloon once and then in the notification line under HTTPS Inspection > Trusted CAs. You can disable automatic updates if necessary.

**To update the Trusted CA list and Certificate Blacklist:**

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

**To disable automatic updates:**

1. In SmartDashboard, select HTTPS Inspection > Trusted CAs.
2. In the Automatic Updates section, clear the Notify when a Trusted CA and Blacklist update file is available for installation checkbox.

**Manually Updating a Trusted CA**

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

**To export a CA certificate to add to the Trusted CAs list:**

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

7. In Firefox, export the certificate.

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

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

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

**HTTPS Validation**

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

**Untrusted server certificate**
When selected, traffic from a site with an untrusted server certificate is immediately dropped. The user gets an error page that states that the browser cannot display the webpage.

When cleared, a self-signed certificate shows on the client machine when there is traffic from an untrusted server. The user is notified that there is a problem with the website's security certificate, but lets the user continue to the website (default).

**Revoked server certificate (validate CRL)**
When selected, the Security Gateway validates that each server site certificate is not in the Certificate Revocation List (CRL) (default).

If the CRL cannot be reached, the certificate is considered trusted (this is the default configuration). An HTTPS Inspection log is issued that indicates that the CRL could not be reached. This setting can be changed with GuiDBedit. Select Other >SSL Inspection >general_confs_obj and change the attribute drop_if_crl_cannot_be_reached from false to true.

To validate the CRL, the Security Gateway must have access to the internet. For example, if a proxy server is used in the organizational environment, you must configure the proxy for the Security Gateway.
To configure the proxy:
1. From the Firewall tab, double-click the Security Gateway that requires proxy configuration.
2. Select Topology >Proxy.
3. Select Use custom proxy settings for this network object and Use proxy server and enter the proxy IP address.
4. Optionally, you can use the default proxy settings.
5. Click OK.

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

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

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

Track validation errors
Choose if the server validation traffic is logged in SmartView Tracker or if it triggers other notifications. The options include:
- None - Does not record the event.
- Log - Records the event details in SmartView Tracker
- Alert - Logs the event and executes a command, such as shows a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in Policy >Global Properties >Log and Alert >Alert Commands
- Mail - Sends an email to the administrator, or runs the mail alert script defined in Policy >Global Properties >Log and Alert >Alert Commands
- SNMP Trap - Sends an SNMP alert to the SNMP GUI, or runs the script defined in Policy >Global Properties >Log and Alert >Alert Commands
- User Defined Alert - Sends one of three possible customized alerts. The alerts are defined by the scripts specified in Policy >Global Properties >Log and Alert >Alert Commands

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

Certificate Blacklisting
You can create a list of certificates that are blocked. Traffic from servers using the certificates in the blacklist will be dropped. If a certificate in the blacklist is also in the Trusted CAs list, the blacklist setting overrides the Trusted CAs list.
- Add - Lets you add a certificate. Enter the certificate serial number (in hexadecimal format HH:HH) and a comment that describes the certificate.
- Edit - Lets you change a certificate in the blacklist.
- **Remove** - Lets you delete a certificate in the blacklist.
- **Search** - Lets you search for a certificate in the blacklist.
- **Track dropped traffic**
  Choose if the dropped traffic is logged in SmartView Tracker or if it triggers other notifications. The options include:
  - **None** - Does not record the event.
  - **Log** - Records the event details in SmartView Tracker
  - **Alert** - Logs the event and executes a command, such as shows a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in **Policy > Global Properties > Log and Alert > Alert Commands**
  - **Mail** - Sends an email to the administrator, or runs the mail alert script defined in **Policy > Global Properties > Log and Alert > Alert Commands**
  - **SNMP Trap** - Sends an SNMP alert to the SNMP GUI, or runs the script defined in **Policy > Global Properties > Log and Alert > Alert Commands**
  - **User Defined Alert** - Sends one of three possible customized alerts. The alerts are defined by the scripts specified in **Policy > Global Properties > Log and Alert > Alert Commands**

**Troubleshooting**

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

- The generated CA was not deployed on clients ("Exporting and Deploying the Generated CA" on page 79).
- The DN in the certificate does not match the actual URL (for example, when you browse to https://www.gmail.com, the DN in the certificate states mail.google.com).
- Applications (such as Firefox and anti-viruses) that use an internal trusted CA list (other than Windows). Adding the CA certificate to the Windows repository does not solve the problem.

The option in the HTTPS Validation pane:

**Log connections of clients that have not installed the CA certificate**

- When selected, logs are recorded for secure connections between a client and server with no traffic in SmartView Tracker (default). Logs are recorded only when a server certificate is trusted by the Security Gateway. If the server certificate is untrusted, a self-signed certificate is created and always results in a log labeled as "Client has not installed CA certificate".
- When cleared, logs are not recorded for secure connections without traffic that can be caused by not installing the CA certificate on clients or one of the above mentioned reasons.

**HTTP/HTTPS Proxy**

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

- One connection between the client in the organization and the proxy.
- One connection between the proxy and the actual destination.

**Proxy Modes**

Two proxy modes are supported:

- **Transparent** - All HTTP traffic on specified ports and interfaces is intercepted and sent to a proxy. No configuration is required on the clients.
- **Non Transparent** - All HTTP/HTTPS traffic on specified ports and interfaces directed to the gateway is sent to a proxy. Configuration of the proxy address and port is required on client machines.

**Access Control**

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

- **All Internal Interfaces** - HTTP/HTTPS traffic from all internal interfaces is forwarded by proxy.
- **Specific Interfaces** - HTTP/HTTPS traffic from interfaces specified in the list is forwarded by proxy.

**Ports**

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

**Advanced**

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

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

**Logging**

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

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

1. From the **General Properties** window of a Security Gateway object, select **HTTP/HTTPS Proxy** from the tree.
2. Select **Use this gateway as a HTTP/HTTPS Proxy**.
3. Select the **Transparent** or **Non Transparent** proxy mode.
   - **Note** - If you select **Non Transparent** mode, make sure to configure the clients to work with the proxy.
4. Select to forward HTTP requests from one of these options:
   - **All Internal Interfaces**
   - **Specific Interfaces** - Click the plus sign to add specified interfaces or the minus sign to remove an interface.
5. To enter more ports on which to forward traffic, select **Add**.
6. To include the actual source IP address in the HTTP header, select Advanced > X-Forward-For header (original client source IP address). The X-Forward-For header must be configured if traffic will be forwarded to Identity Awareness Security Gateways that require this information for user identification.

7. Click OK.

Security Gateway Portals

The Security Gateway runs a number of web-based portals over HTTPS:

- Mobile web access portal
- SecurePlatform WebUI
- Gaia WebUI
- Identity Awareness (Captive Portal)
- DLP portal
- SSL Network Extender portal
- UserCheck portal
- Endpoint Security portals (CCC)

All of these portals can resolve HTTPS hosts to IPv4 and IPv6 addresses over port 443.

These portals (and HTTPS inspection) support the latest versions of the TLS protocol. In addition to SSLv3 and TLS 1.0 (RFC 2246), the Security Gateway supports:

- TLS 1.1 (RFC 4346)
- TLS 1.2 (RFC 5246)

Support for TLS 1.1 and TLS 1.2 is enabled by default but can be disabled in SmartDashboard (for web-based portals) or GuiDBedit (for HTTPS Inspection).

**To configure TLS protocol support for portals:**

1. In SmartDashboard, open Global Properties > SmartDashboard Customization.
2. In the Advanced Configuration section, click Configure. The Advanced Configuration window opens.
3. On the Portal Properties page, set minimum and maximum versions for SSL and TLS protocols.

**To Configure TLS Protocol Support for HTTPS inspection:**

1. In GuiDBedit, on the Tables tab, select Other > ssl_inspection.
2. In the Objects column, select general_confs_obj.
3. In the Fields column, select the minimum and maximum TLS version values in these fields:
   - ssl_max_ver (default = TLS 1.2)
   - ssl_min_ver (default = SSLv3)
HTTPS Inspection in SmartView Tracker

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

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

To open SmartView Tracker:
- From the SmartDashboard toolbar, click SmartConsole > SmartView Tracker.
- With SmartDashboard active, press Control + Shift + T.

HTTPS Inspection Queries

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

- **All** - Shows all HTTPS traffic that matched the HTTPS Inspection policy and was configured to be logged.
- **HTTPS Validations** - Shows traffic with connection problems. The Action values are rejected or detected. The actions are determined by the SSL validation settings ("HTTPS Validation" on page 88) for HTTPS Inspection.

HTTPS Validation values are:
  - Untrusted Server Certificate
  - Server Certificate Expired
  - Revoked Certificate or Invalid CRL
  - SSL Protocol Error (general SSL protocol problems)

Blade Queries

When applying HTTPS Inspection to a specified blade:

- There is an HTTPS Inspection predefined query for each of the blades that can operate with HTTPS Inspection. The query shows all traffic of the specified blade that passed through HTTPS inspection.
- The log in the blade queries includes an HTTP Inspection field. The field value can be inspect or bypass. If the traffic did not go through HTTPS inspection, the field does not show in the log.

Permissions for HTTPS Logs

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

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

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

To open SmartEvent:
- From the SmartDashboard toolbar, click SmartConsole > SmartEvent.
- With SmartDashboard active, press Control + Shift + A.

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

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

- HTTPS Inspection queries
- Blade queries

**HTTPS Inspection Queries**

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

**Blade Queries**

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

**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 Anti-Bot and Anti-Virus 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 **Threat Prevention** tab >**Advanced** pane.
Monitoring Threat Prevention with SmartEvent

In This Section:

- Event Analysis in SmartEvent or SmartEvent Intro ................................................................. 96
- Viewing Information in SmartEvent ................................................................................................ 96
- Anti-Bot and Anti-Virus Reports ..................................................................................................... 98
- Viewing Information in SmartEvent Intro ....................................................................................... 99

Event Analysis in SmartEvent or SmartEvent Intro

SmartEvent and SmartEvent Intro supply 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 Anti-Bot, Threat Emulation and Anti-Virus 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

SmartEvent shows information for all Software Blades in the environment. SmartEvent Intro shows information for one SmartEvent Intro mode. If you select Threat Prevention as the SmartEvent Intro Mode, it shows the Threat Prevention information.

To use SmartEvent or SmartEvent Intro, you must enable it on the Security Management Server or on a dedicated machine. See either:

- R77 SmartEvent Administration Guide
  http://supportcontent.checkpoint.com/solutions?id=sk104859
- R77 SmartEvent Intro Administration Guide
  http://supportcontent.checkpoint.com/solutions?id=sk104859

Viewing Information in SmartEvent

To open SmartEvent do one of these:

- Click Start > Check Point > SmartEvent.
- From the Threat Prevention tab > Navigation Tree > Analyze & Report link.
- From the Threat Prevention tab > Overview > Statistics > Graphs link.
From the SmartDashboard toolbar of any SmartConsole application, select **Window > SmartEvent** or press Control +Shift +A.

When SmartEvent opens, go to **Events > Predefined > Threat Prevention** to use the predefined queries for the Software Blades.

- **Most Important** - Shows Threat Prevention events that are **Critical and High** severity
- **All Events** - Shows all Threat Prevention events grouped by source, includes all prevented and detected events
- **By Activity** - Shows all Threat Prevention events grouped by malware activity
- **Important Anti-Bot** - Shows the Anti-Bot events that are **Critical and High** severity
- **Important Anti-Virus** - Shows the Anti-Virus events that are **Critical and High** severity
- **Important Threat Emulation** - Shows the Threat Emulation events that are **Critical and High** severity
- **More > By Protection Name** - Shows all Threat Prevention events grouped by protection name
- **More > By Protection Type** - Shows all Threat Prevention events grouped by protection type
- **More > Blocked Incidents** - Shows all Threat Prevention blocked incidents
- **More > All Threat Emulation** - Shows all Threat Emulation events

### Updating the Anti-Bot and Anti-Virus Rule Base

In some cases, after evaluating an event, it may be necessary to update a rule or rule exception in the SmartDashboard Rule Base. You can do this directly from within SmartEvent.

#### To update a rule in the Anti-Bot and Anti-Virus Rule Base:

1. Right-click the event or from within event details select the **Anti-Virus** or **Anti-Bot** menu.
2. Select **Go to Rule**.
   
   SmartDashboard opens showing the related rule in the Anti-Bot and Anti-Virus Rule Base.
3. Make related changes.
4. Click **Install Policy** to install the Anti-Bot, Threat Emulation, and Anti-Virus policy (see "Installing the Policy" on page 34).

#### To update a rule exception in the Anti-Bot and Anti-Virus Rule Base:

1. Right-click the event or from within the event details, select the **Anti-Virus** or **Anti-Bot** menu.
2. Select **Add Exception to the Rule**.
   
   SmartDashboard opens and shows an **Add Exception** window in the Threat Prevention Rule Base. These details are shown:
   - **Protection** - The name of the protection. Details are taken from the ThreatCloud repository or, if there is no connectivity, from the log.
   - **Scope** - The scope is taken from the log. If there is no related host object, an object is created automatically after you click **OK**. Click the plus sign to add additional objects.
   - **Install On** - Shows **All** by default. You can use the plus sign to add gateways.
3. Select an **Exception Scope** option:
   - **Apply Exception to rule number X** - If you want the **exception** to apply only to the related rule.
   - **Apply Exception to all rules** - If you want the **exception** to apply to all rules. The exception is added to the **Exception Groups >Global Exceptions** pane.

4. Click **OK**.
   The exception is added to the Rule Base. The **Action** is set to **Detect** by default. Change if necessary.

5. Click **Install Policy** to install the Anti-Bot, Threat Emulation, and Anti-Virus policy (see "Installing the Policy" on page 34).

**Accessing the Threat Wiki**
You can open the Threat Wiki from within SmartEvent to get more information about a specified protection.

**To open the Threat Wiki do one of these:**
- Right-click an event and select Go to Threat Wiki.
- Click the malware protection link in the event log.
- Select Go to Threat Wiki from the Anti-Virus or Anti-Bot tab in the event log.

**Anti-Bot and Anti-Virus Reports**
Daily, weekly, and monthly reports of the events recorded by SmartEvent are configured and stored on the **Reports** tab. These reports show a high-level summary of the event patterns occurring on your network.
Upon creation, reports can be automatically emailed to predefined addresses, eliminating the need to open SmartEvent to learn of the system's status. You can also choose to save them as PDFs or view them in a browser.

Viewing Information in SmartEvent Intro

To open SmartEvent Intro:

1. From the SmartDashboard menu bar, select SmartConsole > SmartEvent Intro or press Control + Shift + E.
2. From SmartEvent Intro Mode, select Threat Prevention.

All of the information in SmartEvent Intro is based on Anti-Bot, Threat Emulation and Anti-Virus events. See the different tabs for detailed information.

The SmartEvent Intro Overview Page

The Overview page shows a quick understandable overview of the Anti-Bot and Anti-Virus traffic in your environment. Double-click on data in any of the sections in the Overview tab to open the associated list of events to investigate issues down to the individual event level.

The Overview page includes these panes:

- Timeline View
- Anti-Bot & Anti-Virus
- Top Source/Destination Countries of Anti-Bot & Anti-Virus
- Top Malwares by Event Count
Monitoring Threat Prevention with SmartEvent

- Top Malicious Activities by Event Count
- Status

Anti-Bot and Anti-Virus Event Queries
See detailed event queries in the Events tab.
- Most Important - Shows Threat Prevention events that are Critical and High severity
- All Events - Shows all Threat Prevention events grouped by source, includes all prevented and detected events
- By Activity - Shows all Threat Prevention events grouped by malware activity
- Important Anti-Bot - Shows the Anti-Bot events that are Critical and High severity
- Important Anti-Virus - Shows the Anti-Virus events that are Critical and High severity
- Important Threat Emulation - Shows the Threat Emulation events that are Critical and High severity
- More >By Protection Name - Shows all Threat Prevention events grouped by protection name
- More >By Protection Type - Shows all Threat Prevention events grouped by protection type
- More >Blocked Incidents - Shows all Threat Prevention blocked incidents
- More >All Threat Emulation - Shows all Threat Emulation events

See the R77 SmartEvent Intro Administration Guide
Monitoring Threat Prevention with SmartView Tracker

**In This Section:**
- Log Sessions .................................................................................................................................. 101
- Threat Prevention Logs ..................................................................................................................... 102
- Viewing Logs .................................................................................................................................... 102
- Viewing Packet Capture Data ........................................................................................................... 103
- Using Predefined Queries ................................................................................................................. 103

**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 SmartView Tracker.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic</td>
<td>4059</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://bws.shopathome.com/RequestHandler.ashx">http://bws.shopathome.com/RequestHandler.ashx</a></td>
</tr>
<tr>
<td>Resource</td>
<td><a href="http://admob.com">http://admob.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://admob.com?language=en">http://admob.com?language=en</a></td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Description</td>
<td>Destination URL has bad reputation</td>
</tr>
<tr>
<td>Source OS</td>
<td>Windows</td>
</tr>
<tr>
<td>Proxyed Source IP</td>
<td>153.70.104.64</td>
</tr>
<tr>
<td>Client Type</td>
<td>Other: SelectRebates</td>
</tr>
<tr>
<td>Suppressed Logs</td>
<td>22</td>
</tr>
<tr>
<td>Sent Bytes</td>
<td>1810</td>
</tr>
<tr>
<td>Received Bytes</td>
<td>1624</td>
</tr>
<tr>
<td>Destination Country</td>
<td>Taiwan</td>
</tr>
<tr>
<td>Malware Family</td>
<td>FraudLoad</td>
</tr>
<tr>
<td>Malware Activity</td>
<td>Communication with Command &amp; Control</td>
</tr>
<tr>
<td>Information</td>
<td>Source OS version: XP SP1, 2000 SF3 confidence_level: 67</td>
</tr>
</tbody>
</table>

In SmartEvent the number of connections during the session is in the **Total Connections** field of the Event Details.

Session duration for all connections that are prevented or detected in the Rule Base, is by default 10 hours. You can change this in SmartDashboard from the Threat Prevention tab > Advanced > Engine Settings > Session Timeout.
Threat Prevention Logs

Logs from Anti-Bot, Threat Emulation and Anti-Virus are shown in SmartView Tracker. A log is generated if you set the Track option in a Rule Base rule to Log.

Viewing Logs

To open SmartView Tracker:
- From the Threat Prevention tab > Navigation Tree > Track Logs link
- From the SmartDashboard menu bar, select SmartConsole > SmartView Tracker

Updating the Anti-Bot and Anti-Virus Rule Base

In some cases, after evaluating a log, it may be necessary to update a rule or rule exception in the SmartDashboard Rule Base. You can do this directly from within SmartView Tracker.

To update a rule in the Anti-Bot and Anti-Virus Rule Base:
1. Right-click the log entry.
2. Select Go to Rule.
   SmartDashboard opens showing the related rule in the Anti-Bot and Anti-Virus Rule Base.
3. Make related changes.
4. Click Install Policy to install the Anti-Bot, Threat Emulation, and Anti-Virus policy (see "Installing the Policy" on page 34).

To update a rule exception in the Anti-Bot and Anti-Virus Rule Base:
1. Right-click the log entry.
2. Select Add Exception to the Rule.
   SmartDashboard opens and shows an Add Exception window in the Threat Prevention Rule Base. These details are shown:
   - Protection - The name of the protection. Details are taken from the ThreatCloud repository or, if there is no connectivity, from the log.
   - Scope - The scope is taken from the log. If there is no related host object, an object is created automatically after you click OK. Click the plus sign to add additional objects.
   - Install On - Shows All by default. You can use the plus sign to add gateways.
3. Select an Exception Scope option:
   - Apply Exception to rule number X - If you want the exception to apply only to the related rule.
   - Apply Exception to all rules - If you want the exception to apply to all rules. The exception is added to the Exception Groups > Global Exceptions pane.
4. Click OK.
   The exception is added to the Rule Base. The Action is set to Detect by default. Change if necessary.
5. Click Install Policy to install the Anti-Bot, Threat Emulation, and Anti-Virus policy (see "Installing the Policy" on page 34).
Accessing the Threat Wiki

You can open the Threat Wiki from within SmartView Tracker to get more information about a specified protection.

To open the Threat Wiki:

- Click the malware protection link in the Protection Name field of a log record.

Viewing Packet Capture Data

If you set a rule with the Packet Capture track option, you can see the captures in SmartView Tracker.

To see packet captures in SmartView Tracker:

1. Locate the log entry with the packet capture.
2. Right-click the entry and select View packet capture.
3. Select Internal Viewer and click OK.

   The packet is shown in the Viewer Output window.

   You can also use a third-party capture application by selecting Choose Program and entering the application in the Program Name field.

Using Predefined Queries

There are multiple predefined queries in Network and Endpoint Queries > Predefined > Network Security Blades > Anti-Bot & Anti-Virus. You can filter the queries to focus on logs of interest.

- All - Shows all Anti-Bot and Anti-Virus traffic, including all prevented and detected connections
- Anti-Bot - Shows Anti-Bot traffic (prevented and detected connections)
- Anti-Virus - Shows Anti-Virus traffic (prevented and detected connections)
- Blocked Incidents - Shows all Anti-Bot and Anti-Virus blocked (prevented) traffic
- Threat Emulation - Shows all traffic that are sent to ThreatCloud or Emulation appliance for emulation
- Malware Detected - Shows files that Threat Emulation identified as malware
- System - Shows updates and installed policies for Threat Emulation
Configuring Advanced Threat Prevention Settings

In This Section:

- Engine Settings .............................................................................................................. 104
- Configuring Whitelist Files ............................................................................................. 106
- Threat Indicators Settings .............................................................................................. 107
- Threat Emulation Settings .............................................................................................. 112
- Using Anti-Bot and Anti-Virus with VSX ........................................................................ 121
- Threat Prevention CLI Commands .................................................................................. 122
- Troubleshooting Threat Emulation .................................................................................. 128

This chapter describes settings that you can configure in the Threat Prevention tab > Advanced pane. These settings apply globally for all gateways enabled with Threat Prevention Software Blades.

Engine Settings

On the Advanced > Engine Settings pane, configure settings related to Threat Prevention inspection engines, the Check Point Online Web Service (ThreatCloud repository), and advanced Anti-Bot and Threat Emulation settings.

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).
Configuring Advanced Threat Prevention Settings

- **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.

Anti-Bot Settings

Emails that are sent to external networks are scanned by the Suspicious Mail engine. Internal emails are not scanned. You can create a list of email addresses or domains that are not inspected by Anti-Bot.

- **Add** - Lets you add an email or domain entry.
- **Edit** - Lets you edit an entry in the list.
- **Remove** - Lets you delete an entry 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 configure the file type actions, go to Threat Prevention > Profiles > Double-click a profile > Threat Emulation Settings > Configure for Process specific file types families.

**To select Threat Emulation file types for the profiles:**

1. From the Threat Emulation Settings section, click **Configure file type support**.
   The File Types Support window opens.
2. Select the file types that are sent for emulation.
   The Emulation supported on column shows the emulation environments that support the file type.
3. Click **OK**.

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 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 adjust the length of a session:
1. 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 change this, click Session Timeout and enter a different value.
2. Click OK.

Configuring Whitelist Files

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.

To add a file to the Whitelist:
1. Select Threat Prevention > Advanced > Whitelist Files.
   The Whitelist Files page opens.
2. Click New.
   The New File Exception window opens.
3. Enter parameters for the new file exception:
   - Name
   - Comment (optional)
   - MD5 signature
   - Select a color (optional) - the default is black
4. Click OK.

To edit attribute of a file from the Whitelist:
1. Select Threat Prevention > Advanced > Whitelist Files.
   The Whitelist Files page opens.
2. Select a file.
3. Click Edit.
4. In the file properties window that opens, make necessary changes.
5. Click OK.

To remove a file from the Whitelist:
1. Select Threat Prevention > Advanced > Whitelist Files.
   The Whitelist Files page opens.
2. Select a file or multiple files.
3. Click Delete.
4. Click Yes to confirm.
**Threat Indicators Settings**

This feature is supported in R77.20 and higher.

Threat Indicators lets you upload *Indicator* (on page 11) files that contain sets of *observables* ("*Observable*" on page 11). These observables are added to the Threat Prevention policy.

**To activate:**

1. Install the R77.20 Add-on. See sk101217
2. If the R77.20 Security Gateway was upgraded from a version earlier than R77, edit these configuration files to add the `include` statement.
   - `$FWDIR/conf/urlrep.eng`: `$include ../amw/ioc/cur/rep/urlrep_ioc.eng`
   - `$FWDIR/conf/av_hash.eng`: `$include ../amw/ioc/cur/md5/av_hash_ioc.eng`
   - `$FWDIR/conf/malware.eng`: `$include ../amw/ioc/cur/sigs/malware_ioc.eng`
3. In a Multi-Domain Security Management environment, you must activate this feature on each domain, after you activate it on the Multi-Domain Server.

**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>TYPE</td>
<td>Type of the observable</td>
<td></td>
<td>Not case sensitive</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>• URL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Domain</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IP Range</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• MD5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mail-subject</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mail-from</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mail-to</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mail-cc</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mail-reply-to</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Advanced Threat Prevention Settings

#### Threat Prevention Administration Guide R77 Versions

<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>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 the observable</td>
<td>• AV</td>
<td>AV - Check Point Anti-Virus Software Blade (default)</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• AB</td>
<td>AB - Check Point Anti-Bot Software Blade</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note - only the Anti-Virus Software Blade can process MD5 observables.</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>
<tr>
<td>IP Range</td>
<td>A range of valid IPv4 addresses, separated by a hyphen: &lt;IP&gt;-&lt;IP&gt;</td>
</tr>
<tr>
<td>MD5</td>
<td>Any valid MD5</td>
</tr>
<tr>
<td>Mail-subject</td>
<td>Any non-empty text string</td>
</tr>
<tr>
<td>Mail-to</td>
<td>Can be one of these:</td>
</tr>
<tr>
<td>Mail-from</td>
<td>• A single email address (Example: <a href="mailto:abc@domain.com">abc@domain.com</a>)</td>
</tr>
<tr>
<td>Mail-cc</td>
<td>• An email domain (Examples: @domain.com or domain.com)</td>
</tr>
<tr>
<td>Mail-reply-to</td>
<td></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
Configuring Indicators in SmartDashboard

Define network objects to hold the Indicator files.

To load Indicators:

1. Select Threat Prevention > Advanced > Indicators.
   The Indicators page opens.

2. Click New.
   The Indicators configuration window opens.

3. Enter a Name.
   Each Indicator must have a unique name.

   The content of each file must be unique. You cannot load duplicate files.

5. Select an action for this Indicator:
   - Ask - Threat Prevention Software Blade asks what to do with the detected observable
Configure Advanced Threat Prevention Settings

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

6. Select a Color.
7. Enter a Comment (optional).
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.

Indicator CLI Commands

You can run these commands on the Security Management Server to manually add indicators to the Threat Prevention policy, or to remove them from the Threat Prevention policy.

load_indicators --add

Description: Add indicators to the Threat Prevention policy.


<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>input files</td>
<td>Adds indicators from one of these:</td>
</tr>
<tr>
<td></td>
<td>• An Indicator file</td>
</tr>
<tr>
<td></td>
<td>• A list of Indicator files, separated by spaces</td>
</tr>
<tr>
<td></td>
<td>• A directory with Indicator files</td>
</tr>
<tr>
<td></td>
<td>• A .zip archive with Indicator files</td>
</tr>
<tr>
<td>Notes</td>
<td>• Use full pathnames or directory names</td>
</tr>
<tr>
<td></td>
<td>• Do not nest directories or archives</td>
</tr>
<tr>
<td></td>
<td>• You can load two files with the same name, but with different contents</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| action       | Assigns one of these actions for detected observables:  
  - *prevent*: blocks the detected observables  
  - *detect*: lets the detected observables go through and creates log entries  
  - *ask*: asks what to do with the detected observables  
  - *inactive*: does nothing |
| name-prefix  | Adds a prefix to the name of the indicator. By default, the name of the indicator is the filename of the input file. If you specify a prefix, the name of the indicator changes to `<prefix>_<indicator name>`.
| comment      | Changes the color coding of the indicator in SmartDashboard. The default is black.  
  **Note**: if you specify an invalid color, the default color is used. |
| color        | Changes the color coding of the indicator in SmartDashboard. The default is black.  
  **Note**: if you specify an invalid color, the default color is used. |
| output file  | Specifies the pathname of an output file with the names of successfully added indicators. If you do not specify this value, `load_indicators.out` is created in the current directory. |
| product      | Specifies the Check Point Software Blade that processes the observables that do not have the *product* specified in the input file. Select one of these:  
  - *AV*: Anti-Virus (default)  
  - *AB*: Anti-Bot  
  **Notes**:  
  - If you do not specify the *product* value, the default value is used  
  - For MD5 observables, the product is always *AV*, regardless of what you specify |
| product.override | Overrides the product for all the observables in the input file, except for MD5. |

**Examples:**

```bash
load_indicators --add -i CIB-20120508-01.csv -a prevent

The CIB-20120508-01.csv Indicator file is loaded. All specified in it observables will be blocked.

load_indicators --add -i CIB-20120508-01.csv CIB-20120508-02.csv CIB-20120508-03.csv -a prevent -n prefix -o my_output.txt

These three indicator files are loaded: CIB-20120508-01.csv, CIB-20120508-02.csv, and CIB-20120508-03.csv. All observables specified in these files will be blocked, the name of the indicator will be prefixed with `prefix_`, and the `my_output.txt` output file will be created in the current directory.

load_indicators --add -i my_indicators_dir -a ask -n prefix123
```
All Indicator files in the `my_indicators_dir` directory are loaded. The observables specified in these files are detected, but as each one arrives, the user will have to decide - to block it or to let it go through.

**load_indicators --delete**

**Description:** Delete indicators from the Threat Prevention policy.

**Syntax:**
```
load_indicators --delete {--indc-files -i <indicator file-names> | --indc-names -i <indicator names> | --list-file -i <file-name> | -all} [-f]
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>--indc-files -i</code>&lt;br&gt;<code>&lt;indicator file-names&gt;</code></td>
<td>Deletes indicators based on the provided indicator file-names:</td>
</tr>
<tr>
<td></td>
<td>• An Indicator file</td>
</tr>
<tr>
<td></td>
<td>• A list of Indicator files, separated by spaces</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - Do not provide filenames with full paths</td>
</tr>
<tr>
<td><code>--indc-names -i</code>&lt;br&gt;<code>&lt;indicator names&gt;</code></td>
<td>Deletes indicators based on the indicator-names:</td>
</tr>
<tr>
<td></td>
<td>• An Indicator name</td>
</tr>
<tr>
<td></td>
<td>• A list of Indicator names, separated by spaces</td>
</tr>
<tr>
<td><code>--list-file -i</code>&lt;br&gt;<code>&lt;file-name&gt;</code></td>
<td>Deletes all loaded indicators listed in the specified output file. See <code>load_indicators --add</code> (on page 110) for information on output files.</td>
</tr>
<tr>
<td><code>-all</code></td>
<td>Deletes all the indicators in the database.</td>
</tr>
<tr>
<td><code>-f</code></td>
<td>Deletes without verification.</td>
</tr>
</tbody>
</table>

**Examples:**
```
load_indicators --delete --list-file -i load_indicators.out

All indicators listed in the `load_indicators.out` file are deleted from the database.
```
```
load_indicators --delete --indc-files -i CIB-20120508-01.csv

All indicators from the `CIB-20120508-01.csv` Indicator file are deleted from the database.
```
```
load_indicators --delete --indc-names -i prefix_CIB-20120508-01 prefix_CIB-20120508-02

Indicators `prefix_CIB-20120508-01` and `prefix_CIB-20120508-02` are deleted from the database.
```
```
load_indicators --delete --all

All indicators are deleted from the database.
```

**Threat Emulation Settings**

**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.
To enable or disable Automatic Updates for Threat Emulation:

1. Select **Threat Prevention >Advanced >Updates**. The **Updates** page opens.
2. Select or clear these settings:
   - **Update Threat Emulation engine**
   - **Update Threat Emulation images**
3. Install the Threat Prevention policy on the applicable Threat Emulation appliances.

**Threat Emulation Engine**

Update packages for the Threat Emulation engine are usually around 10 - 40MB. The default setting is to download the package once a day. We recommend that you configure Threat Emulation to download the package when there is low network activity.

To change the automatic update settings for the Threat Emulation engine:

1. Select **Threat Prevention >Advanced >Updates**. The **Updates** page opens.
2. Make sure that **Update Threat Emulation engine** is selected.
3. Next to the **Update Threat Emulation engine** option, click **Schedule**. The **Scheduled Event Properties** window for the Threat Emulation engine opens.
4. 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.
5. Click **OK** and then install the Threat Prevention policy.

**Threat Emulation Images**

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.

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 change the automatic update settings for Threat Emulation images:

1. Select **Threat Prevention >Advanced >Updates**. The **Updates** page opens.
2. Make sure that **Update Threat Emulation images** is selected.
3. Next to the **Update Threat Emulation image** option, click **Schedule**. The **Scheduled Event Properties** window for the Threat Emulation images opens.
4. 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.
5. Click **OK** and then install the Threat Prevention policy.

Configuring Advanced Profile Settings

**To configure the advanced settings for a Threat Emulation profile:**

1. In the **Threat Prevention** tab, select **Profiles**.
2. Double-click the profile.
3. Configure the Threat Emulation settings for the profile.
4. Click **OK**.
5. Install the Threat Prevention policy.

**File Type Settings**

You can configure the Threat Emulation **Action** and **Emulation Location** for each file type in the Threat Prevention profile.

It is possible to specify "safe" file types that Threat Emulation does not do emulation. File types can be considered safe because they do not normally contain malware threats.

**To configure the file type settings for a profile:**

1. Double-click the Threat Prevention profile.
2. From the navigation tree, select **Threat Emulation Settings**.
3. From the **File Types** section, select **Process specific file types families**.
4. Click **Configure**.
   The **File Types Configuration** window opens.
5. To change the emulation action for a file type, click **Action** and select one of these options:
   - **Inspect** - Threat Emulation opens these files.
   - **Bypass** - Files of this type are considered safe and the Software Blade does not do emulation for them.
6. To change the emulation location for a file type, click **Emulation location** and select one of these options:
   - **According to the gateway** - The **Emulation location** settings that are defined in the **Gateway Properties** window are used for these files
   - **Locally** - Emulation for these file types is done on the Emulation appliance
   - **ThreatCloud** - These file types are sent to the ThreatCloud for emulation
Handling Connections During Emulation

**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.
- For configurations that use Hold mode for SMTP traffic, we recommend that you use an MTA deployment ("Using an MTA" on page 29).

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

**To configure the Threat Emulation Connection Handling Mode:**

1. Double-click the Threat Prevention profile.
2. From the navigation tree, select **Threat Emulation Settings > Advanced**.
3. From the **Emulation Connection Handling Mode** section, select an option:
   - **Background** - Files are sent to destination even if the Threat Emulation analysis is not finished
   - **Hold** - Connections that must have emulation are blocked until the Threat Emulation analysis is finished
   - **Custom** - Select this option and click **Customize** to configure **Background** or **Hold** modes for SMTP and HTTP services

Static Analysis

**Static Analysis** optimizes the file analysis and does 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. We recommend that you disable static analysis only if there is an I/O bottleneck with the ThreatCloud. If you are using an Emulation appliance, and you want to disable static analysis, contact Check Point Technical Support.

**To disable static analysis for the Threat Prevention profile:**

1. Double-click the Threat Prevention profile.
2. From the navigation tree, select **Threat Emulation Settings > Advanced**.
3. From the **Engine settings** section, select **Disable static analysis for filtering files**
4. To enable static analysis, clear **Disable static analysis for filtering files**

Threat Emulation Logs

**To only generate Threat Emulation logs every file that has malware:**

1. Double-click the Threat Prevention profile.
2. From the navigation tree, select **Threat Emulation Settings > Advanced**.
3. From the **Logging** section, clear **Log every file scanned**.
4. To generate logs for each file after emulation is complete, select **Log every file scanned**.

**Configuring MTA Advanced Settings**

The MTA Advanced Settings window lets you configure which interfaces on the Security Gateway are listening for 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
- Maximum amount of free hard drive space that the MTA can use
- 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 emulation as configured in the Fail Mode settings. The Troubleshooting setting lets you receive a log or alert to change the Threat Emulation settings ("Configuring Threat Emulation Settings" on page 69) for the profile and reduce the delay time.

**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 are sent for emulation
   - **All external** - SMTP traffic from the external interfaces are sent for emulation
   - **Use specific** - SMTP traffic from the list of specified interfaces are sent for emulation. 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 amount of free hard drive space that the MTA can use, configure these settings:
   - **% of storage** - Percentage of free hard disk space that the MTA can use
   - **MB** - Total MB of free hard disk space that the MTA can use
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 SmartView Tracker
   - **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 SmartView Tracker), **Alert** (logs the event and sends the configured alert).
8. Click OK.
9. Install the policy.

Disabling the MTA

To disable the MTA:
1. Configure the network to disable the MTA.

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.

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.

Disabling MTA on the Security Gateway

To disable the Security Gateway as an MTA:
1. Double-click the Security Gateway and from the navigation tree select Mail Transfer Agent. The Mail Transfer Agent page opens.
2. Clear Enable as a Mail Transfer Agent.
3. Click OK and then install the policy.

Fine-Tuning the Emulation Appliance

You can change these advanced settings on the Emulation appliance to fine-tune Threat Emulation for your deployment.

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.

Changing the Analysis Location

When you run the Threat Emulation First Time Configuration Wizard you select the location where the emulation analysis is done. 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 ("Configuring the Virtual Environment (Profile)" on page 70).

You can send files that are not supported on the local Emulation appliance to the ThreatCloud for emulation. It is necessary to have a ThreatCloud license to send files 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:
   - Check Point ThreatCloud - Files are sent to the Check Point ThreatCloud for emulation
   - Locally - Select the Security Gateway that does the emulation and of the files
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.

Configuring the Emulation Limits

To prevent too many files that are waiting for emulation, configure these emulation limits settings:

- Maximum file size (up to 100,000 KB)
- 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 ("Configuring MTA Advanced Settings" on page 116).

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

To configure the emulation limits:
1. In the Threat Prevention tab, select Advanced > Engine Settings. The Engine Settings pane opens.
2. From the Threat Emulation Settings section, click Configure settings. The Threat Emulation Settings window opens.
3. Configure the settings for the emulation limits.
4. 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
5. 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. We recommend that you do not change this setting.

To change the size of the local cache:
1. In the Threat Prevention tab, select Advanced > Engine Settings. The Engine Settings pane opens.
2. From the Threat Emulation Settings section, 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.
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, there can be an effect on network and emulation performance. You can configure the settings for these system resources:

- Minimum available hard disk space (If emulation is not done on a file, the Fail Mode settings for Threat Prevention define if a file is allowed or blocked)
- Maximum available RAM that can be used for Virtual Machines
  If you are going 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. From Stop emulation when disk space falls below, configure the minimum percentage of hard disk space that must be available to do emulation.
   The default value is 20%.
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 (Security Gateway or Emulation appliance), and for each Threat Emulation profile ("Configuring the Virtual Environment (Profile)" on page 70). If different images are defined for them, Threat Emulation uses images that are selected in the two places. An image that is selected only for the appliance or for the profile is not used for emulation.

We recommend that you change these settings only if one appliance uses an image and another one does not use it.

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.

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 the Threat Prevention tab, select Advanced > Engine Settings.
   The Engine Settings pane opens.
2. From the Threat Emulation Settings section, click Configure settings.
   The Threat Emulation Settings window opens.
3. Enter the Network and Mask for the IP address for the virtual interface.
4. Click OK and then install the policy.

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 (VS0)
  VSO handles contract validation for all Virtual Systems.
- Can connect to the internet
A Virtual System will try to get updates through the VSX Gateway (VSO). If the VSX Gateway fails, each Virtual System gets the update by connecting to the internet using its proxy settings.

**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) and/or the Virtual Systems:
   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):
   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. Repeat steps 1-2 for all Virtual Systems that use **Anti-Bot** and **Anti-Virus**.

4. Select the Threat Prevention and configure the policies.

5. Install the Threat Prevention policy (and access policy if needed) on the VSX Gateway (VSO) and the relevant Virtual Systems.


### Threat Prevention CLI Commands

You can run commands from the CLI (Command Line Interface) to install Threat Prevention policy and for advanced Threat Emulation management.

**fwm load -p threatprevention**

**Description**: Run this command on the Security Management Server to manually install the Threat Prevention policy on the specified Security Gateways.

**Syntax**: `fwm load -p threatprevention <rulebase> <targets>`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rulebase</td>
<td>Name of the Rule Base</td>
</tr>
<tr>
<td>targets</td>
<td>Install the Threat Prevention policy on one or more of these Security Gateways</td>
</tr>
</tbody>
</table>

**Example**: `fwm load -p threatprevention Standard gw1 gw2`

**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`. 
Configuring Advanced Threat Prevention Settings

**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...
: 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](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](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}}`

<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></td>
</tr>
<tr>
<td>enable</td>
<td>Enables the appliance or Security Gateway to scan local connection</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the appliance or Security Gateway to scan local connection</td>
</tr>
</tbody>
</table>

**Example:**

`tecli d o or tecli debug on`

`tecli d s l e or tecli debug scan local enable`

---

**tecli show**

**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>
</tbody>
</table>
### Configuring Advanced Threat Prevention Settings

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tecli s c q</code></td>
<td>Shows the quota for ThreatCloud emulation</td>
</tr>
<tr>
<td><code>tecli s e e</code></td>
<td>Shows the current status of the emulation queue</td>
</tr>
<tr>
<td><code>tecli s u a</code></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 or tecli show cloud identity
```

```
tecli s c in or 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>}}` |

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>emulations</td>
<td>Shows the current status of the emulation queue</td>
</tr>
<tr>
<td>synopsis</td>
<td>Shows a summary of the VMs</td>
</tr>
<tr>
<td>detailed</td>
<td>Shows data and details of the VMs</td>
</tr>
<tr>
<td>id &lt;ID&gt;</td>
<td>Shows data for the VM with this ID</td>
</tr>
</tbody>
</table>

**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>
</tbody>
</table>
### Configuring Advanced Threat Prevention Settings

#### Threat Prevention Administration Guide R77 Versions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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:

```plaintext
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`

**Results**:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Last day</th>
<th>Last week</th>
<th>Last 30 days</th>
</tr>
</thead>
<tbody>
<tr>
<td>scanned files</td>
<td>262</td>
<td>262</td>
<td>262</td>
</tr>
<tr>
<td>benign files</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>average process time for emulated files</td>
<td>177 sec.</td>
<td>177 sec.</td>
<td>177 sec.</td>
</tr>
<tr>
<td>peak queue size</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>peak queue size</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>malicious files on cloud</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>average cloud process time</td>
<td>181 sec.</td>
<td>181 sec.</td>
<td>181 sec.</td>
</tr>
</tbody>
</table>

**Last Sharing succeeded**: Thu Aug 8 03:01:00 2013

**Sharing identifier**: HASHED_7dc322936b6f1edd6d6472632f019f30d-222c90527b6f0b1bebecefl468b8ad1fca
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 s t mi or tecli show throughput minute
```
```
tecli s t mo or tecli show throughput month
```

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
```

**Results:**
```
# tecli s u a
[prepare]
  - system state                   (15)
  - policy                         (15)
  - file                           (1)
  - contract                       (1)
  - cache inquirer                 (1)
[processing]
  - duplicate                      (1)
  - static analysis                (1)
  - emulator                       (1)
  - cloud emulation                (1)
  - remote emulation               (1)
[finalizing]
  - forensics                      (15)
  - cache updater                  (15)
  - threat cloud sharing           (15)
  - threat cloud statistics        (15)
  - file saver                     (15)
  - logger                         (15)
  - local filter counter           (15)
```
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

If you are blocking SMTP traffic with the Prevent action, we recommend that you enable MTA on the Security Gateway ("Using an MTA" on page 29). If you do not enable the MTA, it is possible that emails are dropped and do not reach the mail server.
Using Anti-Spam and Mail

In This Section:

Introduction to Anti-Spam and Mail Security ................................................................. 129
Mail Security Overview ........................................................................................................ 130
Configuring Anti-Spam .......................................................................................................... 132
Configuring Anti-Virus Protection for Mail ......................................................................... 135
Configuring a Disclaimer ...................................................................................................... 137
Anti-Spam Logging and Monitoring ...................................................................................... 137
Reporting False Positives to Check Point ............................................................................ 137
Anti-Spam Tracking and Reporting Options ........................................................................ 137

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.
The following figure illustrates the Anti-Spam workflow:

1. Proxy SMTP server on the gateway receives incoming mail
2. The SMTP proxy forwards the mail to an Anti-Spam daemon to extract selected message characteristics, and produce a hash fingerprint.
3. Using a special Anti-Spam protocol, the Anti-Spam daemon queries the Detection center. The hashed fingerprint is compared to other fingerprints in the pattern repository to determine whether the email is spam.
4. The detection classifies the email as either spam or not spam, and returns the result to the gateway.
5. If the email has been classified 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 has been 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 a rule can be configured to delete all emails with the word SPAM in either the subject line or header.

To prevent delays while large email files are scanned for Spam, a feature known as Adaptive Continuous Download transfers email to the recipient while Anti-Spam detection takes place.

Adaptive Continuous Download

To avoid 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 protocol's support Adaptive Continuous Download for the entire email message.
Configuring Anti-Spam

Configuring a Content Anti-Spam Policy

A content Anti-Spam policy is set on the Anti-Spam & Mail tab of SmartDashboard > Anti-Spam > Content based Anti-Spam.

1. Use the slider to select an Anti-Spam policy protection level.
2. Select flagging options.
3. In the Security Gateway Engine settings section, set a maximum data size to scan.
4. 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.

UTM-1 Edge devices contain their own Anti-Spam engines. Values entered in the UTM-1 Edge Engine settings section are used to correlate SofaWare Anti-Spam engine ratings with Check Point Anti-Spam engine ratings. For example if a particular email message is rated by the SofaWare Anti-Spam engine as 90, and this value, once translated into Check Point ratings, means the email should be treated as spam, then the Actions defined for Spam or Suspected spam on the Anti-Spam Policy page are enforced.

5. 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.

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. In this way, the IP reputation feature creates a list of trusted email sources.

1. 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

2. 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.

Configuring a Block List
A list of email sources to block can be configured according to the sender's name, domain name, or IP address.

1. 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
2. In the Blocked senders\domains section, click Add and enter the name of a sender or domain to be rejected.
3. In the Blocked IPs section, click Add and enter an IP address that should be blocked.
4. From the drop-down list in the Tracking section, select a tracking option for blocked mail or non-spam.

Configuring Anti-Spam SMTP
SMTP traffic can be scanned according to direction.

1. Select a scanning direction for:
   - Incoming files
   - Outgoing files
   - Internal files through the gateway
2. Select Activate Continuous download to avoid client time-outs when large files are scanned.
   See Adaptive Continuous Download ("Continuous Download" on page 146) for further information.

Configuring Anti-Spam POP3
POP3 traffic can be scanned according to direction.

1. Select a scanning direction for:
   - Incoming files
   - Outgoing files
   - Internal files
2. Select Activate Continuous download to avoid client time-outs when large files are scanned.
   See Adaptive Continuous Download ("Continuous Download" on page 146) for further information.
Configuring Network Exceptions

An Anti-Spam policy can be enforced on all email traffic or only on traffic that has not been deliberately excluded from the policy.

To exclude sources and destinations:
1. In the Anti-Spam & Mail tab, click Anti-Spam > Advanced > Network Exceptions.
2. Select Enforce the Anti-Spam policy on all traffic except for traffic between the following sources and destinations.
3. Click Add. The Network Exception window opens.
4. For Source and Destination, select Any, or select Specific and one gateway from each list.
5. Click OK.

Configuring an Allow List

A list of email sources to allow can be configured according to either the senders name and domain name, or IP address.

1. In the Anti-Spam & Mail tab, click Anti-Spam > Advanced > Allow List.
2. In the Allowed Senders / Domains section, click Add and enter the name of a sender or domain to be allowed.
3. In the Allowed IPs section, click Add and enter an allowed IP address.
4. From the drop-down list in the Tracking section, select a tracking option.

Selecting a Customized Server

You can select an alternative data center for Anti-Spam analysis.

To select a data center:
1. In the Anti-Spam & Mail tab, click Anti-Spam > Advanced > Customized Server.
2. Select Use Customized Server.
3. From the drop-down list, select a server.

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 email from being used as a virus delivery mechanism.

To configure a mail Anti-Virus policy:

1. In the Anti-Spam & Mail tab, click Traditional Anti-Virus > Security Gateway > Mail Protocols > Mail Anti-Virus.
2. Set the slider to Block.
3. 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

Configuring Zero Hour Malware Protection

By proactively scanning the Internet, the Data 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.

1. In the Anti-Spam & Mail tab, click Traditional Anti-Virus > Security Gateway > Mail Protocols > Zero Hour Malware Protection.
2. Using the slider, select a Zero hour malware protection level:
   - Off
   - Monitor Only
   - Block
3. Select tracking options for blocked, SMTP and POP3 mail. Tracking options include:
   - None (no logging)
   - Log
   - Popup alert
   - Mail alert
   - SNMP trap alert
4. Three custom user-defined scripts
Configuring SMTP and POP3

SMTP and POP3 traffic can be scanned according to direction or by IPs.

1. In the Anti-Spam & Mail tab, click Traditional Anti-Virus > Security Gateway > Mail Protocols > SMTP or POP3.

2. Using the slider, select a protection level:
   - Off
   - Monitor Only - SMTP and HTTP are the only protocols that support this protection level
   - Block

3. When scanning by File Direction, select a scanning direction for:
   - Incoming files
   - Outgoing files
   - Internal files through the gateway

4. When scanning by IPs, create rules for the Rule Base to specify 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 (on page 145) for further information. FTP and POP3 are set to Proactive Detection mode automatically.

6. If Proactive Detection has been configured, select the Activate Continuous Download checkbox to avoid client time-outs when large files are scanned. See Continuous Download (on page 146) for further information.

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.

- In the Anti-Spam & Mail tab, click Traditional Anti-Virus > Security Gateway > File Types page and set the actions.
Configuring Settings

Define maximum sizes for files and archives that should be scanned. Configure actions to take if the set limits are exceeded, or when a scan fails.

- In the **Anti-Spam & Mail** tab, click **Traditional Anti-Virus > Security Gateway > Settings** page, configure the fields.

Configuring a Disclaimer

You can create your own custom disclaimer notice.

1. In the **Anti-Spam & Mail** tab, click **Advanced > Disclaimer**.
2. Select **Add disclaimer to email scanned by Anti-Virus and Anti-Spam engines**.
3. In the text box, type your disclaimer notice.

Anti-Spam Logging and Monitoring

Logs derived from Anti-Spam scanning are sent to Security Management Server, and viewed using SmartView Tracker.

Anti-Spam status is monitored using SmartView Tracker. The Anti-Spam status appears under the Firewall product. The status contains information such as the Anti-Spam engine version. Anti-Spam status also includes statistics regarding scanned files. See also: Tracking and Reporting Options (**"Anti-Spam Tracking and Reporting Options" on page 137**).

Reporting False Positives to Check Point

A small number of genuine emails will inevitably be classified as spam. To help Check Point fine-tune the Anti-Spam service, please report them to Check Point support.

The sender of an email that is falsely classified as spam will receive an email notification that the email could not be delivered. This email contains an **Email session ID**.

1. Request the email session ID from the sender.
2. Open SmartView Tracker.
3. On the **Log tab > Content-based Anti-Spam** section locate the email session ID.
4. Open the **Record Details** and click **Copy**.
5. At the **Check Point Support Center**, open a Service Request and paste in the record details.
   For more information on how to create and view Service Requests, refer to sk31615 http://supportcontent.checkpoint.com/solutions?id=sk31615.

Anti-Spam Tracking and Reporting Options

Anti-Spam tracking and reporting options are available in:

- SmartView Tracker
- SmartView Monitor
- SmartReporter
SmartView Tracker

SmartView Tracker logs Anti-Spam activity. Record details exist for Number, Date, Time, Product, Interface, Origin, Type, Action, Service, Source, Source country, Destination, Sender, Original sender, Recipients, Original recipients, Spam category, Control, and Information.

Right-clicking on a row displays a new Follow Email Session ID option. Following the session provides granular information.

<table>
<thead>
<tr>
<th>No.</th>
<th>Date</th>
<th>Time</th>
<th>Origin</th>
<th>Product</th>
<th>Service</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
<th>Source country</th>
<th>Recipients</th>
<th>Original sender</th>
<th>Original recipients</th>
<th>Control</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>5441</td>
<td>Sep 2007</td>
<td>9:17:26</td>
<td>spam,plot</td>
<td>smtp</td>
<td>smtp</td>
<td>chenley,checkpoint.... spam,plot</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5442</td>
<td>Sep 2007</td>
<td>9:17:26</td>
<td>spam,plot</td>
<td>smtp</td>
<td>smtp</td>
<td>chenley,checkpoint.... spam,plot</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5443</td>
<td>Sep 2007</td>
<td>9:17:26</td>
<td>spam,plot</td>
<td>smtp</td>
<td>smtp</td>
<td>chenley,checkpoint.... spam,plot</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SmartView Monitor

SmartView Monitor reports on Anti-Spam and Anti-Virus activity.

SmartReporter

New express reports for content inspection have been added to SmartReporter:

- Anti-Virus
- Anti-Spam
Managing Traditional Anti-Virus

Traditional Anti-Virus inspection uses these detection modes:

- Proactive mode - a file-based solution where traffic for the selected protocols is trapped in the kernel and forwarded to the security server. The security server forwards the data stream to the Traditional Anti-Virus engine. The data is allowed or blocked based on the response of the Traditional Anti-Virus engine.
- Stream mode - where traffic for the selected protocols is processed in the kernel on the stream of data without storing the entire file. The data is allowed or blocked based on the response of the kernel.

The POP3 and FTP protocols work only in Proactive mode. The SMTP and HTTP protocols can be configured to work in either Proactive or Stream mode. Anti-Virus scanning is applied only to accepted traffic that has been allowed by the security policy.

Use the instructions in this section to configure Traditional Anti-Virus in your system.

Enabling Traditional Anti-Virus

The Anti-Virus blade and Traditional Anti-Virus can be activated on Security Gateways in your system.

عزي - You cannot activate the Anti-Virus blade and Traditional Anti-Virus on the same Security Gateway.

To configure traditional Anti-Virus:

1. On the Firewall > Overview tab, double-click the required Security Gateway network object.
2. Select Other > More Settings > Enable Traditional Anti-Virus.
3. Click OK.
4. Define rules in the Firewall Policy Rule Base to permit specific services. Anti-Virus scanning is applied only to accepted traffic.
5. From Threat Prevention tab > Traditional Anti-Virus, select the services to scan using these options:
   a) From the Database Update page, configure when to perform automatic signature updates or initiate a manual signature update.
   b) From the Security Gateway > Mail Protocol page, configure Anti-Virus scanning options for Mail Anti-Virus, Zero Hour Malware, SMTP, and POP3 services.
   c) From the Security Gateway > FTP page, configure FTP traffic scanning options.
   d) From the Security Gateway > HTTP page, configure HTTP traffic scanning options.
   e) From the Security Gateway > File Types page, configure the options to scan, block or pass traffic according to the file type and configure continuous download options.
   f) From the Security Gateway > Settings page, configure options for file handling and scan failures.

Database Updates

The following kinds of database updates are available:

- **Automatic**: Updates of the virus signature can be scheduled at a predefined interval.
- **Manual**: Updates of virus signatures can be initiated at any time.

Download updates from a Check Point server prior to downloading signature updates. First verify that:

- HTTP and HTTPs Internet connectivity with DNS is properly configured.
- You have a valid Check Point User Center user name and password.

The following signature update methods are available (the default update interval is 120 minutes for all methods):

- **Download signature updates every x minutes**: Enables you to define the update interval.
- **Download from Check Point site**: Indicates that each Security Gateway is responsible for contacting Check Point’s site to obtain Traditional Anti-Virus signatures. Updates are downloaded directly to the CI gateways. This method usually results in faster update times.
- **Download from My local Security Management Server**: Indicates that updates are only downloaded by the Security Management Server from the default Check Point signature distribution server and then redistributed all CI gateways. This method is useful when Internet access is not available for all gateways or if the download can only occur once for all the gateways.
Understanding Traditional Anti-Virus Scanning Options

In This Section
 Definitions ...........................................................................................................................................141
 Comparing Scan by File Direction and by IPs ..............................................................................141
 Scanning by File Direction: Selecting Data to Scan ....................................................................144
 Understanding Proactive and Stream Mode Detection ..................................................................145
 Continuous Download ....................................................................................................................146
 File Type Recognition ......................................................................................................................146

Definitions

Scan by File Direction and Scan by IPs are two file scanning methods used by Content Inspection. Traditional Anti-Virus scanning is performed only on traffic that is allowed by the Security Rule Base.

Scan By File Direction

Scan by File Direction scans all files passing in one direction, either to or from the external, internal and/or DMZ networks. Using this method (the default) is fairly intuitive and does not require the specification of hosts or networks. This method also enables you to define exceptions, for example, locations to or from which files are not scanned.

Scan By IP Address

Scan by IPs lets you define the traffic to be scanned. For example, if all incoming traffic from external networks reaches the DMZ using Scan by IPs, you can configure Traditional Anti-Virus to scan only traffic to the FTP, SMTP, HTTP and POP3 servers. Conversely, Scan by File Direction scans all traffic to the DMZ.

When using Scan by IPs, use a Rule Base to specify the source and destination of the data to be scanned. For FTP, for each rule, you can scan either the GET or the PUT methods, or both. For HTTP, for each rule, you can scan either the HTTP Request, the HTTP Response or both.

Comparing Scan by File Direction and by IPs

Scan by File Direction enables you to specify file scanning according to the file's (and not necessarily the connection's) origin and destination.

Scan by IPs enables you to specify file scanning according to the connection they are sent through and the protocol phase/command (where applicable).

If you want most or all files in a given direction to be Traditional Anti-Virus scanned, select Scan by File Direction.

If you want to specify a connection or part of a connection's source or destination to be scanned, select Scan by IPs.
Comparing Scan by File Direction and by IPs for SMTP Protocol

For the SMTP protocol, Scan by File Direction and Scan by IPs are comparable options. The next figure illustrates that for the SMTP protocol, the files (data) are always sent in the same direction as the connection. The SMTP protocol is used to send mail. Protocols that are used to receive mail (for example, POP3 and IMAP) are not scanned when SMTP is selected.

Comparing Scan by File Direction and by IPs for POP3 Protocol

The next figure illustrates that POP3 data files are always sent in the opposite direction of the connection.
Comparing Scan by File Direction and by IPs for FTP Protocol

For the FTP protocol, the difference between Scan by IPs and Scan by File Direction is illustrated in the next figure. When the FTP GET command is used, files are transferred in the opposite direction to the connection. When the FTP PUT command is used, files are transferred in the same direction as the connection. In this scenario, the Scan by File Direction option enables you to scan files without having to consider the direction of the connection.

Comparing Scan by File Direction and by IPs for HTTP Protocol

For the HTTP protocol, the difference between Scan by IPs and Scan by File Direction is illustrated in the next figure. Using Scan by IP, the source and destination of the connection are specified and whether the Request, Response or both is scanned.
Scanning by File Direction: Selecting Data to Scan

When using Scan by File Direction, you must select the direction of the data to scan, which depends on whether you want to scan files to or from the internal networks and the DMZ.

**What is a DMZ?**

The DMZ (demilitarized zone) is an internal network with an intermediate level of security. Its security level lies between trusted internal networks, such as a corporate LAN, and non-trusted external networks, such as the Internet.

Typically, the DMZ contains devices accessible to Internet traffic, for example, Web (HTTP), FTP, SMTP (email), DNS and POP3 servers.

Scan By File Direction enables you to define a level of Traditional Anti-Virus scanning that is specific to the DMZ. For example, you can decide not to scan traffic passing from external networks to the DMZ, but to still scan traffic passing from the DMZ to internal networks and from the external to internal networks.

**Scan By File Direction Options**

The following Scan By File Direction options are available:

- **Incoming files arriving to**: Files arriving from external interfaces: the internal networks (1), the DMZ (2) and the DMZ and internal networks (1 and 2).

- **Outgoing files leaving**: Files leaving through external interfaces: the internal networks (1), the DMZ (2) and the DMZ and internal networks (1 and 2).
• **Internal files**: If there is no DMZ, files passing between all internal networks (1). If there is a DMZ, files passing between the DMZ and internal networks and files passing between all internal networks (between internal networks (1), from the DMZ to internal networks (2) and from internal networks to the DMZ (3)).

Understanding Proactive and Stream Mode Detection

Traditional Anti-Virus scanning can be enabled in either the proactive or stream detection mode.

• **Proactive detection mode** - a comprehensive, file-based Traditional Anti-Virus solution where traffic for the selected protocols is trapped in the kernel of the Security Gateway and forwarded to the security server for scanning. It detects not only known viruses, but also zero-day attacks, by using advanced proactive techniques. This mode uses sandboxes and heuristics to detect malicious code throughout the traffic as opposed to passive signature based detection. Scanned data is either allowed or blocked based on the response of the state-of-the-art Traditional Anti-Virus engine.

  Proactive detection provides a high level of protection but has an impact on performance. The FTP and POP3 protocols only work in Proactive mode.

  This mode is not available for Virtual System gateways.

• **Stream detection mode** - where traffic is scanned for viruses as it passes through the network on streams of data, without storing entire files and without causing an impact on performance. The SMTP and HTTP protocols can be set to work in either mode.

  This mode is based on state-of-the-art virus signatures that are frequently updated in order to detect recent Malware outbreaks.

In newly installed systems, stream mode is activated by default.

In upgraded systems, the detection mode that is activated by default is dependent upon whether the Traditional Anti-Virus feature was previously activated or not.

• In upgraded systems that previously used the Traditional Anti-Virus scanning feature, proactive detection is activated by default.

• In upgraded systems that previously did not use the Traditional Anti-Virus scanning feature, stream mode detection is activated by default.

You can configure which detection mode to use from SmartDashboard for the SMTP and HTTP protocols.
Continuous Download

The Traditional Anti-Virus engine acts as a proxy which caches the scanned file before delivering it to the client for files that need to be scanned.

When scanning large files, if the whole file is scanned before being made available, the user may experience a long delay before the file is delivered. A similar problem may arise when using client applications with short timeout periods (for example, certain FTP clients) to download large files. If the whole file is cached and scanned before being delivered, the client applications may time out while waiting.

To address this problem, Continuous Download starts sending information to the client while Traditional Anti-Virus scanning is still taking place. If a virus is found during the scan, file delivery to the client is terminated.

**Note** - Continuous Download is only relevant if you have selected to use the **Activate proactive detection** option.

You can specify the file types for which you do not want Continuous Download to occur. Some file types (for example, Adobe Acrobat PDF and Microsoft Power Point files) can open on a client computer before the whole file has been downloaded. If Continuous Download is allowed for those file types, and a virus is present in the opened part of the file, it could infect the client computer.

**Note** - The SMTP and POP3 protocols support Continuous Download for the entire email message.

File Type Recognition

IPS has a built-in File Type recognition engine, which identifies the types of files passed as part of the connection and enables you to define a per-type policy for handling files of a given type.

You can specify safe file types that are allowed to pass through IPS without being scanned for viruses. It is also possible to configure file types to be scanned or blocked.

The following file types can be configured:

- **Scan**: Performs Traditional Anti-Virus file scanning according to the settings in the different services pages. By default, all unrecognized file types are scanned.
- **Block**: Does not allow passage of file types that are preset for blocking according to IPS advisories.
- **Pass**: Allows files to pass through the Security Gateway without being scanned for viruses. Files specified as this type are considered to be safe.

File types are considered to be safe if they are not known to contain viruses, for example, some picture and video files are considered safe. Other formats are considered to be safe because they are relatively hard to tamper with. What is considered to be safe changes according to published threats and depends on how the administrator balances security versus performance considerations.

IPS reliably identifies binary file types by examining the file type signatures (magic numbers). IPS does not rely on the file extension (such as *.GIF), which can be spoofed. It also does not use the MIME headers (such as image/gif) in HTTP and mail protocols, which can also be spoofed.
Configuring Traditional Anti-Virus

For detailed explanations regarding the options described in the procedures in this section, see Understanding Traditional Anti-Virus Scanning Options (on page 141).

Configuring Mail Traditional Anti-Virus

The Mail Traditional Anti-Virus policy prevents email from being used as a virus delivery mechanism.

1. In the Traditional Anti-Virus tab, click Traditional Anti-Virus > Security Gateway > Mail Protocols > Mail Traditional Anti-Virus.
2. Set the slider to Block.
3. 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

Configuring Zero Hour Malware

By proactively scanning the Internet, the Data 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.

1. In the Traditional Anti-Virus tab, click Traditional Anti-Virus > Security Gateway > Mail Protocols > Zero Hour Malware Protection.
2. Using the slider, select a Zero hour malware protection level:
   - Off
   - Monitor Only
   - Block
3. 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

Configuring SMTP, POP3, FTP and HTTP

SMTP and POP3 traffic can be scanned according to direction or by IPs.

1. In the Traditional Anti-Virus tab, click Traditional Anti-Virus > Security Gateway > Mail Protocols > SMTP, POP3, FTP or HTTP.
2. Using the slider, select a protection level:
   - Off
   - Monitor Only - SMTP and HTTP are the only protocols that support this protection level
   - Block
3. When scanning by File Direction, select a scanning direction for:
   - Incoming files
   - Outgoing files
   - Internal files through the gateway
4. When scanning by IPs, create rules for the Rule Base to specify 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 (on page 145) for further information. FTP and POP3 are set to Proactive Detection mode automatically.
6. If Proactive Detection has been configured, select the **Activate Continuous Download** checkbox to avoid client time-outs when large files are scanned. See Continuous Download (on page 146) for further information.

### 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.

**File Types**

![File Types Table]

- In the **Anti-Spam** tab, click **Traditional Anti-Virus >Security Gateway >File Types** page and set the actions. See File Type Recognition (on page 146) for more information.

In this window, you can also configure Continuous Download options. Continuous Download options are only relevant if scanning is set to Proactive Detection. See Continuous Download (on page 146) for more information.
Configuring Security Gateway Settings

In Traditional Anti-Virus tab, click Traditional Anti-Virus >Security Gateway >Mail Protocols > Settings you can configure scan failure settings and Proactive scan settings (file handling and archive file handling).

Scan Failure

The following scan failure options are available:

- **When Traditional Anti-Virus engine is overloaded or scan fails**: Determines whether to scan or block the file.
- **When Traditional Anti-Virus engine fails to initialize**: Determines whether to scan or block the file.

File Handling

The following file handling options are available:

- **Maximum file size to scan**: Limits the file size that is allowed to pass through the gateway. If the file is a compressed archive, the limit applies to the file after decompression (the Traditional Anti-Virus engine decompresses archives before scanning them). Before performing Traditional Anti-Virus scanning, the gateway reassembles the entire file and then scans it. The limit protects the gateway resources and the destination client. An archive is a file that contains one or more files in a compressed format. Archives (and all other file types) are recognized by their binary signature. By default, any file type that is not identified as non-archive is assumed to be an archive and the Traditional Anti-Virus engine tries to expand it.
- **When file exceeds limit**: Determines whether to scan or block the file.

  **Note** - An email is treated as an archive and as a result it is not affected when the file exceeds the limit.

Archive File Handling

The following file handling archiving options are available:

- **Maximum archive nesting level**: Limits the number of nested archives (one within another). This limit protects the gateway and destination client from attacks that employ deep nesting levels.
- **Maximum compression ratio**: Prevents attacks that employ a small size archive that decompresses into a very large file on target.
- **When archive file exceeds limit or extraction fails**: Determines whether to scan or block the file.

Logging and Monitoring

Logging information on the Traditional Anti-Virus scan is sent to the Security Management Server and can be viewed using SmartView Tracker. Scan results information is shown in the logs. In addition, there are logs for signature updates, new update checks, and download results.

The Traditional Anti-Virus status is monitored using SmartView Monitor. The Traditional Anti-Virus status appears under the Firewall product. The status contains information on the currently
installed signature file and the Traditional Anti-Virus engine version. The Traditional Anti-Virus status also includes statistics about scanned files and found viruses.

**UTM-1 Edge Traditional Anti-Virus**

You can now enable Traditional Anti-Virus protection within UTM-1 Edge. Selecting the **Enable Traditional Anti-Virus** option indicates that Traditional Anti-Virus protection is installed and that updates are sent to the specified gateway.

Using UTM-1 Edge Traditional Anti-Virus, you can define the maximum archive file sizes for UTM-1 Edge machines that are scanned, and configure procedures for when these limits are exceeded and/or the scan fails.

The UTM-1 Edge Traditional Anti-Virus feature enables you to automatically or manually update virus signatures for UTM-1 Edge machines and provides you with the tools to configure how UTM-1 Edge traffic is scanned.

**Note** - It is important to configure a valid DNS server address on your management and gateway in order for the signature update to work.

The UTM-1 Edge Traditional Anti-Virus scanning policy enables you to select the service(s) to and from which a source and/or destination is scanned. Files set for scanning is determined using a classic Rule Base, which defines the source and destination of the connection to be scanned. It is recommended to use this method if you want to define exactly which traffic to scan, for example, if all incoming traffic from external networks reaches the DMZ, you can specify that only traffic to the Traditional Anti-Virus servers is scanned.

To enable and configure Traditional Anti-Virus protection:

1. From the **General Properties** tab of the UTM-1 Edge gateway, select the **Other > More Settings > Enable Traditional Anti-Virus**.
2. In the **Edge Traditional Anti-Virus** section of the **Traditional Anti-Virus** tab, configure Traditional Anti-Virus to work on UTM-1 Edge gateways. All of the Traditional Anti-Virus settings in the **Traditional Anti-Virus** tab do not work for UTM-1 Edge machines. The Edge Traditional Anti-Virus settings in the **Traditional Anti-Virus** tab only work for UTM-1 Edge machines.
Regular Expressions

In This Appendix

Regular Expression Syntax ................................................................. 151
Using Regular Expressions in Custom Sites ........................................... 152
Using Non-Printable Characters ......................................................... 152
Using Character Types ................................................................. 153

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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>non-printable characters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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 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>Wildcard</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>.*.example.com</td>
<td>.example.com</td>
<td></td>
</tr>
</tbody>
</table>

More examples of regular expressions:

To match subdomains of mydomain.com:   (^|.*\.)mydomain\.com
To match domain and subdomains of mydomain.com:   (^|.*\.)*mydomain\.com

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 07)</td>
</tr>
<tr>
<td>\cx</td>
<td>&quot;control-x&quot;, where x is any character</td>
</tr>
<tr>
<td>\e</td>
<td>escape (hex 1B)</td>
</tr>
<tr>
<td>\f</td>
<td>formfeed (hex 0C)</td>
</tr>
<tr>
<td>\n</td>
<td>newline (hex 0A)</td>
</tr>
<tr>
<td>\r</td>
<td>carriage return (hex 0D)</td>
</tr>
<tr>
<td>\t</td>
<td>tab (hex 09)</td>
</tr>
<tr>
<td>\ddd</td>
<td>character with octal code ddd</td>
</tr>
<tr>
<td>\xhh</td>
<td>character with hex code hh</td>
</tr>
</tbody>
</table>
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>
Index

A
Accessing the Threat Wiki • 98, 103
Action • 11, 60, 84
Adaptive Continuous Download • 131
Adding a New Host Site • 84
Adding a Server Certificate • 81
Adding Exception Groups to the Rule Base • 53
Adding Exceptions to Exception Groups • 53
Adding Trusted CAs for Outbound HTTPS Inspection • 86
Affinity • 11
Analyzing Threats • 13
Anti-Bot • 11, 18
Anti-Bot and Anti-Virus Event Queries • 100
Anti-Bot and Anti-Virus Licensing and Contracts • 21
Anti-Bot and Anti-Virus Reports • 98
Anti-Bot Settings • 105
Anti-Spam • 130
Anti-Spam Logging and Monitoring • 137
Anti-Spam on UTM-1 Edge Devices • 134
Anti-Spam Tracking and Reporting Options • 137
Anti-Virus • 20
Archive File Handling • 149
Ask • 11
Automatically Updating the Trusted CA List and Certificate Blacklist • 87

B
Blade • 85
Blade Queries • 93
Blocking Bots • 33
Blocking Viruses • 37
Bridge Mode and Anti-Spam • 134
Bypassing HTTPS Inspection for Software Update Services • 85

C
Certificate • 85
Certificate Blacklisting • 89
Changing the Analysis Location • 118
Changing the Local Cache • 119
Check Point Online Web Service • 104
Check Point ThreatCloud Network • 17
Comparing Scan by File Direction and by IPs • 141
Comparing Scan by File Direction and by IPs for FTP Protocol • 143
Comparing Scan by File Direction and by IPs for HTTP Protocol • 143
Comparing Scan by File Direction and by IPs for POP3 Protocol • 142
Comparing Scan by File Direction and by IPs for SMTP Protocol • 142
Configuring a Block List • 133
Configuring a Cluster • 40
Configuring a Content Anti-Spam Policy • 132
Configuring a Disclaimer • 137
Configuring a Malware DNS Trap • 71
Configuring Advanced Engine Settings for Threat Extraction • 42
Configuring Advanced Profile Settings • 114
Configuring Advanced Threat Prevention Settings • 104
Configuring an Allow List • 134
Configuring an IP Reputation Policy • 132
Configuring Anti-Bot Settings • 67
Configuring Anti-Spam • 132
Configuring Anti-Spam POP3 • 133
Configuring Anti-Spam SMTP • 133
Configuring Anti-Virus Protection for Mail • 135
Configuring Anti-Virus Settings • 68
Configuring File Types • 136
Configuring File Types • 148
Configuring Inbound HTTPS Inspection • 80
Configuring Indicators in SmartDashboard • 109
Configuring Inspection of Links Inside Mail • 72
Configuring Mail Anti-Virus • 135
Configuring Mail Traditional Anti-Virus • 147
Configuring MTA Advanced Settings • 116
Configuring Network Exceptions • 134
Configuring Outbound HTTPS Inspection • 77
Configuring Postfix for MTA • 128
Configuring Security Gateway Settings • 149
Configuring Settings • 137
Configuring SMTP and POP3 • 136
Configuring SMTP, POP3, FTP and HTTP • 147
Configuring the Emulation Limits • 118
Configuring the Network to Disable the MTA • 117
Configuring the Network to Use an MTA • 30
Configuring the Security Gateway • 39
Configuring the Security Gateway for UserCheck • 62
Configuring the Threat Extraction Blade • 39
Configuring the Threat Prevention Profile • 40
Configuring the Virtual Environment (Profile) • 70
Configuring Threat Emulation Settings • 69
Configuring Traditional Anti-Virus • 147
Configuring User Interaction • 65
Configuring Whitelist Files • 106
Configuring Zero Hour Malware • 147
Configuring Zero Hour Malware Protection • 135
Connecting to the Internet for Updates • 51
Connection Unification • 105
Continuous Download • 146
Converting Exceptions into an Exception Group • 58
Monitoring Threat Prevention with SmartEvent • 96
Monitoring Threat Prevention with SmartView Tracker • 101
My Organization • 47

Name • 58, 82
Number (No.) • 58, 82

Observable • 11
Optimizing File Emulation • 25
Optimizing System Resources • 120

Parts of the Rule • 82
Parts of the Rules • 58
Permissions for HTTPS Logs • 93
Policy • 11
Predefined Rule • 56, 82
Preparing for Local or Remote Emulation • 26
Prevent • 11
Preventing Bot Damage • 20
Problems with Email Emulation • 128
Profiles Pane • 65
Protected Scope • 58
Protection • 60
Protections Browser • 55

Redirecting to an External Portal • 64
Regular Expression Syntax • 151
Regular Expressions • 151
Reporting False Positives to Check Point • 137
RSS Feeds • 49
Rule • 11
Running the First Time Configuration Wizard • 27

Sample Workflow - Creating a Threat Emulation Profile • 31
Saving a CA Certificate • 88
Scan By File Direction • 141
Scan By File Direction Options • 144
Scan By IP Address • 141
Scan Failure • 149
Scanning by File Direction
   Selecting Data to Scan • 144
Scheduling Updates • 51
Searching Protections • 56
Security Gateway • 11
Security Gateway Portals • 92
Security Management Server • 11
Security Policy • 11
Selecting a Customized Server • 134

Selecting Emulation File Types • 105
Selecting the Correct Location • 15
Selecting the Threat Emulation Deployment • 16
Server Certificates • 81
Server Validation • 88
Services • 83
Setting the Activation Mode • 117
Site Category • 83
Sites Pane • 74
SmartDashboard • 11
SmartDashboard Toolbar • 14
SmartReporter • 138
SmartView Monitor • 138
SmartView Tracker • 11, 138
Sorting Protections • 56
Source • 83
Static Analysis • 115
Statistics • 48
STIX • 11
System Specifications • 17

Sample Workflow - Creating a Threat Emulation Profile • 31
Saving a CA Certificate • 88
Scan By File Direction • 141
Scan By File Direction Options • 144
Scan By IP Address • 141
Scan Failure • 149
Scanning by File Direction
   Selecting Data to Scan • 144
Scheduling Updates • 51
Searching Protections • 56
Security Gateway • 11
Security Gateway Portals • 92
Security Management Server • 11
Security Policy • 11
Selecting a Customized Server • 134

Selecting Emulation File Types • 105
Selecting the Correct Location • 15
Selecting the Threat Emulation Deployment • 16
Server Certificates • 81
Server Validation • 88
Services • 83
Setting the Activation Mode • 117
Site Category • 83
Sites Pane • 74
SmartDashboard • 11
SmartDashboard Toolbar • 14
SmartReporter • 138
SmartView Monitor • 138
SmartView Tracker • 11, 138
Sorting Protections • 56
Source • 83
Static Analysis • 115
Statistics • 48
STIX • 11
System Specifications • 17

tec_add_file • 122
tecli • 123
tecli advanced clear • 124
tecli cache clean • 124
tecli control sizing • 124
tecli debug • 124
tecli show • 124
tecli show cloud • 125
tecli show downloads • 125
tecli show emulator • 125
tecli show remote • 126
tecli show statistics • 126
tecli show throughput • 127
tecli show unit • 127
The Check Point Anti-Bot Solution • 19
The Check Point Anti-Virus Solution • 20
The Check Point Threat Prevention Solution • 13
The Check Point ThreatCloud • 49
The HTTPS Inspection Policy • 82
The Need for Anti-Bot • 18
The Need for Anti-Virus • 20
The Need for Threat Emulation • 15
The Policy Rule Base • 56
The SmartEvent Intro Overview Page • 99
The Threat Prevention Overview Page • 47
The ThreatCloud Repository • 50
Threat Emulation • 11, 15
Threat Emulation Analysis Locations • 22
Threat Emulation Deployments • 25
Threat Emulation Engine • 113
Threat Emulation Images • 113
Threat Emulation License Requirements • 18
Threat Emulation Logs • 115
Threat Emulation Private Cloud Appliance • 12
Threat Emulation Settings • 112
Threat Emulation Virtual Interface • 121
Threat Extraction Statistics • 43
Threat Indicators Settings • 107
Threat Prevention and UserCheck • 61
Threat Prevention CLI Commands • 122
Threat Prevention Logs • 102
ThreatCloud Emulation • 22
ThreatCloud Repository • 12
ThreatSpect Engine • 12
ThreatSpect engine and ThreatCloud repository • 20
Track • 60, 84
Traffic • 12
Traffic Direction and Interface Type Settings • 59
Troubleshooting • 90
Troubleshooting the Threat Extraction Blade • 44
Troubleshooting Threat Emulation • 128

U
Understanding Proactive and Stream Mode Detection • 145
Understanding Traditional Anti-Virus Scanning Options • 141
Updating the Anti-Bot and Anti-Virus Rule Base • 97, 102
Updating the Malware Database • 51
Updating Threat Emulation • 112
UserCheck • 12
Using a Fallback Action • 64
Using an MTA • 29
Using Anti-Bot and Anti-Virus with VSX • 121
Using Anti-Spam and Mail • 129
Using Character Types • 153
Using Cloud Emulation • 27
Using Local or Remote Emulation • 28
Using MTA with ClusterXL • 128
Using Non-Printable Characters • 152
Using Predefined Queries • 103
Using Protected Scope with SPAN and TAP Configurations • 59
Using Regular Expressions in Custom Sites • 152
Using the Gateway CLI • 43
Using the Threat Prevention UserCheck Pane • 61
Using the Threat Wiki • 50
Using Threat Prevention Software Blades • 13
Using Threat Prevention with HTTPS Traffic • 76
Using Traditional Anti-Virus • 139
UTM-1 Edge Traditional Anti-Virus • 150

V
Viewing Information in SmartEvent • 95, 96
Viewing Information in SmartEvent Intro • 99