13 March 2017

Threat Prevention

R80.10 Versions

Administration Guide

Check Point
SOFTWARE TECHNOLOGIES LTD.

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Check Point R80.10

For more about this release, see the R80.10 home page http://supportcontent.checkpoint.com/solutions?id=sk111841.

Latest Version of this Document

Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=TBD.

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

Feedback

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

Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Threat Prevention R80.10 Versions Administration Guide.

Searching in Multiple PDFs

To search for text in all the R80.10 PDF documents, download and extract the complete R80.10 documentation package http://supportcontent.checkpoint.com/documentation_download?ID=TBD.
Use **Shift-Control-F** in Adobe Reader or Foxit reader.

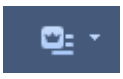
Revision History

Date	Description
13 March 2017	First release of this document

SmartConsole Toolbars

For a guided tour of SmartConsole, click **What's New** in the left bottom corner of SmartConsole.

Global Toolbar (top left of SmartConsole)

	Description and Keyboard Shortcut
	The main SmartConsole Menu
	The **Objects** menu. Also leads to the Object Explorer **Ctrl+E**

	Description and Keyboard Shortcut
	Install policy on managed gateways **Ctrl+Shift+Enter**

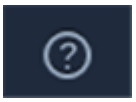
Navigation Toolbar (left side of SmartConsole)

	Description and Keyboard Shortcut
	Gateway configuration view **Ctrl+1**
	Security Policies Access Control view Security Policies Threat Prevention view **Ctrl+2**
	Logs & Monitor view **Ctrl+3**
	Manage & Settings view - review and configure the Security Management Server settings **Ctrl+4**

Command Line Interface Button (left bottom corner of SmartConsole)

	Description and Keyboard Shortcut
	Open a command line interface for management scripting and API **F9**

What's New Button (left bottom corner of SmartConsole)

	Description and Keyboard Shortcut
	Open a tour of the SmartConsole

Objects and Validations Tabs (right side of SmartConsole)

	Description
Objects	Manage security and network objects
Validations	Validation warnings and errors

System Information Area (bottom of SmartConsole)

	Description
Task List	Management activities, such as policy installation tasks
Server Details	The IP address of the Security Management Server

	Description
Connected Users	The administrators that are connected to the Security Management Server

LICENSE

Contents

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.

Anti-Virus

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

Ask

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

Detect

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

Event

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

Indicator

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

IPS

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

Malware Database

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

Observable

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

Policy

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

Prevent

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

Rule

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

Security Gateway

A computer or an appliance that inspects traffic and enforces Security Policies for connected network resources.

Security Management Server

The server that manages, creates, 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 with packet inspection.

SmartConsole

A Check Point GUI application used to manage security policies, monitor products and events, install updates, provision new devices and appliances, and manage a multi-domain environment.

STIX

Structured Threat Information eXpression. A language that describes cyber threat information in a standardized and structured way.

Threat Emulation

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

Threat Emulation Private Cloud Appliance

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

ThreatCloud IntelliStore

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

ThreatCloud Repository

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

ThreatSpect Engine

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

Traffic

The flow of data between network 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:

Threat Prevention Components

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

- IPS - A complete IPS cyber security solution, for comprehensive protection against malicious and unwanted network traffic, which focuses on application and server vulnerabilities, as well as in-the-wild attacks by exploit kits and malicious attackers.
- Anti-Bot - Post-infection detection of bots on hosts. Prevents bot damages by blocking bot C&C (Command and Control) communications. The Anti-Bot Software Blade is continuously updated from ThreatCloud, a collaborative network to fight cybercrime. Anti-Bot discovers infections by correlating multiple detection methods.
- Anti-Virus - Pre-infection detection and blocking of malware at the gateway. The Anti-Virus Software Blade is continuously updated from ThreatCloud. It detects and blocks malware by correlating multiple detection engines before users are affected.
- SandBlast:
  - Threat Emulation - Protection against infections from undiscovered exploits, zero-day and targeted attacks. This innovative solution quickly inspects files and runs them in a virtual sandbox to discover malicious behavior. Discovered malware is prevented from entering the network. The ThreatCloud Emulation service reports to the ThreatCloud and automatically shares the newly identified threat information with other Check Point customers.
  - Threat Extraction - Protection against incoming malicious content. To remove possible threats, the Threat Extraction blade creates a simpler version of the file in PDF format while the Threat Emulation Software Blade inspects the original file for potential threats.

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

IPS

The IPS Software Blade delivers complete and proactive intrusion prevention. It delivers 1,000s of signatures, behavioral and preemptive protections. It gives another layer of security on top of Check Point firewall technology. IPS protects both clients and servers, and lets you control the network usage of certain applications. The hybrid IPS detection engine provides multiple defense layers which allows it excellent detection and prevention capabilities of known threats, and in many cases future attacks as well. It also allows unparalleled deployment and configuration flexibility and excellent performance.

Elements of Protection

IPS protection include:

- Detection and prevention of specific known exploits.
- Detection and prevention of vulnerabilities, including both known and unknown exploit tools, for example protection from specific CVEs.
- Detection and prevention of protocol misuse which in many cases indicates malicious activity or potential threat. Examples of commonly manipulated protocols are HTTP, SMTP, POP, and IMAP.
- Detection and prevention of outbound malware communications.
- Detection and prevention of tunneling attempts. These attempts may indicate data leakage or attempts to circumvent other security measures such as web filtering.
- Detection, prevention or restriction of certain applications which, in many cases, are bandwidth consuming or may cause security threats to the network, such as Peer to Peer and Instant Messaging applications.
- Detection and prevention of generic attack types without any pre-defined signatures, such as Malicious Code Protector.

Check Point constantly updates the library of protections to stay ahead of emerging threats.

Capabilities of IPS

The unique capabilities of the Check Point IPS engine include:

- Clear, simple management interface.
- Reduced management overhead by using one management console for all Check Point products
- Integrated management with SmartConsole.
- Easy navigation from business-level overview to a packet capture for a single attack.
- Up to 15 Gbps throughput with optimized security, and up to 2.5 Gbps throughput with all IPS protections activated
- #1 security coverage for Microsoft and Adobe vulnerabilities.
- Resource throttling so that high IPS activity will not impact other blade functionality
- Complete integration with Check Point configuration and monitoring tools in SmartConsole, to let you take immediate action based on IPS information.

For example, some malware can be downloaded by a user unknowingly when he browses to a legitimate web site, also known as a drive-by-download. This malware can exploit a browser vulnerability to create a special HTTP response and sending it to the client. IPS can identify and

block this type of attack even though the firewall may be configured to allow the HTTP traffic to pass.

Anti-Bot

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

When a bot infects a computer, it:

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

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

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

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

- **Identify the C&C addresses used by criminals to control bots**

  These web sites are constantly changing and new sites are added on an hourly basis. Bots can attempt to connect to thousands of potentially dangerous sites. It is a challenge to know which sites are legitimate and which are not.

- **Identify the communication patterns used by each botnet family**

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

- **Identify bot behavior**

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

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

Anti-Virus

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

The Anti-Virus Software Blade scans incoming and outgoing files to detect and prevent these threats. It also gives pre-infection protection from malware contained in these files.

The Anti-Virus Software Blade:

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

SandBlast

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

Threat Emulation

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

When emulation is done on a file:

- The file is opened on more than one virtual computer with different operating system environments.
- The virtual computers are closely monitored for unusual and malicious behavior, such as an attempt to change registry keys or run an unauthorized process.
- Any malicious behavior is immediately logged and you can use Prevent mode to block the file from the internal network.
- The cryptographic hash of a new malicious file is saved to a database and the internal network is protected from that malware.

- After the threat is caught, a signature is created for the new (previously unknown) malware which turns it into a known and documented malware. The new attack information is automatically shared with Check Point ThreatCloud to block future occurrences of similar threats at the gateway.

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

Learn more about Threat Emulation ("The Threat Emulation Solution" on page 21).

Threat Extraction

Threat Extraction is supported on R77.30 and higher.

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

- Creates a simpler version of the file in PDF format, or
- Extracts exploitable content out of the file.

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

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

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

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

Before you enable the Threat Extraction blade, you must deploy the gateway as a Mail Transfer Agent ("Enabling MTA on the Security Gateway" on page 47).

Assigning Administrators for Threat Prevention

You can create administrator accounts dedicated to the role of Threat Prevention, with their own installation and SmartConsole Read/Write permissions.

For more about how to configure administrator permissions, see the *R80.10 Security Management Administration Guide* http://downloads.checkpoint.com/dc/download.htm?ID=TBD.

Analyzing Threats

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

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

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

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

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

The Threat Emulation Solution

In This Section:

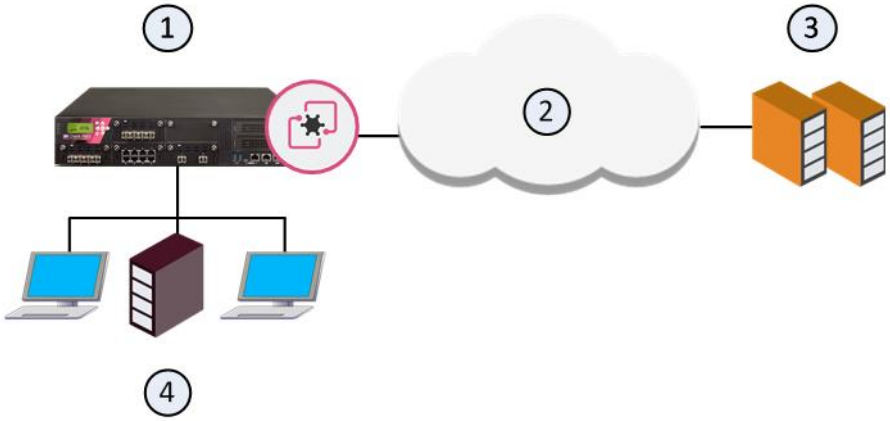
ThreatCloud Emulation

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



Item	Description
1	Perimeter Security Gateway
2	ThreatCloud
3	Check Point ThreatCloud virtual computers
4	Internal network

Threat Emulation Analysis Locations

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

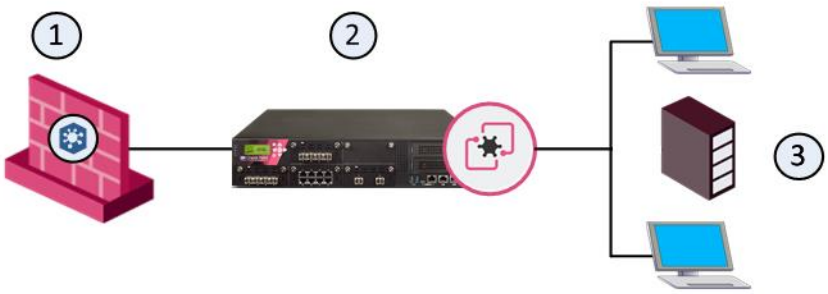
- **ThreatCloud** - You can send all files to the Check Point ThreatCloud for emulation. Network bandwidth is used to send the files and there is a minimal performance impact on the Security Gateway.
- **Threat Emulation Private Cloud Appliance (Emulation appliance) in the Internal network** - You can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

Local or Remote Emulation

You can install an Emulation appliance in the internal network.

Sample Workflow for Emulation Appliance in a Local Deployment

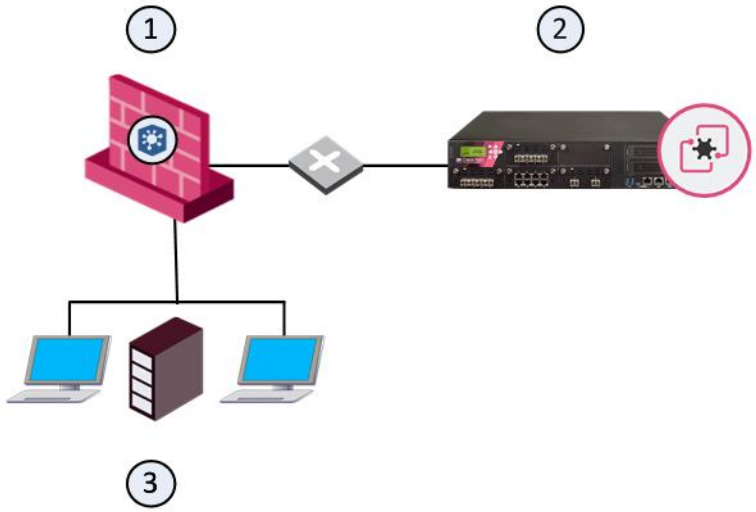
1. The Emulation appliance receives the traffic, and aggregates the files.
2. The Emulation appliance compares the cryptographic hash of the file with the database.
   - The file is already in the database, no more emulation is necessary.
   - If the file is not in the database, the virtual computers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



Item	Description
1	Perimeter Security Gateway
2	TE1000X Threat Emulation Private Cloud Appliance
3	Internal network

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.



Item	Description
1	Perimeter Security Gateway
2	TE250X Threat Emulation Private Cloud Appliance
3	Internal network

Optimizing File Emulation

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

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

This database helps to optimize emulation and give better network performance.

Selecting the Threat Emulation Deployment

What are my options to send traffic for emulation?

- Inline - Traffic is sent for emulation before it is allowed to enter the internal network. You can use the Threat Prevention policy to block malware.
- SPAN/TAP - You can use a mirror or TAP port to duplicate network traffic. Files are sent to the computer in the internal network. If Threat Emulation discovers that a file contains malware, the appropriate log action is done.
- MTA (Mail Transfer Agent) - 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. **Best Practice -** 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?

- 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:

	Block Malware
Inline	Yes
SPAN/TAP	No
MTA	Recommended with Prevent action for emails

Inline Deployments (Prevent and Ask)

Use the Prevent or Ask UserCheck action to quarantine a malicious file ("Threat Prevention and UserCheck" on page 79).

Sample Inline Emulation Workflow (Prevent Action)

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

Monitor Deployments

Sample Monitor Emulation Workflow

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

Threat Emulation Deployments with a Mail Transfer Agent

Best Practice - If you use the Prevent action to block SMTP traffic, we recommend that you enable the Security Gateway as an MTA (Mail Transfer Agent). You can use the MTA to help manage the emulation of emails and attachments ("Using an MTA" on page 46).

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.

Out-of-the-Box Protection from Threats

In This Section:

Getting Quickly Up and Running with the Threat Prevention Policy

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

To get quickly up and running with Threat Prevention:

1. Enable the Threat Prevention blades on the gateway.
2. **Install Policy**.

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

Name	Protected Scope	Action	Track	Install On
Out-of-the-box Threat Prevention policy	Any	Optimized	Log Packet Capture	Policy Targets

Notes:

- The **Optimized** ("Optimized Protection Profile Settings" on page 62) profile is installed by default.
- The **Protection/Site** ("Protection" on page 34) column is used only for protection exceptions.

Enabling the Threat Prevention Software Blades

Enabling the IPS Software Blade

Enable the IPS Software Blade on the Security Gateway.

To enable the IPS Software Blade:

1. In the **Gateways & Servers** view, double-click the gateway object.
   The **General Properties** window opens.
2. In the **General Properties** > **Network Security** tab, click **IPS**.
3. Follow the steps in the wizard that opens.
4. Click **OK**.

5. Click **OK** in the **General Properties** window.
6. **Install Policy** ("Installing the Threat Prevention Policy" on page 28).

Enabling the Anti-Bot Software Blade

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

1. In the **Gateways & Servers** view, double-click the gateway object.
   The **General Properties** window of the gateway opens.
2. From the **Network Security** tab, select **Anti-Bot**.
   The **Anti-Bot and Anti-Virus First Time Activation** window opens.
3. Select an activation mode option:
   - **According to the Anti-Bot and Anti-Virus policy** - Enable the Anti-Bot Software Blade and use the Anti-Bot settings of the Threat Prevention profile in the Threat Prevention policy.
   - **Detect only** - Packets are allowed, but the traffic is logged according to the settings in the Threat Prevention Rule Base.
4. Click **OK**.
5. **Install Policy** ("Installing the Threat Prevention Policy" on page 28).

Enabling the Anti-Virus Software Blade

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

To enable the Anti-Virus Software Blade:

1. In the **Gateways & Servers** view, double-click the gateway object.
   The **General Properties** window of the gateway opens.
2. From the **Network Security** tab, click **Anti-Bot**.
   The **Anti-Bot and Anti-Virus First Time Activation** window opens.
3. Select one of the activation mode options:
   - **According to the Anti-Bot and Anti-Virus policy** - Enable the Anti-Virus Software Blade and use the Anti-Virus settings of the Threat Prevention profile in the Threat Prevention policy.
   - **Detect only** - Packets are allowed, but the traffic is logged according to the settings in the Threat Prevention Rule Base.
4. Click **OK**
5. **Install Policy** ("Installing the Threat Prevention Policy" on page 28).

Enabling SandBlast Threat Emulation Software Blade

Use the First Time Configuration Wizard in SmartConsole 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.

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

To enable ThreatCloud emulation:

1. In the **Gateways & Servers** view, double-click the Security Gateway object.
   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 Policy** ("Installing the Threat Prevention Policy" on page 28).

Enabling the SandBlast Threat Extraction Blade

To enable the Threat Extraction Blade:

1. In the Gateways & Servers view, right-click the gateway object and select **Edit**.
   The **Gateway Properties** window opens.
2. On the **General Properties** > **Network Security** tab, select **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 **SmartConsole** > **Global Properties**.
2. On the **User Directory** page, select **Use User Directory for Security Gateways**.
3. Click **OK**.

Installing the Threat Prevention Policy

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

To install the Threat Prevention policy:

1. From the Global toolbar, click **Install Policy**.
   The **Install Policy** window opens showing the installation targets (Security Gateways).
2. Click **Advanced**.
3. Select the relevant **Advanced** options:
   Settings > **Policies**: Select only **Threat Prevention**.
   Settings > **Install Mode** gives you these installation options:
   - **Install on each selected gateway independently** - Install the policy on the selected Security Gateways without reference to the other targets. A failure to install on one Security Gateway does not affect policy installation on other gateways.

     If the gateway is a member of a cluster, install the policy on all the members. The Security Management Server makes sure that it can install the policy on all the members before it installs the policy on one of them. If the policy cannot be installed on one of the members, policy installation fails for all of them.
   - **Install on all selected gateways, if it fails do not install on gateways of the same version** - Install the policy on all installation targets. If the policy fails to install on one of the Security Gateways, the policy is not installed on other targets of the same version.
4. Click **OK**.

Predefined Rule

When you enable one of the Threat Prevention Software Blades, a predefined rule is added to the Rule Base. The rule defines that all traffic for all network objects, regardless of who opened the connection, (the protected scope (on page 33) value equals any) is inspected for all protections according to the optimized profile ("Profiles Pane" on page 62). By default, logs are generated and the rule is installed on all Security Gateways that use a Threat Prevention Software Blade.

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

- 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.

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

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

The Threat Prevention Policy

In This Section:

Workflow for Creating a Threat Prevention Policy

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

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

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

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

1. Enable the Threat Prevention Software Blades on the Security Gateways,
2. Update the IPS database and Malware database with the latest protections.
3. Optional: Create Threat Prevention Policy Layers.

   Note - For each Policy Layers, configure a Threat Prevention Rule Base with the Threat Prevention profile as the *Action* of the rule.
4. Install the Threat Prevention policy.

Threat Prevention Policy Layers

With R80.10 Gateways, you can create a Threat Prevention Rule Base with multiple Policy Layers. Each Policy Layer calculates its action separately from the other Layers. When a connection matches rules in more than one Layer, the gateway enforces the strictest action and settings.

For your convenience, you can divide the Policy Layers by Software Blades, services or networks.

Important - For Threat Emulation, the gateway takes the action and settings from the first layer matched.

Action Enforcement in Multiple-Layered Security Policies

These examples show how the Threat Prevention Software Blade resolves conflicting actions in different Layer.

Example 1

	Data Center Layer	Corporate LAN Layer

	Data Center Layer	Corporate LAN Layer
Rule matched	Rule 3	Rule 1
Profile action	Prevent	Detect

Enforced action: Prevent

Example 2

	Data Center Layer	Corporate LAN Layer
Rule matched	Rule 3	Rule 1
Profile action	Prevent	Detect
Exception for protection X	Inactive	-

Enforced action for protection X: Detect

Example 3

	Data Center Layer	Corporate LAN Layer
Rule matched	Rule 3	Rule 1
Profile action	Prevent	Detect
Override for protection X	Detect	-
Exception for protection X	Inactive	-

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

The action for the Corporate LAN Layer is Detect.

Enforced action for protection X: Detect.

Example 4

	Data Center Layer	Corporate LAN Layer
Rule matched	Rule 3	Rule 1
Profile action	Deep Scan all files	Process specific file type families: Inspect doc files and Drop rtf files.

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

Example 5

MIME nesting level and Maximum archive scanning time

The strictest action is:

Block combined with the minimum nesting level/scanning time, or

Allow combined with the maximum nesting level/scanning time, or

If both Block and Allow are matched, the enforced action is Block.

Example 6

UserCheck, DNS Trap

	HR Layer	Finance Layer	Data Center Layer 3
Rule matched	Rule 3	Rule 1	Rule 4
Profile action	Detect	Prevent	Detect
Configured page	Page A	Page B	Page C

The first Layer with the strictest action is enforced.

Enforced Action: Prevent with UserCheck Page B.

Threat Prevention Layers in Pre-R80 Gateways

When you upgrade to R80 or higher from earlier versions:

Gateways that have the IPS and Threat Prevention Software Blades enabled will have their Threat Prevention policies split into two parallel layers: IPS and Threat Prevention. The IPS Layer includes the ThreatCloud IPS protections. Core IPS protections stay in the Access Control Policy.

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

You can add more Layer to the two Layer created during upgrade.

All layers are evaluated in parallel.

Threat Prevention Rule Base

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

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

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

Parts of the Rules

The columns of a rule define the traffic that it matches and what is done to that traffic.

Number (No.)

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

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

Name

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

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

Protected Scope

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

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

Protected Scope objects can be:

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

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

Traffic Direction and Interface Type Settings

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

- **Inspect incoming files from**:

  Sends **only incoming** files from the specified interface type for inspection. Outgoing files are not inspected. Select an interface type from the list:

  - **External** - Inspect incoming files from external interfaces. Files from the DMZ and internal interfaces are not inspected.
  - **External and DMZ** - Inspect incoming files from external and DMZ interfaces. Files from internal interfaces are not inspected.
  - **All** - Inspect all incoming files from all interface types.
- **Inspect incoming and outgoing files** - Sends all incoming and outgoing files for inspection.

When you select the **Any** option in the **Protected Scope** section of a rule, the traffic direction and interface type are defined by the **Profile** assigned to that rule. If you add objects to the Protected Scope in a rule, files that match these objects are inspected for all connections.

Using Protected Scope with SPAN and TAP Configurations

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

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

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

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

Limitations and Troubleshooting

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

Protection

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

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

To add a protection to an exception:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the navigation tree, select a **Policy Layer**.
3. Right-click the rule and select **New Exception**.

   An exception sub-rule is added to the policy.
4. Right-click the **Protection/Site** cell and select **Add new items**.
5. From the list of Anti-Bot, Anti-Virus, or IPS protections, click the add button of protections to add to the exception.

   The protections are added to the exception sub-rule.
6. **Install Policy**.

To search for a malware in the Protection viewer:

1. Put your mouse in the **Protection/Site** column and click the plus sign to open the Protection viewer.
2. Select the protection category.
3. Enter the malware name in the search field.

Action

Action refers to how traffic is inspected.

- For **rules**, this is defined by the profile. The profile contains the configuration options for different confidence levels and performance impact ("Profiles Pane" on page 62).
- For **rule exceptions** and **exception groups**, the action can be set to **Prevent** or **Detect**.

To select a profile for a rule:

1. Click in the **Action** column.
2. Select an existing profile from the list, create a new profile, or edit the existing profile.

Threat Prevention Track Options

- **None** - Do not generate an alert.
- **Alert** - Generate a log and run a command, such as display a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in the **Menu > Global Properties > Log and Alert > Alerts**.
- **Packet Capture** - Adds raw IPS, Anti-Virus, Anti-Bot, Threat Emulation and Threat Extraction packet data to the Threat Prevention logs. Only blocked packets are added.

Install On

Select the gateways on which to install the rule. The default is All (all gateways that have a Threat Prevention blade enabled). Put your mouse in the column and a plus sign shows. Click the plus sign to open the list of available gateways and select. If you right-click a column in the table, you can add more columns to the table from the list that shows.

Creating Threat Prevention Rules

In This Section:

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

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

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

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

Configuring IPS Profile Settings

To configure IPS settings for a Threat Prevention profile:

1. In SmartConsole, select **Security Policies** > **Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.
   The **Profiles** page opens.
3. Right-click the profile, and click **Edit**.
4. From the navigation tree, click **IPS** > **Additional Activation**.
5. Configure the customized protections for the profile ("Additional Activation Fields" on page 37).
6. From the navigation tree, click **IPS** > **Updates**.
7. Configure the settings for newly downloaded IPS protections.
8. If you are importing IPS profiles from a pre-R80 deployment:
   a) From the navigation tree, click **IPS** > **Pre-R80 Settings**.
   b) Activate the applicable **Client** and **Server** protections.
   c) Configure the IPS protection categories to exclude from this profile.
   Note - These categories are different from the protections in the **Additional Activation** page.
9. Click **OK**.
10. **Install Policy**.

Additional Activation Fields

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

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

  These categories will only filter out or add protections that comply with the activation mode thresholds (Confidence, Severity, Performance).

  For example, if a protection is inactive because of its Performance rating, it will not be enabled even if its category is in **Protections to activate**.

Updates

There are numerous protections available in IPS. It takes time to become familiar with those that are relevant to you environment. Some are easily configured for basic security and can be safely activated automatically.

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

In the Threat Prevention profile, you can configure an updates policy for IPS protections that were newly updated. You can do this with the **IPS** > **Updates** page in the **Profiles** navigation tree. Select one of these settings for **Newly Updated Protections**:

- **Active - According to profile settings -** Protections are activated according to the settings in the **General** page of the Profile.

  Optional: Select **Set activation as staging mode** - The default action is Detect. You can change the action manually in the IPS **Protections** page ("Updating IPS Protections" on page 89).

  Click **Configure** to exclude protections from the staging mode.
- **Inactive** - Newly updated protections will not be activated

Pre R80 Settings

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

Protections Activation

Activate protections of the following types:

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

  If a network has only clients or only servers, you can enhance gateway performance by

deactivation of protections. If you select Client Protections and Server Protections, all protections are activated, except for those that are:

- Excluded by the options selected here
- Application Controls or Engine Settings
- Defined as Performance Impact — Critical

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

Configuring Anti-Bot Settings

To configure the Anti-Bot settings for a Threat Prevention profile:

1. In SmartConsole, select **Security Policies** > **Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.
   The **Profiles** page opens.
3. Right-click the profile, and click **Edit**.
4. From the navigation tree, click **Anti-Bot**.
5. Configure the Anti-Bot **UserCheck Settings**:
   - **Prevent** - Select the UserCheck message that opens for a **Prevent** action
   - **Ask** - Select the UserCheck message that opens for an **Ask** action
6. Click **OK** and **Install Policy**.

Blocking Bots

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

Protected Scope	Action	Track	Install On
Any	Optimized	Log Packet Capture	Policy Targets

To block bots in your organization:

1. In SmartConsole, click **Gateways & Servers**.
2. Enable the **Anti-Bot** Software Blade on the Gateways that protect your organization. For each Gateway:
   a) Double-click the Gateway object.
   b) In the **Gateway Properties** page, select the **Anti-Bot** Software Blade.
      The First Time **Activation** window opens.
   c) Select **According to the Anti-Bot and Anti-Virus policy**
   d) Click **OK**.
3. Click **Security Policies > Threat Prevention > Policy > Threat Prevention**.

You can block bots with the out-of-the-box Threat Prevention policy rule with the default **Optimized** Profile.

Alternatively, add a new Threat Prevention rule:

a) Click **Add Rule**.

A new rule is added to the Threat Prevention policy. The Software Blade applies the first rule that matches the traffic.

b) Make a rule that includes these components:

- **Name** - Give the rule a name such as **Block Bot Activity**.
- **Protected Scope -** The list of network objects you want to protect. By default, the **Any** network object is used.
- **Action -** The Profile that contains the protection settings you want ("Profiles Pane" on page 62). The default profile is **Optimized**.
- **Track -** The type of log you want to get when the gateway detects malware on this scope.
- **Install On** - Keep it as **Policy Targets** or select Gateways to install the rule on.

4. Install the Threat Prevention policy (see "Installing the Threat Prevention Policy" on page 28).

Monitoring Bot Activity

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

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

Name	Protected Scope	Action	Track	Install On
Monitor bot activity	Any	A profile that has **these** changes relative to the **Optimized** profile: **Confidence** (High\Medium\Low): **Detect\Detect\Detect**	Log	Policy Targets

To monitor all bot activity:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. Create a new profile:

a) From the **Threat Tools** section, click **Profiles**.

The **Profiles** page opens.

b) Right-click a profile and select **Clone**.

c) Give the profile a name such as **Monitoring_Profile**.

d) Edit the profile, and under **Activation Mode**, configure all confidence level settings to **Detect**.

e) Select the **Performance Impact** - for example, **Medium or lower**.

This profile detects protections that are identified as an attack with low, medium or high confidence and have a medium or lower performance impact.

3. Create a new rule:
   a) Click **Threat Prevention > Policy > Threat Prevention**.
   b) Add a rule to the Rule Base.
      The first rule that matches is applied.
   c) Make a rule that includes these components:
      - **Name** - Give the rule a name such as **Monitor Bot Activity**.
      - **Protected Scope -** Keep **Any** so the rule applies to all traffic in the organization.
      - **Action -** Right-click in this cell and select **Monitoring_Profile**.
      - **Track -** Keep **Log**.
      - **Install On** - Keep it as **Policy Targets** or choose Gateways to install the rule on.
4. Install the Threat Prevention policy (see "Installing the Threat Prevention Policy" on page 28).

Configuring Anti-Virus Settings

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

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

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

You can configure 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 Anti-Virus settings for a Threat Prevention profile:

1. In SmartConsole, select **Security Policies** > **Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.
   The **Profiles** page opens.
3. Right-click the profile, and click **Edit**.
4. From the navigation tree, click **Anti-Virus**.
5. Select the Anti-Virus **UserCheck Settings** options:
   - **Prevent** - Select the UserCheck message that opens for a **Prevent** action.
   - **Ask** - Select the UserCheck message that opens for an **Ask** action.

6. 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.
7. Select the applicable **Protocols** that Anti-Virus scans.
8. **Optional:** Configure how Anti-Virus inspects SMTP traffic.
   a) Click **Configure**.

      The **Anti-Virus 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.
9. Select **File Types**:
   - **Process file types known to contain malware**
   - **Process all file types**
   - **Process specific file types families**
10. To configure the specific file type families:
    a) Click **Configure**.

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

    c) Click **OK** to close the **File Types Configuration** window.
11. Click **OK** and close the Threat Prevention profile window.
12. **Install Policy**.

To enable Archive Scanning:

1. Select **Enable Archive 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 setting is **Allow**.
5. Click **OK** and close the Threat Prevention profile window.
6. **Install Policy**.

Blocking Viruses

To block viruses and malware in your organization:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
2. In the **General Properties** page, select the **Anti-Virus** Software Blade.
   The **First Time Activation** window opens.
3. Select **According to the Anti-Bot and Anti-Virus policy** and click **OK**.
4. Close the gateway Properties window and publish the changes.
5. Click **Security Policies** > **Threat Prevention** > **Policy** > **Threat Prevention**.
6. Click **Add Rule**.
   A new rule is added to the Threat Prevention policy. The Software Blade applies the first rule that matches the traffic.
7. Make a rule that includes these components:
   - **Name** - Give the rule a name such as **Block Virus Activity**.
   - **Protected Scope -** The list of network objects you want to protect. In this example, the **Any** network object is used.
   - **Action -** The Profile that contains the protection settings you want ("Profiles Pane" on page 62). The default profile is **Optimized**.
   - **Track -** The type of log you want to get when detecting malware on this scope. In this example, keep **Log** and also select **Packet Capture** to capture the packets of malicious activity. You will then be able to view the actual packets in **SmartConsole > Logs & Monitor > Logs**.
   - **Install On** - Keep it as **All** or choose specified gateways to install the rule on.
8. Install the Threat Prevention policy.

Configuring Threat Emulation Settings

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

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

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

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

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

To configure Threat Emulation settings for a Threat Prevention profile:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.

The **Profiles** page opens.

3. Right-click the profile, and click **Edit**.
4. From the navigation tree, click **Threat Emulation > General**.
5. Select the Threat Emulation **UserCheck Settings** options:
   - **Prevent** - Select the UserCheck message that opens for a **Prevent** action
   - **Ask** - Select the UserCheck message that opens for an **Ask** action
6. In the **Protected Scope** section, select an interface type and traffic direction option:
7. Select the applicable **Protocols** to be emulated.
8. 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.
9. **Optional:** 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.
10. Select the **File Types** to be emulated.
11. Click **OK** and close the Threat Prevention profile window.
12. Install the Threat Prevention policy.

Selecting the Threat Emulation Action

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. 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.

  Note - To estimate the system requirements and amount of file emulations for a network, go to sk93598 http://supportcontent.checkpoint.com/solutions?id=sk93598.

Preparing for Local or Remote Emulation

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

1. Open SmartConsole.
2. Create the network object for the Emulation appliance.
3. If you are running emulation on HTTPS traffic, configure the settings for HTTPS Inspection ("Using Threat Prevention with HTTPS Traffic" on page 121).
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.

Using Local or Remote Emulation

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

Note - Prepare the network for the Emulation appliance before you run the First Time Configuration Wizard ("Preparing for Local or Remote Emulation" on page 44).

To enable an Emulation appliance for Local and Remote emulation:

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

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

1. In SmartConsole, go to **Gateways & Servers** and double-click the Security Gateway.
   The **Gateway Properties** window opens.
2. From the **Network Security** tab, select **Threat Emulation**.
   The **Threat Emulation First Time Configuration Wizard** opens and shows the **Emulation Location** page.
3. Configure the Security Gateway for Remote Emulation:
   a) Select **Other 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.
7. Install the Threat Prevention policy on the Security Gateway and the Emulation appliance.

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.

To configure the virtual environment settings for the profile:

1. From the Threat Prevention profile navigation tree, select **Threat Emulation** > **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**
4. Click **OK** and close the Threat Prevention profile window.
5. Install the Threat Prevention policy.

File Type Settings

To configure the file type settings for a profile:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.
3. Double-click the Threat Prevention profile.
4. From the navigation tree, select **Threat Emulation**.
5. From the **File Types** section, select **Process specific file types families**.
6. Click **Configure**.

   The **File Types Configuration** window opens.
7. 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.
8. 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.

9. **Install Policy**.

Excluding Emails

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. From the Threat Prevention profile navigation tree, select **Threat Emulation** > **Excluded Mail Addresses**.
2. In the **Recipients** section, you can click the Add button and enter one or more emails.
   Emails and attachments that are sent to these addresses are not sent for emulation.
3. In the **Senders** section, you can click the Add button and enter one or more emails.
   Emails and attachments that are received from these addresses are not sent for emulation.
4. Click **OK** and close the Threat Prevention profile window.
5. Install the Threat Prevention policy.

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.
- **Best practice -** 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.

Note - MTA configuration also applies to VSX gateways.

To use the Security Gateway as an MTA:

1. Enable the Security Gateway as an MTA ("Enabling MTA on the Security Gateway" on page 47).
2. Configure the network to forward emails to the MTA ("Configuring the Network to Use an MTA" on page 47).

Note - When you enable a gateway as an MTA, an implied rule is created which opens port 25 on the gateway. To disable this implied rule, see sk110758 http://supportcontent.checkpoint.com/solutions?id=sk110758.

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. In SmartConsole, go to **Gateways & Servers** and 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 48).
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 115).
7. Click **OK** and then install the Threat Prevention 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 116), 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. In SmartConsole, go to **Gateways & Servers** and 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 `192.0.2.0`
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 Threat Prevention policy.

Troubleshooting Threat Emulation

Using MTA with ClusterXL

When you enable MTA with a ClusterXL deployment, make sure that the standby cluster member is also able to connect to one or more of the next hops. If not, it is possible that when there is a failover to the standby member, emails in the MTA do not go to their destination.

Configuring Postfix for MTA

The Check Point MTA uses Postfix, and you can add custom user-defined Postfix options http://www.postfix.org/postconf.5.html (http://www.postfix.org/postconf.5.html).

To add Postfix options:

1. From the Security Gateway CLI, create the file `$FWDIR/conf/mta_postfix_options.cf`
2. Edit the file and add the definitions.
3. Save the file.
4. Install the Threat Prevention policy.

Problems with Email Emulation

Best Practice - If you are blocking SMTP traffic with the Prevent action, we recommend that you enable MTA on the Security Gateway ("Using an MTA" on page 46). If you do not enable the MTA, it is possible that emails are dropped and do not reach the mail server.

Configuring Threat Extraction Settings

To configure Threat Extraction settings for a Threat Prevention profile:

1. In the **Security Policies** view > **Threat Tools** section, click **Profiles**.
2. Right-click a profile and select **Edit**.
   The **Profiles** properties window opens.
3. On the **General Policy** page in the **Blade Activation** area, select **Threat Extraction**.
4. On the **Threat Extraction** > **General** page, configure:

   UserCheck Settings

   - **Allow the user to access the original file**
   - **Allow access to original files that are not malicious according to Threat Emulation**

     Note - This option is only configurable when the Threat Emulation blade is activated in the **General Properties** pane of the profile.
   - **UserCheck Message**

     Select a message to show the user when the user receives the clean file. In this message, the user selects if they want to download the original file or not. To select the success or cancelation messages of the file download, go to Manage & Settings > **Blades** > **Threat Prevention** > **Advanced Settings** > **UserCheck** (**"Selecting Approved and Cancel UserCheck Messages" on page 84**). You can create or edit UserCheck messages on the UserCheck page ("Threat Prevention and UserCheck" on page 79).
   - Optional: To give the user access to the original email, click **Insert Field**, and select **Send Original Mail**.

     Send Original Mail is added to the message body.

   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, JavaScript, images and so on.

- **Convert to PDF** - selected by default

  Converts the file to PDF, and keeps text and formatting.

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

Extraction Settings

- **Process all files** - selected by default
- **Process malicious files when the confidence level is:**

  Set a low, medium or high confidence level. This option is only configurable when the Threat Emulation blade is activated in the **General Properties** pane of the profile.

File Types

- **Process all supported file types** - selected by default
- **Process specific file type families -**

  Click **Configure** to select if you want Threat Extraction support for only some file types from the list. This list includes only specified file types that the administrator selected. To change the selection, go to the **Manage & Settings** view > **Blades** > **Threat Prevention** > **Advanced Settings** > **Threat Extraction** > **Configure File Type Support**.

Notes:

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

5. On the **Exclude/Include Users** page, configure these settings:
   - **Scan all emails** - selected by default

     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 the **Application menu** > **Global Properties** > **User Directory**, make sure that you have selected the **Use User Directory for Security Gateways** option.
6. In **Threat Tools** > **Profiles** > **Threat Extraction** > **Advanced**, configure these settings:

   Logging

   - **Log only those files from which threats were extracted** - selected by default
   - **Log every file**

   Threat Extraction Exceptions

   - **Corrupted attachments**

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 attachments**

  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 attachments**

  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.

7. Click **OK**.

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

Configuring Threat Extraction on the Security Gateway

1. In the **Gateways & Servers** view, open the **gateway properties** > **Threat Extraction** page.
2. Set the **Activation Mode** to **Active**.
3. In the **Resource Allocation** section, configure the resource settings.
4. Click **OK**.
5. **Install Policy**.

Configuring Threat Extraction in a Cluster

1. In the **Gateways & Servers** view, right-click the cluster and click edit.
2. Open the **ClusterXL and VRRP** page.
3. Select **High Availability**.
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 **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 **Threat Extraction**.
8. Set the **Activation Mode** to **Active**.
9. In the resource, allocate disk space resources.
10. Click **OK**.
11. **Install Policy**.

Threat Extraction Statistics

You can see Threat Extraction statistics in the CLI:

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

Using the Gateway CLI

The R80.10 gateway has a Threat Extraction menu to:

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

To use the Threat Extraction command line:

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

Option	Description
`debug`	Controls debug messages.

Option	Description
`queues`	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: • Number of pending requests from the MTA to the `scrubd` daemon • Maximum number pending requests from the MTA to the `scrubd` daemon • Current number of pending requests from `scrubd` to `scrub_cp_file_convert` • Maximum number of pending requests from scrubd to `scrub_cp_file_convert`
`send_orig_email`	Sends original email to recipients. To send the original email get: • The reference number - Click on link in the email received by the user. • The email ID - Found in the **Logs & Monitor** logs or debug logs.
`bypass`	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.
`counters`	shows and resets counters.
`update`	manages updates from the download center
`send_orig_file`	sends original file by email

Using the Web API

In addition to Threat Extraction which is performed on the user's computer, you can use the Threat Extraction API to build a client that sends files to the gateway for cleaning. For example, if you get files delivered on a USB stick or CD, or sent to a database. You can put the stick/CD in your workstation, open the client and use it to send the files to the gateway for Threat Extraction.

To enable the Threat Extraction Web API:

1. In SmartConsole, double-click the gateway.
2. From the navigation tree, select **Threat Extraction**.
3. Select **Enable API**.

Troubleshooting the Threat Extraction Blade

This section covers common problems and solutions.

The Threat Extraction blade fails to extract threats from emails belonging to LDAP users

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

Mails with threats extracted do not reach recipients

1. Make sure the gateway passed the MTA connectivity test during the First Time Configuration Wizard.
   a) Disable then enable the Threat Extraction blade.
   b) Complete the First Time Configuration Wizard again.
   c) Make sure the wizard passes the connectivity test.
2. Test the connection to the target MTA.
   a) Open a command prompt on the gateway.
   b) Telnet to port 25 of the designated Mail Transfer Agent.

Threat Extraction fails to extract threats from emails

1. Open **SmartConsole** > **Gateway Properties** > **Mail Transfer Agent**.
2. Make sure you selected **Enable as Mail Transfer Agent**.
3. Access the organizations mail relay. Configure the Threat Extraction gateway as the relay's next hop.

Users have stopped receiving emails

1. On the gateway command line interface, run: `scrub queues`.
   If the queues are flooded with requests, the Threat Extraction load is too high for the gateway.
   a) Bypass the scrub daemon.
      Run: `scrub bypass on`.
   b) Ask affected users if they are now receiving their emails. If they are, reactivate Threat Extraction.
      To reactivate, run: `scrub bypass off`.
2. Make sure the queue is not full.
   a) Run:
      ```
      /opt/postfix/usr/sbin/postqueue -c /opt/postfix/etc/postfix/ -p
      ```
   b) If the queue is full, empty the queue.
      Run:
      ```
      /opt/postfix/usr/sbin/postsuper -c /opt/postfix/etc/postfix/ -d ALL
      ```
      Emptying the queue loses the emails
   c) To prevent losing important emails, flush the queue. Flushing forcefully resends queued emails.
      Run:
      ```
      /opt/postfix/usr/sbin/postfix -c /opt/postfix/etc/postfix/ flush
      ```
3. If queues remain full, make sure that the MTA is not overloading the gateway with internal requests. The MTA should be scanning only emails from outside of the organization.

Users have no access to original attachments

Make sure users are able to access the UserCheck portal from the e-mail they get when an attachment is cleaned.

1. Click the link sent to users.
2. Make sure that the UserCheck Portal opens correctly.
3. If users are not able to access the UserCheck portal but see the Gaia portal instead, make sure that accessibility to the UserCheck portal is correctly configured.
   a) In **SmartConsole**, open **Gateway Properties > UserCheck**.
   b) Under **Accessibility**, click **Edit**.
   c) Make sure the correct option is selected according to the topology of the gateway.
4. Open **CPView**.
   Make sure the `access to original attachments` statistic is no longer zero.

Attachments are not scanned by Threat Extraction

The `scanned attachment` statistic in CPView fails to increment.

On the gateway:

1. Make sure that the disk or directories on the gateway are not full.
   a) Run `df -h` on the root directory of the disk
   b) Run `df -h` on: `/var/log`
2. Make sure directories used by Threat Extraction can be written to.
   Run:
   a) `touch /tmp/scrub/test`
   b) `touch /var/log/jail/tmp/scrub/test`
   c) `touch $FWDIR/tmp/email_tmp/test`

CPView shows Threat Extraction errors

In `CPview > Software-blades > Threat-extraction > File statistics`, the number for `internal errors` is high compared to the total number of emails.

1. Open the **Logs & Monitor** view.
2. In the query search bar, enter: blade: Threat Extraction.
3. Right-click the table heading, and select **Edit Profile**.
4. Add **Threat Extraction Activity** to the **Selected Fields**.

If the ThreatSpect engine is overloaded or fails while inspecting an attachment, a log is generated. By default, attachments responsible for log errors are still sent to email recipients. To prevent these attachments being sent, set the engine's fail-over mode to **Block all connections**.

1. Go to **Manage & Settings** > **Blades** > **Threat Prevention** > **Advanced Settings**.
2. In the **Fail Mode** section, select **Block all connections (fail-close)**.

The Threat Extraction blade continues to scan, but attachments that generate internal system errors are prevented from reaching the recipient.

Corrupted attachments cannot be cleaned, and by default generate log entries in the Logs & Monitor view. Corrupted attachments are still sent to the email recipient. To prevent corrupted attachments from reaching the recipient:

1. In SmartConsole, open **Threat Prevention > Profiles > Profile > Threat Extraction Settings >**.
2. In the **Threat Extraction Exceptions** area, select **Block** for attachments.

Attachments look disordered after conversion to PDF

1. In **Security Policies** > **Threat Prevention** > **policy,** right-click the **Action** column and select **Edit**.
2. In **Threat Extraction** > **File Types**, select **Process specific file types** and click **Configure**.
   The **File Types Configuration** window opens.
3. For the pdf file type, set the extraction method to **clean**.

To check MTA connectivity on a Virtual System:

1. Open an ssh connection to the gateway.
2. Go to expert mode.
3. Run `vsenv <VS #>`
4. Run `touch $FWDIR/conf/scrub_connectivity_results.txt`
5. Run `/etc/fw/scripts/scrub_cvsenvheck_connectivity.sh <mail server IP> $FWDIR/conf/scrub_connectivity_results.txt`
6. Check `$FWDIR/conf/scrub_connectivity_results.txt` and see the result

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:

To set the Malware DNS Trap parameters for the profile:

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

To set the Malware DNS Trap parameters for a gateway:

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

Exception Rules

If necessary, you can add an **exception** directly to a rule. The object in the **Protected Scope** column can have a different **Action** from the specified Threat Prevention rule. Here are some examples of exception rules:.

- A profile that only detects protections. You can set one or more of the protections for a user to **Prevent**.
- The Research and Development (R&D) network protections are included in a profile with the **Prevent** action. You can set that network to **Detect**.

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

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

You can expand or collapse the rule exceptions by clicking on the minus or plus sign next to the rule number in the **No**. column.

To add an exception to a rule:

1. In the **Policy** pane, select the rule to which you want to add an exception.
2. Click **Add Exception.**
3. Select the **Above**, **Below**, or **Bottom** option according to where you want to place the exception.
4. Enter values for the columns. Including these:
   - **Protected Scope -** Change it to reflect the relevant objects.
   - **Protection** - Click the plus sign in the cell to open the Protections viewer. Select the protection(s) and click **OK**.
5. **Install Policy**.

Disabling a Protection on a Specified Server

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

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

Name	Protected Scope	Protection/Site	Action	Track	**Install On**
Monitor Bot Activity	Any	- N/A	A profile based on the Optimized profile, with these changes: **Confidence** (Low/Medium/High): Prevent/Prevent/Prevent	Log	Policy Targets
Exclude	Server_1	Backdoor.Win32.Agent.AH	Detect	Log	Server_1

To add an exception to a rule:

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

     Note - To add EICAR files as exceptions, you must add them as Whitelist Files ("Adding a File to the Whitelist" on page 101). When you add EICAR files through Exceptions in Policy rules, the gateway still blocks them.
   - **Action -** Keep it as **Detect**.
   - **Track** - Keep it as **Log**.
   - **Install On** - Keep it as **Policy Targets** or select specified gateways to install the rule on.
6. **Install Policy**.

Blade Exceptions

You can also configure an exception for an entire blade.

To configure a blade exception:

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

Creating Exceptions from IPS Protections

To create an exception from an IPS protection:

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

Exception Groups

An exception group 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:

Option	Meaning
New	Creates a new exception group.
Edit	Modifies an existing exception group.
Delete	Deletes an exception group.
Search	Search for an exception group.

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

To create an exception group:

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

- **Automatically attached to all rules** - This exception group applies to all Threat Prevention rules.

4. Click **OK**.
5. Install the Threat Prevention policies.

Adding Exceptions to Exception Groups

To use exception groups, you must add exception rules to them ("Parts of the Rules" on page 32).

To add exceptions to an exception group:

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

Adding Exception Groups to the Rule Base

You can add exception groups to Threat Prevention rules. This only applies to exception groups that are configured to **Manually attach to a rule**.

To add an exception group to the Rule Base:

1. Click **Security Policies** > **Threat Prevention** > **Policy**.
2. Right-click the rule and select **Add Exception Group** > **<group name>**.
3. Install the Threat Prevention policies.

Creating Exceptions from Logs or Events

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

To update a rule exception or global exception from a log:

1. Click **Logs & Monitor** > **Logs** tab.
2. Right-click the log and select **Add Exception**.
3. Configure the settings for the exception.
4. Click **OK**.
5. In the New Exception Rule window:
   - To show the exception in the policy, click **Go to**
   - Otherwise, click **Close**
6. **Install Policy**.

Threat Prevention Profiles

In This Section:

Introducing Profiles

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

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

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

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

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

A *profile* is a set of configurations based on:

- *Activation settings* (prevent, detect, or inactive) for each *confidence level* of protections that the ThreatSpect engine analyzes
- IPS Settings
- Anti-Bot Settings
- Anti-Virus Settings
- Threat Emulation Settings
- Threat Extraction Settings
- 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.

SmartConsole includes these default Threat Prevention profiles:

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

Optimized Protection Profile Settings

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

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

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

Profiles Pane

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

Option	Meaning
New	Creates a new profile.
View	Shows an existing profile.

Option	Meaning
Edit	Modifies an existing profile.
Clone	Creates a copy of an existing profile.
Delete	Deletes a profile.
Where Used	Shows you reference information for the profile.
Search	Searches for a profile.
Last Modified	Shows who last modified the selected profile, when and on which client.

Performance Impact

Performance impact is how much a protection affects the gateway performance. Some activated protections might cause issues with connectivity or performance. You can set protections to not be prevented or detected if they have a higher impact on gateway performance.

There are three options:

- High or lower
- Medium or lower
- Low

Severity

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

There are three degrees of severity:

- Low or above
- Medium or above
- High or above

Activation Settings

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

Confidence Level

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

Creating Profiles

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

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

To create a new Threat Prevention profile:

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

Cloning Profiles

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

To clone a Threat Prevention profile:

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

Editing Profiles

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

To edit a profile:

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

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**.

Importing and Exporting Profiles

IPS lets you import and export profiles using the `ips_export_import` command from the CLI. Supported in Security Management Server and Multi-Domain Security Management environments, the command lets you copy profile configurations between management servers of the same version.

The exported profile is stored in a tar archive. The archive includes all protection settings but does not include:

- Network Exceptions
- Network object information that is specified in the protection settings

On a Multi-Domain Server, you must use one of these methods to set the environment in which the command will run:

- Run `mdsenv` to set the environment (Multi-Domain Server or specific Domain Management Server) where the IPS profile is configured.
- Use `-p <ip>` to enter the IP address of the Multi-Domain Server or Domain Management Server where the IPS profile is configured.

To export an IPS profile:

- From the command line, run:

```
ips_export_import export <profile-name> [-o <export-file-name>] [-p <ip>]
```

You must enter the exact name of the profile that you want to export.

The archive will be named `<profile-name>.tar` and is saved to your present working directory. You can also use the `-o <file-name>` to give the archive a specific name.

To import an IPS profile:

- From the command line, run:

```
ips_export_import import <new-profile-name> -f <file-name> [-p <ip>]
```

You must enter a name for the profile and the location of the archive. You can either import an archive that is in your present working directory or enter the exact location of the archive that you want to import.

Deleting Threat Prevention Profiles

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

To delete a profile:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.
   The **Profiles** page opens.
3. Right-click the profile, and click **Delete**.
   A window opens and shows a confirmation message.
4. Click **Yes**.
   If the profile is used by another object, you cannot delete it. The error message is shown in the Tasks window.
5. **Install Policy**.

To show the objects that use a profile:

1. From the **Profiles** page, select the profile.
   The Summary
2. From the **Where Used** section in the **Summary** tab, click **Where Used**.
   The **Where Used** window opens and shows the profile.
3. Right click the rule and select **View in policy**.

Showing Changes to a Threat Prevention Profile

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

To show the Audit log for a Threat Prevention profile:

1. In SmartConsole, click Logs & Monitor.
2. Click the **Audit** tab, or press **CTRL + T** and click **Open Audit Logs View**.
3. In **Enter search query**, enter the name of the profile.
4. To refine the search:
   a) Right-click the **Object Type** column heading and select **Add Filter**.
   b) Enter **Threat Prevention Profile**.
   c) Click the filter to add it to the search.
   d) Click **OK**.

   The search results are filtered to Threat Prevention profiles.
5. To see more information about the changes to a profile, double-click the Audit log.

Monitoring Threat Prevention

In This Section:

Log Sessions

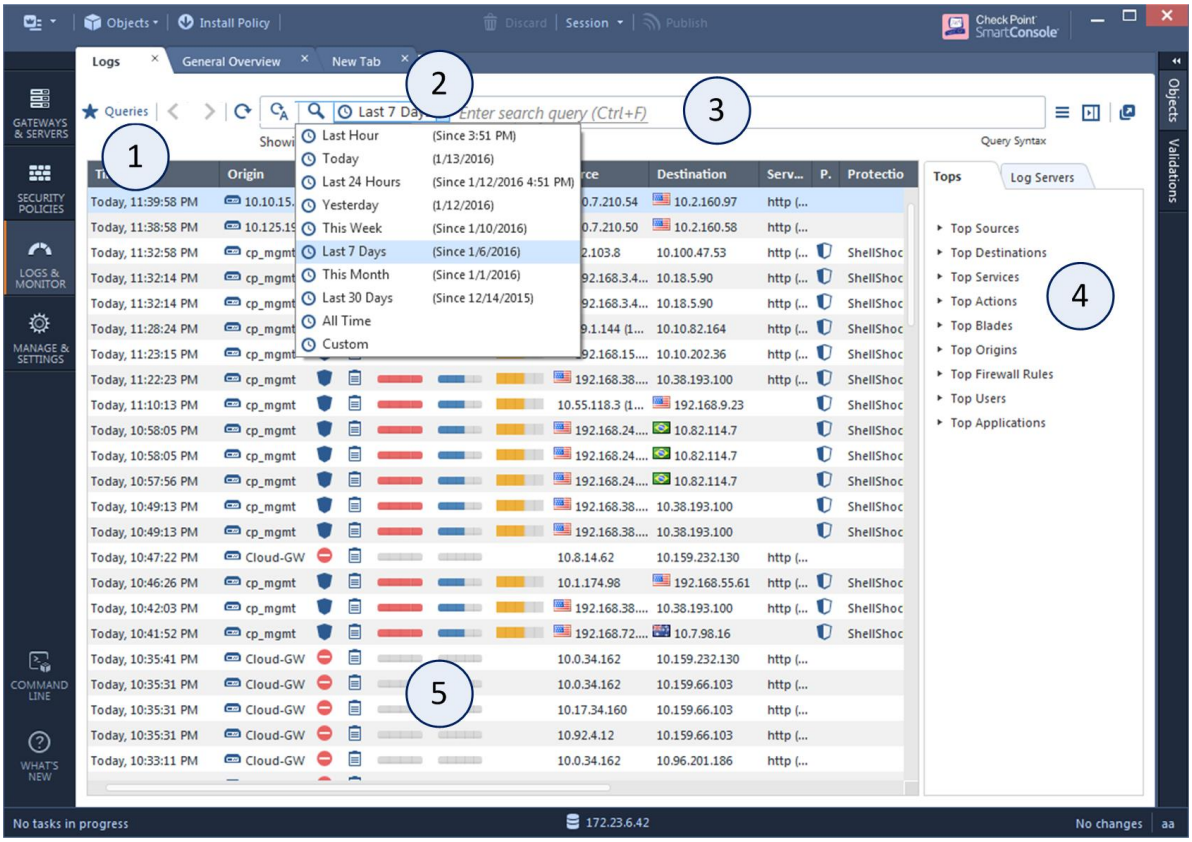
Gateway traffic generates a large amount of activity. To make sure that the amount of logs is manageable, by default, logs are consolidated by session. A session is a period that starts when a user first accesses an application or site. During a session, the gateway records one log for each application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

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

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

Using the Log View

This is an example of the **Log** view.



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

Viewing Threat Prevention Rule Logs

To see logs generated by a specified rule:

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

Predefined Queries

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

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

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

Creating Custom Queries

Queries can include one or more criteria. To create custom queries, use one or a combination of these basic procedures:

- Right-click columns in the grid view and select **Add Filter**.
- Click in the **Query search bar** and select the fields and filter criteria for those fields.
- Manually enter filter criteria in the **Query search bar**.

To create a new custom query, run an existing query, and use one of these procedures to change it. You can save the new query in the **Favorites** list.

When you create complex queries, the log search tool suggests, or automatically enters, an appropriate Boolean operator. This can be an implied AND operator, which does not explicitly show.

Selecting Query Fields

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

To select field criteria:

1. If you start a new query, click **Clear**  to remove query definitions.
2. Put the cursor in the Query search bar.
3. Select a criterion from the drop-down list or enter the criteria in the Query search bar.
   The query runs automatically.

Selecting Criteria from Grid Columns

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

To select query criteria from grid columns:

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

To enter more criteria, use this procedure or other procedures.

Manually Entering Query Criteria

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

As you type, the **Search** shows recently used query criteria or full queries. This helps you to search. To use these suggestions, select them from the drop-down list. If you make a syntax error in a query, the **Search** shows a helpful error message that identifies the error and suggests a solution.

Packet Capture

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

The packet capture option is activated by default.

To deactivate packet capture:

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

To see a packet capture:

1. In SmartConsole, go to the **Logs & Monitor** view.
2. Open the log.
3. Click the link in the **Packet Capture** field.
   The **Packet Capture Viewer Output** window opens.
4. Optional: Click **Save** to save the packet capture data as a text file.

Threat Analysis in the Logs & Monitor View

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

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

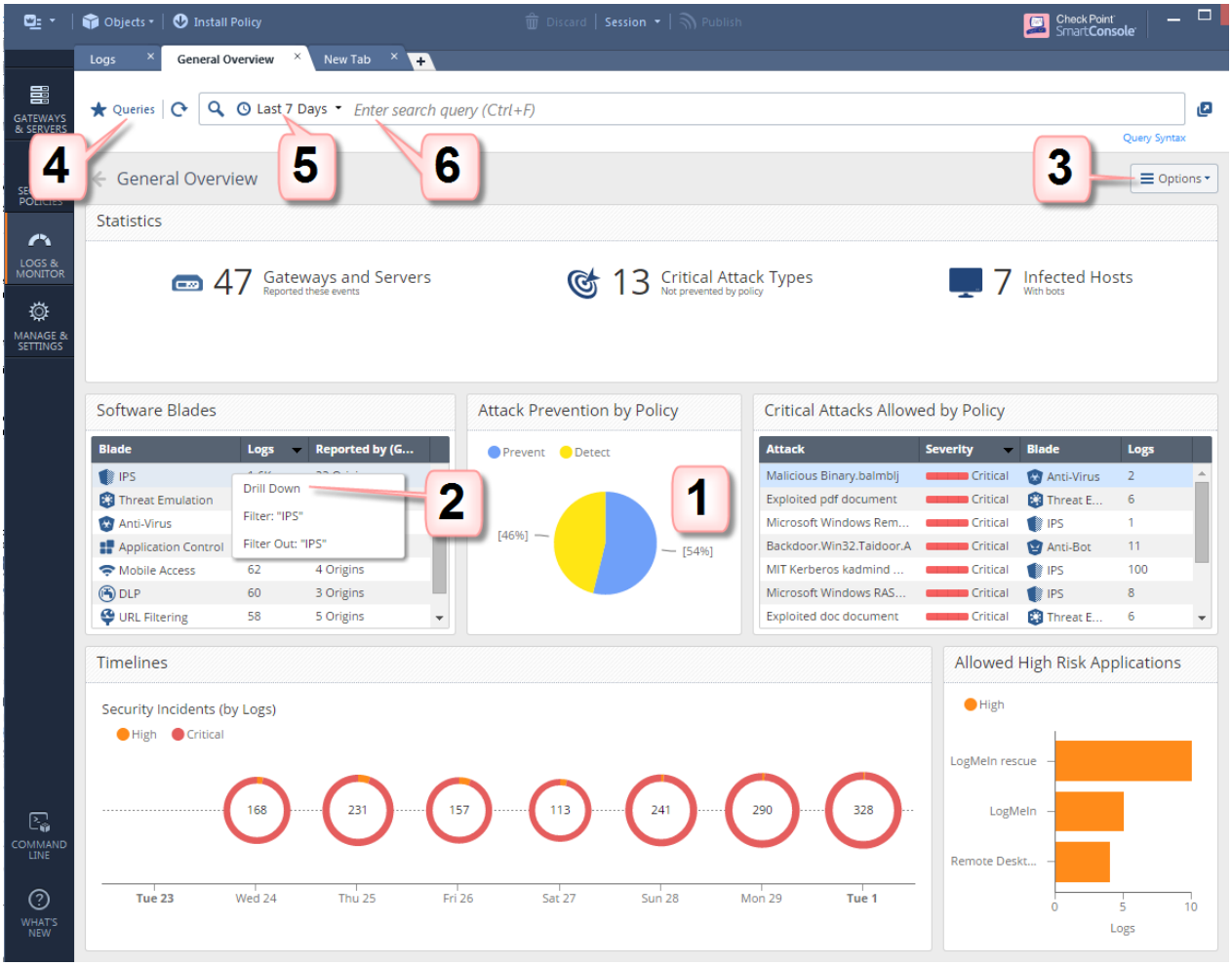
- Real-time and historical graphs and reports of threat incidents
- Graphical incident timelines for fast data retrieval
- Easily configured custom views to quickly view specified queries
- Incident management workflow
- Reports to data owners on a scheduled basis

Views

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

SmartConsole comes with several predefined views. You can create new views that match your needs, or you can customize an existing view.

In the Logs & Monitor view, clicking the (+) tab opens a catalog of all views and reports, predefined and customized. Click a view to open it.



Item	Description
1	**Widget**- The output of a query. A Widget can show information in different formats, for example, a graph or a table.
2	**Drill Down** - To find out more about the events, double-click a widget to drill down to a more specific view or raw log files.
3	**Options** - Customize the view
4	**Queries** - Predefined and favorite search queries
5	**Time Period** - Specify the time periods for the view.

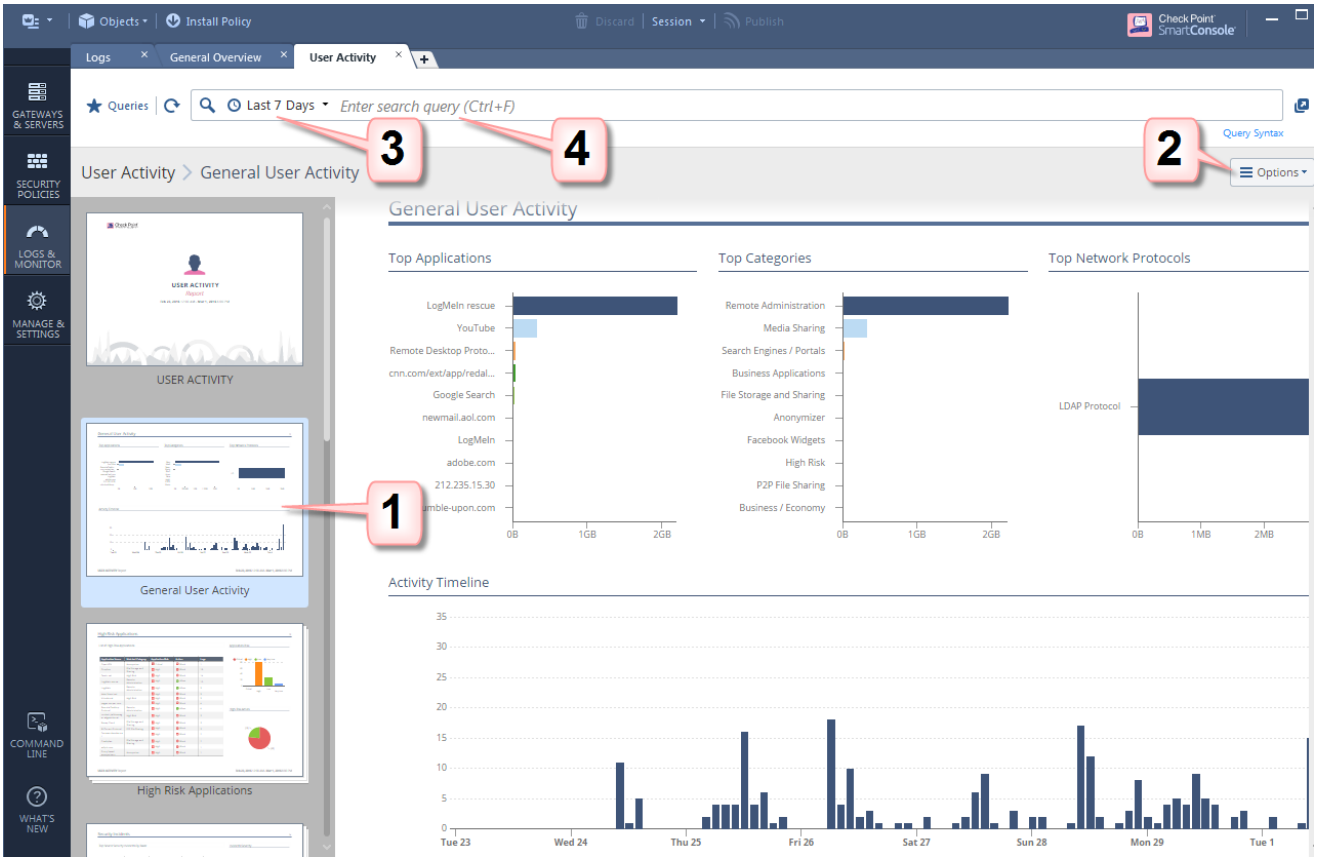
Item	Description
6	**Query search bar** - Define custom queries using the GUI tools, or manually entering query criteria. Shows the query definition for the most recent query.

For more information on using and customizing Reports, see the *Logging and Monitoring R80.10 Administration Guide*.

Reports

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

In the Logs & Monitor view, clicking the (+) tab opens a catalog of all views and reports, predefined and customized. Click a report to open it.



Item	Description
1	**Preview bar** - A report is divided onto pages, usually, one view on one page. Editing a report is done per page, in the same way as you edit a view.
2	**Options** - Customize, and generate a report.
3	**Time Period** - Specify the time periods for the report.
4	**Query Search bar** - Define custom queries using the GUI tools, or manually entering query criteria. Shows the query definition for the most recent query.

For more information on using and customizing Reports, see the *Logging and Monitoring R80.10 Administration Guide.*

The Check Point ThreatCloud

In This Section:

Check Point ThreatCloud is a dynamically updated service that is based on an innovative global network of threat sensors and organizations that share threat data and collaborate to fight against modern malware. Customers can send their own threat data to the ThreatCloud and benefit from increased security and protection and enriched threat intelligence. The ThreatCloud distributes attack information, and turns zero-day attacks into known signatures that the Anti-Virus Software Blade can block. The Security Gateway does not collect or send any personal data.

Participation in Check Point information collection is a unique opportunity for Check Point customers to be a part of a strategic community of advanced security research. This research aims to improve coverage, quality, and accuracy of security services and obtain valuable information for organizations.

The ThreatCloud repository contains more than 250 million addresses that were analyzed for bot discovery and more than 2,000 different botnet communication patterns. The ThreatSpect engine uses this information to classify bots and viruses.

For the reputation and signature layers of the ThreatSpect engine, each Security Gateway also has:

- A local database, the Malware database that contains commonly used signatures, URLs, and their related reputations. You can configure automatic or scheduled updates for this database.
- A local cache that gives answers to 99% of URL reputation requests. When the cache does not have an answer, it queries the ThreatCloud repository.
  - For Anti-Virus - the signature is sent for file classification.
  - For Anti-Bot - the host name is sent for reputation classification.

Access the ThreatCloud repository from:

- **SmartConsole** - You can add specific malwares to rule exceptions when necessary. From the Threat Prevention Rule Base in SmartConsole, click the plus sign in the **Protection** column in the rule exceptions, and the Protection viewer opens.
- **Threat Wiki** - A tool to see the entire Malware database. Open Threat Wiki in SmartConsole or access it from the Check Point website.

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:

```
<entry engineType="3" sigID="-1" attackName="CheckPoint - Testing Bot"
sourceIP="7a1ec646fe17e2cd" destinationIP="d8c8f142" destinationPort="80"
host="www.checkpoint.com"
```

```
path="/za/images/threatwiki/pages/TestAntiBotBlade.html"
numOfAttacks="20" />
```

This is an example of an event that was detected by a Check Point Security Gateway. It includes the event ID, URL, and external IP addresses. Note that the data does not contain confidential data or internal resource information. The source IP address is obscured. Information sent to the Check Point Lab is stored in an aggregated form.

Configuring Check Point ThreatCloud for a Specified Gateway

To configure the Security Gateway to share information with the Check Point ThreatCloud:

1. Double-click the Security Gateway.
   The gateway window opens and shows the **General Properties** page.
2. Configure the settings for the Anti-Bot and Anti-Virus Software Blades.
   a) From the navigation tree click **Anti-Bot and Anti-Virus**.
      The **Anti-Bot and Anti-Virus** page opens.
   b) To configure a Security Gateway to share Anti-Bot and Anti-Virus information with the ThreatCloud, select **Share anonymous attack information with Check Point ThreatCloud**.
   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. Configure the settings for the IPS Software Blade.
   a) From the navigation tree click **IPS**.
      The **IPS** page opens.
   b) To configure a Security Gateway to share IPS information with the ThreatCloud, select **Help Improve Check Point Threat Prevention product by sending anonymous information about feature usage, infections details and product customizations**.
5. Click **OK**.

Check Point ThreatCloud Network

By default, all gateways send threat information to the ThreatCloud.

You can change this default behavior in SmartConsole.

To configure all gateways not to send information to the ThreatCloud:

1. Open **Global Properties > Security Management Access**.
2. In the **Internet Access** area, clear this setting: **Improve product experience by sending data to Check Point**.
3. Click **OK**.
4. Restart SmartConsole.
5. **Install Policy**.

Scheduling Updates

You can change the default automatic schedule for when updates are automatically downloaded and installed. If you have Security Gateways in different time zones, they are not synchronized when one updates and the other did not yet update.

To configure Threat Prevention scheduled updates:

1. In SmartConsole, go to the **Security Policies** page and select **Threat Prevention**.
2. In the **Threat Tools** section of the Threat Prevention Policy, click **Updates**.
3. In the section for the applicable Software Blade, click **Schedule Update**.
   The **Scheduled Update** window opens.
4. Make sure **Enable <feature> scheduled update** is selected.
5. Click **Configure**.
6. In the window that opens, set the **Update at** time and the frequency:
   - **Daily** - Every day
   - **Days in week** - Select days of the week
   - **Days in month** - Select dates of the month
7. Optional, for IPS only:
   - Select **Perform retries on update failure -** lets you configure how many tries the Scheduled Update makes if it does not complete successfully the first time.
   - Select **On successful update perform Install Policy** - automatically installs the policy on the devices you select after the IPS update is completed. Click **Configure** to select these devices.
8. Click **OK**.
9. Click **Close**.
10. **Install Policy**.

The ThreatCloud Intellistore

ThreatCloud Intellistore is a threat intelligence marketplace which supplements ThreatCloud and provides intelligence data from leading cyber security vendors. The data includes threat information such as IPs, domains, URLs, command and control networks, DOS attacks and more.

Intellistore classifies the information feeds according to specific geographies, types of attacks or industries, and you can select the feeds that best suit your needs.

A security feed represents specialized intelligence gathered and analyzed by the vendors. ThreatCloud translates these feeds into protections which run on Security Gateways.

Threat Prevention and UserCheck

In This Section:

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

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

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

For more about using UserCheck objects and settings, see the UserCheck chapters in the *R80.10 Data Loss Prevention Administration Guide* http://supportcontent.checkpoint.com/documentation_download?ID=TBD.

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:

Option	Meaning
New	Creates a new UserCheck object
Edit	Modifies an existing UserCheck object
Delete	Deletes an UserCheck object
Clone	Clones the selected UserCheck object

These are the default UserCheck messages:

Name	Action Type	Description
Software Blade Blocked	Block	Shows when a request is blocked.
Company Policy Software Blade	Ask	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.
Software Blade Success Page	Approve	Shows when the action for the rule is **Approve**. From the Success page you can download the links to the original file or receive the original email.
Cancel Page Anti-Malware	Cancel	The **Ask** and **Approve** pages include a **Cancel** button that you 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
- **Email** - How the message shows in an email
- **Agent -**How the message shows in the UserCheck agent

Configuring the Security Gateway for UserCheck

Enable or disable UserCheck directly on the Security Gateway. Make sure that the UserCheck is enabled on each Security Gateway in the network.

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

To configure UserCheck on a Security Gateway:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
   The **Gateway Properties** window opens.
2. From the navigation tree, click U**serCheck**.
   The **UserCheck** page opens.
3. Make sure **Enable UserCheck for active blades** is selected
4. In the **UserCheck Web Portal** section:
   In the **Main URL** field, enter the primary URL for the web portal that shows the UserCheck notifications.
   If users connect to the Security Gateway remotely, make sure that the Security Gateway internal interface (in the **Network Management** page) is the same as the Main URL.
   Note - The **Main URL** field must be manually updated if:
   - The Main URL field contains an IP address and not a DNS name.
   - You change a gateway IPv4 address to IPv6 or vice versa.
5. **Optional:** Click **Aliases** to add URL aliases that redirect different hostnames to the **Main URL**.
   The aliases must be resolved to the portal IP address on the corporate DNS server
6. In the **Certificate** section, click **Import** to import a certificate that the portal uses to authenticate to the Security Management Server.

By default, the portal uses a certificate from the Check Point Internal Certificate Authority (ICA). This might generate warnings if the user browser does not recognize Check Point as a trusted Certificate Authority. To prevent these warnings, import your own certificate from a recognized external authority.

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

   Users are sent to the UserCheck portal if they connect:

   - **Through all interfaces**
   - **Through internal interfaces** (default)
     - **Including undefined internal interfaces**
     - **Including DMZ internal interfaces**
     - **Including VPN encrypted interfaces** (default)

       Note: Make sure to add a rule to the Firewall Rule Base that allows the encrypted traffic.
   - **According to the Firewall Policy**. Select this option if there is a rule that states who can access the portal.

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

   - **Through all interfaces** - necessary in VSX environment
   - **According to the Firewall Policy**
8. In the **Mail Server** section, configure a mail server for UserCheck. This server sends notifications to users that the Gateway cannot notify using other means, if the server knows the email address of the user. For example, if a user sends an email which matched on a rule, the Gateway cannot redirect the user to the UserCheck portal because the traffic is not http. If the user does not have a UserCheck client, UserCheck sends an email notification to the user.
   - **Use the default settings** - Click the link to see which mail server is configured.
   - **Use specific settings for this gateway** - Select this option to override the default mail server settings.
   - **Send emails using this mail server** - Select a mail server from the list, or click **New** and define a new mail server.
9. Click **OK**.
10. If there is encrypted traffic through an internal interface, add a new rule to the Firewall Layer of the Access Control Policy. This is a sample rule:

Source	Destination	VPN	Services & Applications	Action
Any	Security Gateway on which UserCheck client is enabled	Any	UserCheck	Accept

11. Install the Access Control Policy.

Creating Threat Prevention UserCheck Objects

Create a UserCheck Interaction object from the **UserCheck** page or Threat Prevention Software Blade profile **Settings**.

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

To show the Threat Prevention UserCheck objects:

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

To change text input modes:

From the menu-bar in the UserCheck object window, click the applicable option:

- **Source** - Enter HTML code
- **Design** - Enter text with formatting buttons and options

To create a new Threat Prevention UserCheck object:

1. From the **UserCheck** page, click **New** and select the object type.
   The window opens for the new UserCheck object.
2. Enter a **Name**.
3. **Optional:** Click **Language** and select one or more languages for the message.
   The default language for messages is English.
4. Enter the text for the message.
   - Title, subtitle, and body

   In the body of the message click these options for additional functionality:
   - **Insert Field** - Dynamic text such as: Original URL, Source IP address, and so on
   - **Insert User Input** - Such as: Confirm check box, Report Wrong Category and so on
5. **Optional:** Click **Add logo** to add a graphic to the message.
   The size of the graphic must be 176 x 52 pixels.
6. You can also click **Settings** from the navigation tree to configure one or more of these options:
   - Using a Fallback Action (on page 82)
   - Redirecting to an External Portal (on page 83)
   - Configuring User Interaction (on page 83)
7. Click **OK**.
8. Install the Threat Prevention policy.

Using a Fallback Action

Configure the default action for an Ask UserCheck object if the user cannot see the message. You can select one of these options:

- **Drop** - The connection or traffic is dropped and does not enter the internal network
- **Accept** - The connection or traffic is accepted and enters the internal network

To configure a fallback action for an Ask object:

1. From the navigation tree, click **Settings**.
2. In the **Fallback Action** section, select to **Drop** or **Accept** traffic when the user cannot see the UserCheck message.

Redirecting to an External Portal

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

To redirect a user to an external portal:

1. From the navigation tree, click **Settings**.
2. Click **Redirect to External Portal**.
3. In **External Portal URL**, enter the URL for the external portal.

   The specified URL can be an external system that obtains authentication credentials from the user, such as a user name or password. It sends this information to the Security Gateway.
4. **Optional:** Select **Add UserCheck Incident ID to the URL query** to add an incident ID to the end of the URL query.

Configuring User Interaction

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

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

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

To configure the necessary user interaction for an Ask object:

1. From the navigation tree, click **Settings**.
2. In the **Conditions** section, select one or more of these options:
   - **User accepted and selected the confirm checkbox**
   - **User entered the required textual input in the user input field**

   The traffic or connection is blocked until the user does the necessary actions.

Configuring UserCheck to Send Original Mail

Threat Extraction extracts potentially-malicious attachments from the email, and gives the user a clean version of the attachment. In addition to access to the original attachments, which you can configure on the profile ("Configuring Threat Extraction Settings " on page 49), you can give the user access to the original email.

To configure

Click **Insert Field**, and select **Send Original Mail**.

Send Original Mail is added to the message body.

Editing UserCheck Objects

To edit a UserCheck object:

1. Go to the **Security Policies** view > **Threat Prevention** > **Threat Tools** > **UserCheck**.
2. Right-click the **UserCheck** page and select **Clone**.
   The **New Object Editor** opens.
3. Enter a name for the new object.
4. Make the necessary changes.
5. Click **OK**.

Selecting Approved and Cancel UserCheck Messages

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

- **Approved Page** - Only applicable for Threat Extraction. When Threat Extraction sends you a clean file, you can select to download the original file. If you select to download the original file, you receive a UserCheck success message. If you select not to download the original file, you receive a UserCheck cancel message.
- **The Cancel Page** - Applicable to all the Threat Prevention Software Blade. The page shows after you refuse to receive access to a page or a file.

To select Approved and Cancel pages:

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

IPS Protections

In This Section:

Protections Browser

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

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

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

Severity

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

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

Confidence Level

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

The Confidence parameter can help you troubleshoot connectivity issues with the firewall. If legitimate traffic is blocked by a protection, and the protection has a **Confidence** level of *Low*, you have a good indication that more granular configurations might be required on this protection.

Performance Impact

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

Note -The Performance Impact of protections is rated based on how they affect gateways of this version which run SecurePlatform and Windows operating systems. The Performance Impact on other gateways may be different than the rating listed on the protection.

For example, you might want to make sure that protections that have a Critical or High Performance Impact are not activated unless they have a Critical or High Severity, or you know the protection is necessary.

If your gateways experience heavy traffic load, be careful about activating High/Critical Performance Impact protections on profiles that affect a large number of mixed (client and server) computers.

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

Protection Types

The IPS protections are divided into two main types:

- **Core protections** - These protections are included in the product and are assigned per gateway. They are part of the Access Control policy
- **ThreatCloud protections** - Updated from the Check Point cloud ("Updating IPS Protections" on page 89). These protections are part of the Threat Prevention policy.

Browsing IPS Protections

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

To show IPS protections:

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

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

To filter the protections:

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

To sort the protections list by information:

Click the column header of the information you want.

Activating Protections

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

Activating Protections for All Profiles

To manually activate a protection in all profiles:

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

Activating Protections for a Specific Profile

To manually activate a protection for a specified profile:

1. In the **Protections Browser**, find the protection to activate.
2. Click **Edit**.
3. Select the profile to activate for this protection.
4. Click **Edit**.
   You can activate the protection for one profile and make it inactive for another profile. It will be activated for some gateways and inactive for others.
   If the protection is inactive according to the policy, you can override the policy preference or change the policy criteria.

To override the settings for this one protection, continue with this procedure.

5. Click **Override with**.
6. Select the action to apply:
   - **Prevent**: Activate IPS inspection for this protection and run active preventions on the gateways to which this profile is assigned.
   - **Detect**: Activate IPS inspection for this protection, tracking related traffic and events.
   - **Inactive**: Do not enforce this protection.
7. Configure the **Logging** settings:
   - **Track**: Define how administrators get notifications (log, alert, mail, or other options).
   - **Capture Packets**: Captures packets relevant to the protection for further analysis. A packet capture is automatically attached to the first log of an attack, even if this option is not selected.
8. **Install Policy**.

Removing Activation Overrides

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

To remove IPS protection overrides on selected protections:

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

To remove IPS protection overrides on all protections:

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

Editing Core IPS Protections

To edit core protections:

1. Go to **Security Policies** > **Threat Prevention** > **Threat Tools** > **IPS Protections**.

2. Right-click a protection and select **Edit**.
3. Configure the required settings.
4. Install the Access Control policy.

Updating IPS Protections

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

Note - To enforce the IPS updates, you must install policy.

To update IPS Protections:

1. In SmartConsole, click **Security Policies** > **Threat Prevention**.
2. In the **Threat Tools** section, click **Updates**.
3. In the **IPS** section > **Update Now**, from the drop-down menu, select:
   - Download using SmartConsole (if your Security Management Server has no internet access), or
   - Download using Security Management Server.
4. **Install Policy**.

If you selected to automatically mark new protections for Follow Up, you have the option to open the Follow Up page directly to see the new protections.

To manually update IPS Protections:

1. In SmartConsole, click **Security Policies** > **Threat Prevention**.
2. In the **Threat Tools** section, click **Updates**.
3. In the **IPS** section > **Update Now**, click the drop-down menu.
4. Select **Offline Update**.
   The file directory opens.
5. Select the required file for the update and click **Open**.
6. **Install Policy**.

Reverting to an Earlier IPS Protection Package

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

To revert to an earlier protection package:

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

Scheduling IPS Updates

You can configure a schedule for downloading the latest IPS protections and protection descriptions ("Scheduling Updates " on page 77).

Reviewing New Protections

To see newly downloaded protections:

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

Configuring Advanced Threat Prevention Settings

In This Section:

Threat Prevention Engine Settings

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

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

The **Threat Prevention Engine Settings** window opens.

Fail Mode

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

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

Check Point Online Web Service

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

- **Block connections when the web service is unavailable**
  - When selected, connections are blocked when there is no connectivity to the Check Point Online Web Service.
  - When cleared, connections are allowed when there is no connectivity (default).

- **Resource categorization mode** - You can select the mode that is used for resource categorization:
  - **Background - connections are allowed until categorization is complete** - When a connection cannot be categorized with a cached response, an uncategorized response is received. The connection is allowed. In the background, the Check Point Online Web Service continues the categorization procedure. The response is cached locally for future requests (default).
    This option reduces latency in the categorization process.
  - **Hold - connections are blocked until categorization is complete** - When a connection cannot be categorized with the cached responses, it remains blocked until the Check Point Online Web Service completes categorization.
  - **Custom - configure different settings depending on the service** - Lets you set different modes for Anti-Bot and Anti-Virus. For example, click **Customize** to set Anti-Bot to Hold mode and Anti-Virus to Background mode.

Connection Unification

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

To adjust the length of a session:

1. In the **Engine Settings** window > **Connection Unification** > **Session unification timeout (minutes)**, enter a different value.
2. Click **OK**.

Configuring Anti-Bot Whitelist

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

To add an email address or domain whose internal emails are not scanned by Anti-Bot:

1. Go to the **Threat Prevention Engine Settings** window > **Anti-Bot**.
2. Click the **+** sign.

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

Selecting Emulation File Types

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

To select Threat Emulation file types that are supported in Threat Prevention profiles:

1. In SmartConsole, select **Manage & Settings > Blades**.
2. From the **Threat Prevention** section, click **Advanced Settings**.

The **Threat Prevention Engine Settings** window opens.

3. From the **Threat Emulation Settings** section, click **Configure file type support**.

   The **File Types Support** window opens.
4. Select the file types that are sent for emulation. By default all file types are sent for emulation.

   The **Emulation supported on column** shows the emulation environments that support the file type.
5. Click **OK** and close the **Threat Prevention Engine Settings** window.
6. Install the Threat Prevention policy.

To configure the file type actions in the Threat Prevention profile:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.

   The **Profiles** page opens.
3. Right-click the profile, and click **Edit**.
4. From the navigation tree, click **Threat Emulation > General**.
5. From the **File Types** section, click **Process specific file types**.
6. Click **Configure**.
7. Configure the Threat Emulation file type actions.
8. Click **OK** and close the Threat Prevention profile.
9. Install the Threat Prevention policy.

Configuring Advanced Engine Settings for Threat Extraction

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

Configuring File Type Support

To configure file type support:

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

   The **Threat Extraction Supported File Types** window opens.
2. From the list select the file types which the Threat Extraction blade supports.
3. Click **OK**.

Configuring Mail Signatures

To configure mail signatures:

1. In the **Threat Prevention Engine Settings** window > **Threat Extraction**, click **Configure Mail Signatures**.

   The **Threat Extraction Mail Signatures** window opens.

Use this window to configure text for:

- **Mail signatures for attachments with potential threats extracted**

  The first signature is always attached to an email that had threats extracted.

  The second signature is added to the first if the email recipient has access to the original file.

- **Mail signatures for unmodified attachments**

  You can insert predefined field codes into the signature text, such as:

  - A link to the file before it was modified by the blade.

  The link opens the UserCheck Portal. The portal shows a list of attachments the recipient can download.

  - Reference ID.

  Use this ID to send the file to the recipient. You can also find the ID in the logs.

  On the gateway, run the command: `scrub send_orig_email`.

2. Click **OK**.

SNORT Signature Support

In This Section:

SNORT is a popular, open source, Network Intrusion Detection System (NIDS). You can import SNORT rules (plain text files with **.rules** extension) that you downloaded or that you created yourself. If you download, make sure to use trusted sources. See snort.org http://www.snort.org for more information.

Snort Protections get these levels automatically:

- Severity - **High**
- Confidence Level - **Medium-Low**
- Performance Impact - **High**

The name of the imported SNORT protection is the value of the **msg** field in the original SNORT rule.

- If one SNORT rule has multiple msg strings with the same value, they are aggregated to one IPS SNORT protection.
- If multiple rules are imported at different times and have the same msg string, the new import overrides the old protection.

Importing SNORT Rules to Security Management Server

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

To import and convert SNORT rules:

1. Make sure no SmartConsole is connected to the Security Management Server.
2. Copy the rules file to the Security Management Server.
   Best practice: put the file in `/home/admin`.
3. In SmartConsole, go to **Threat Prevention** > **Policy** > **IPS Protections** > **Actions** > **Snort Protections** > **Import snort rules**.
   The tool converts the rules to Check Point syntax and updates the protections database.
4. Make sure that SNORT protections are activated in the IPS profile.
5. **Install policy**.

Importing SNORT Rules to Multi-Domain Server

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

To import Snort rules to the Multi-Domain Server:

1. Copy a Snort Rules file to the Multi-Domain Server.
2. In the SmartConsole Multi-Domain view, go to **Threat Prevention** > **Policy** > **IPS Protections** > **Actions** > **Snort Protections** > **Import snort rules**.
3. Make sure that Snort Protections are activated in the Global IPS Profile.
4. Click **Global Policies**.
5. Right-click the Multi-Domain Server object and select **Reassign Global Policy and IPS to all assigned Domains**.

Deleting SNORT Protections

After you convert and import a SNORT rule, it is a part of the IPS database. You cannot delete it from the SmartConsole. You must delete it with the SnortConvertor tool, to make sure that the database is updated.

To delete all SNORT protections:

1. Make sure no SmartConsole is connected to the Security Management Server.
2. In the SmartConsole API, enter: `delete threat-protections`

To delete the SNORT protections in Multi-Domain Security Management:

1. In SmartConsole, go to API, enter: `delete threat-protections`
2. In the Global Domain view, click **Global Policies**.
3. Right-click the Multi-Domain Server object and select **Reassign Global Policy and IPS to all assigned Domains**

Creating SNORT Rule Files

You can write your own SNORT rules and then import them to be protections. SNORT rules use signatures to define attacks. A SNORT rule has a *rule header* and *rule options*. For more about SNORT, see snort.org http://www.snort.org.

Check Point supports snort 2.9 and lower.

SNORT Rule Header:

```
< Action > < Protocol > < Address > < Port > < Direction > < Address > < Port >
```

SNORT Rule Options:

```
<keyword>:"<option>"
```

Example:

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

Where:

- Action = **alert**
- Protocol = **tcp**
- Address = **any**
- Port = **any**
- Direction = **->**
- Address = **any**
- Port = **any**
- Keyword = **content**
- Option = **|90|**
- Name of protection in IPS = **Possible exploit**

Supported Snort syntax:

In general, these are the supported syntax components. There are some limitations ("Unsupported SNORT Syntax" on page 97).

- Supported Snort Keywords: *"data", "content", "length", "test", "re", "jump", "pcre", "flowbits", "byte_test", "byte_jump", "isdataat", "stateop_global", "stateop", "no_match", "inspect"*
- Supported Content Keyword Modifiers: *"nocase", "rawbytes", "depth", "offset:", "distance:", "within", "urilen"*
- Supported Threshold Rule Types - *Threshold* , *Both* (*Limit* is not supported.)
- Supported Macros - HTTP_PORTS (Interpreted as 80 and 8080 ports.)

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

Debugging:

`$FWDIR/log/SnortConvertor.elg` is updated with the debug messages from the last SnortConvertor run.

To find failed rule debugs in the `SnortConvertor.elg` file, search for: **Failed to convert rule**

Unsupported SNORT Syntax

This syntax is not supported and will not convert:

- pcre modifiers: 'G', 'O', 'A', 'C','K'
- pcre regular expression with lookahead assertion: `?!`
- Using `byte_test` keyword with operator not in: `<,>,=,&,^`
- Content modifiers: `http_cookie`, `http_raw_cookie`
- `http_method` is not supported if it is the only http modifier type in the Snort Rule
- Protocols: icmp, ip. (`all` is interpreted as udp and tcp protocols)
- Snort Rule without content keyword
- All `PORT` macros, except `HTTP_PORTS`

- Specification of source port (only `any` is supported)

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

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

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

- `rawbytes` content, or `B` pcre modifiers with `http_uri` content or `U` pcre modifiers
- With http content or pcre modifiers:
  - `http_raw_uri` content or `I` pcre modifiers
  - `http_stat_msg` content or `Y` pcre modifiers
  - `http_stat_code` content or `S` pcre modifiers
- Without http content or pcre modifiers:
  - Two or more uses of `http_header` content or `H` pcre modifiers
  - Two or more uses of `http_raw_header` content or `D` pcre modifiers
- With `depth` or `offset` content and http content that is one of these on the same content keyword, or ^ (carrot) in pcre with one of these http pcre modifiers on the same pcre keyword:
  - `http_header` content or `H` pcre modifiers
  - `http_raw_header` content or `D` pcre modifiers
  - `http_stat_msg` content or `Y` pcre modifiers
  - `http_stat_code` content or `S` pcre modifiers
  - `http_uri` content or `U` pcre modifiers
- Use of `depth` or `offset` content, or ^ (carrot) in pcre, without any http content, and with destination ports that are not `HTTP_PORTS` macro
- `http_client_body` content or `P` pcre modifier
- A pcre keyword with `{}` (curly braces) quantifier
- Use of both content and `byte_test` keywords
- `http_header` content modifiers or `H` pcre modifiers enforced only on raw http data (not decoded and normalized header data)
- Use of the `urilen` keyword, except in a SNORT Rule that has only `http_uri` and `U` pcre modifiers, or `http_raw_uri` content modifier and `I` pcre modifiers.
  - If the SNORT Rule has only `http_uri` content or `U` pcre modifiers, the size will be of the decoded and normalized buffer.
  - If the SNORT Rule has only `http_raw_uri` content or `I` pcre modifiers, the size will be of the raw uri buffer.

Optimizing IPS

In This Section:

IPS is a robust solution which protects your network from threats. Implementation of the recommendations in this chapter will help maintain optimal security and performance.

During the tuning process, keep in mind that Check Point bases its assessment of performance impact and severity on an industry standard blend of traffic, which places greater weight on protocols such as HTTP, DNS, and SMTP. If your network traffic has high levels of other network protocols, you need to take that into consideration when you assess the inspection impact on the gateway or severity of risk to an attack.

Managing Performance Impact

A Check Point Security Gateway performs many functions in order to secure your network. At times of high network traffic load, these security functions may weigh on the gateway's ability to quickly pass traffic. IPS includes features which balance security needs with the need to maintain high network performance.

Bypass Under Load

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

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

To bypass IPS inspection under heavy load:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
   The gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **IPS**.
3. Select **Bypass IPS inspection when gateway is under heavy load**.
4. To set logs for activity while IPS is off, in the **Track** drop-down list, select a tracking method.
5. To configure the definition of heavy load, click **Advanced**.
6. In the **High** fields, provide the percentage of **CPU Usage** and **Memory Usage** that defines Heavy Load, at which point IPS inspection will be bypassed.

7. In the **Low** fields, provide the percentage of **CPU Usage** and **Memory Usage** that defines a return from Heavy Load to normal load.
8. Click **OK** to close the **Gateway Load Thresholds** window.
9. Click **OK**.
10. **Install Policy**.

Troubleshooting IPS for a Security Gateway

IPS includes the ability to temporarily stop protections on a Security Gateway set to Prevent from blocking traffic. This is useful when troubleshooting an issue with network traffic.

To enable Detect-Only for Troubleshooting:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
   The gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **IPS**.
3. In the **Activation Mode** section, click **Detect Only**.
4. Click **OK**.
5. **Install Policy**.
   All protections set to Prevent allow traffic to pass, but continue to track threats according to the Track setting.

Tuning Protections

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

IPS Policy Settings

The IPS Policy settings allow you to control the entire body of protections by making a few basic decisions. Activating a large number of protections, including those with low severity or a low confidence level, protects against a wide range of attacks, but it can also create a volume of logs and alerts that is difficult to manage. That level of security may be necessary for highly sensitive data and resources; however it may create unintended system resource and log management challenges when applied to data and resources that do not require high security.

Best Practice - adjust the IPS Policy settings to focus the inspection effort in the most efficient manner. Once system performance and log generation reaches a comfortable level, the IPS Policy settings can be changed to include more protections and increase the level of security. Individual protections can be set to override the IPS Policy settings.

For more information on IPS Policy, see Automatically Activating Protections.

Note - A careful risk assessment should be performed before disabling any IPS protections.

Focus on High Severity Protections

IPS protections are categorized according to severity. An administrator may decide that certain attacks present minimal risk to a network environment, also known as low severity attacks. Consider turning on only protections with a higher severity to focus the system resources and logging on defending against attacks that pose greater risk.

Focus on High Confidence Level Protections

Although the IPS protections are designed with advanced methods of detecting attacks, broad protection definitions are required to detect certain attacks that are more elusive. These low confidence protections may inspect and generate logs in response to traffic that are system anomalies or homegrown applications, but not an actual attack. Consider turning on only protections with higher confidence levels to focus on protections that detect attacks with certainty.

IPS Network Exceptions can also be helpful to avoid logging non-threatening traffic.

Focus on Low Performance Impact Protections

IPS is designed to provide analysis of traffic while maintaining multi-gigabit throughput. Some protections may require more system resources to inspect traffic for attacks. Consider turning on only protections with lower impact to reduce the amount system resources used by the gateway.

Enhancing System Performance

Performance Pack

Check Point Performance Pack improves gateway performance. For more information on Performance Pack and how to optimize it, see the *R80.10Performance Pack Administration Guide* http://supportcontent.checkpoint.com/documentation_download?ID=TBD.

CoreXL

For SecurePlatform gateways running on multi-core hardware, installing CoreXL on the gateway will allow the gateway to leverage the multiple cores to more efficiently handle network traffic. For more information on CoreXL and optimizing the CoreXL configuration, see the *R80.10 Performance Tuning Administration Guide* http://supportcontent.checkpoint.com/documentation_download?ID=TBD.

Using the Whitelist

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

Adding a File to the Whitelist

To configure files on the Threat Prevention Whitelist:

1. In SmartConsole, click **Security Policies > Threat Prevention > Policy > Threat Tools > Whitelist Files**.
2. Click **New**.

   The **Whitelist File** window opens.
3. Enter the **Object Name** and **MD5 signature** for the new file exception.

   Note - To edit or remove Whitelist files, right-click the file and select the applicable option.
4. Click **OK**.
5. Install the Threat Prevention policy.

Threat Indicators Settings

Threat Indicators lets you upload *Indicator* (on page 13) files that contain sets of *observables* ("Observable" on page 13). These observables are added to the Threat Prevention policy.

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:

Field	Description	Valid Values	Value Criteria	Optional
UNIQ-NAME	Name of the observable	Free text	Must be unique	No
VALUE	A value that is valid for the type of the observable	See the table below	See the table below	No
TYPE	Type of the observable	• `URL` • `Domain` • `IP` • `IP Range` • `MD5` • `Mail-subject` • `Mail-from` • `Mail-to` • `Mail-cc` • `Mail-reply-to`	Not case sensitive	No
SEVERITY	Degree of threat the observable presents	• `low` • `medium` • `high` • `critical`	Default - high	Yes
PRODUCT	Check Point Software Blade that processes the observable	• `AV` • `AB`	AV - Check Point Anti-Virus Software Blade (default) AB - Check Point Anti-Bot Software Blade **Note** - only the Anti-Virus Software Blade can process MD5 observables.	Yes

Field	Description	Valid Values	Value Criteria	Optional
COMMENT		Free text		Yes

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:

Observable Type	Validation Criteria
URL	Any valid URL
Domain	Any URL domain
IP	Standard IPv4 address
IP Range	A range of valid IPv4 addresses, separated by a hyphen: `<IP>-<IP>`
MD5	Any valid MD5
Mail-subject	Any non-empty text string
Mail-to Mail-from Mail-cc Mail-reply-to	Can be one of these: • A single email address (Example: `abc@domain.com`) • An email domain (Examples: `@domain.com` or `domain.com`)

Requirements for validation of CSV Indicator files:

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

Example of a CSV Indicator File

```
#! DESCRIPTION = indi file boaz,,,,,,
"#! REFERENCE = Indicator Bulletin; Feb 20, 2014",,,,,,
# FILE FORMAT:,,,,,,
"#      All lines beginning  ""#"" are comments",,,,,,
"#      All lines beginning  ""#!"" are metadata read by the SW",,,,,,
"# UNIQ-NAME,VALUE,TYPE,CONFIDENCE,SEVERITY,PRODUCT,COMMENT",,,,,,
observ1,8d9b6b8912a2ed175b77acd40cbe9a73,MD5,medium,medium,AV,FILENAME:WUC
 Invitation Letter Guests.doc
observ2,76700f862a0c241b8f4b754f76957bda,MD5,high,high,AV,FILENAME:essais~.swf|
NOTE:FWS type Flash file
observ7,http://somemaliciousdomain.com/uploadfiles/upload/exp.swf?info=
789c333432d333b4d4b330d133b7b230b03000001b39033b&infosize=00840000
,URL,high,high,AV,IPV4ADDR:196.168.25.25
observ8,svr01.passport.ServeUser.com,Domain,low,high,AB,TCP:80|
IPV4ADDR:172.18.18.25|NOTE:Embedded EXE Remote C&C and Encoded Data
```

```
observ9,somemaliciousdomain2.com,Domain,,low,AV,TCP:8080|IPV4ADDR:172.22.14.10
observ10,http://www.bogusdomain.com/search?q=%24%2B%25&form=MOZSBR&pc=
MOZI,URL,low,low,AB,IPV4ADDR:172.25.1.5
observ11,http://somebogussolution.com/register/card/log.asp?isnew=-1&LocalInfo=
Microsoft%20Windows%20XP%20Service%20Pack%202&szHostName=
ADAM-E512679EFD&tmp3=tmp3,URL,medium,,AB,
observ14,172.16.47.44,IP,high,medium,AB,TCP:8080
observ15,172.16.73.69,IP,medium,medium,AV,TCP:443|NOTE:Related to Flash
exploitation
observ16,abc@def.com,mail-to,,high,AV,"NOTE:truncated; samples have appended to
the subject the string ""PH000000NNNNNNN"" where NNNNNNN is a varying number"
observ34,stamdomain.com,domain,,,AB,
observ35,stamdomain.com,mail-from,high,medium,AV,
observ37,xyz.com,mail-from,medium,medium,AB,
observ38,@xyz.com,mail-from,medium,medium,AB,
observ39,a@xyz.com,mail-from,medium,medium,AB,
```

Configuring Indicators in SmartConsole

Define network objects to hold the Indicator files.

To load Indicators:

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

To delete Indicators:

1. Select an *Indicator*.
2. Click **Delete**.
3. In the window that opens, click **Yes** to confirm.

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

Using Anti-Bot and Anti-Virus with VSX

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

- Is enabled and configured on the relevant Virtual Systems and enabled and configured on the VSX Gateway (VS0)

  VS0 handles contract validation for all Virtual Systems.

- Can connect to the internet

  A Virtual System gets updates through the VSX Gateway (VS0). If the VSX Gateway fails, each Virtual System uses its proxy settings to get the update from the internet.

Note - Where applicable, make sure the routing, DNS, and proxy settings for the VSX Gateway (VS0) are configured correctly.

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

1. If applicable, configure proxy settings for the VSX Gateway (VS0) or the Virtual Systems or both:
   a) From the **Network Object** tree, double-click the VSX Gateway (VS0).
   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 (VS0) for all Virtual Systems that use **Anti-Bot** and **Anti-Virus**:
   a) From the **Network Object** tree, double-click the Virtual System.
   b) In the **Network Security** section, select **Anti-Bot** and **Anti-Virus**.
   c) Click **OK**.
3. Select the Threat Prevention and configure the policies.
4. Install the Threat Prevention policy (and access policy if needed) on the VSX Gateway (VS0) and the relevant Virtual Systems.

Using Threat Extraction with VSX

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

- Is enabled and configured on the relevant Virtual Systems and enabled and configured on the VSX Gateway (VS0).
- The Virtual Systems are configured with a Mail Transfer Agent (MTA).

Note - Where applicable, make sure that the routing, DNS, and proxy settings for the VSX Gateway (VS0) are configured correctly.

To enable Threat Extraction on Virtual Systems:

1. In the Gateways & Servers view, right-click the Virtual System object and select **Edit**.
   The **Virtual System Properties** window opens.

2. On the **General Properties** > **Network Security** tab, select **Threat Extraction**.
3. The **Threat Extraction First Time Activation Wizard** opens go to the VS object and enable Threat Extraction.
4. In the **Next Hop Configuration** window, select **skip this configuration now**, and click **Next**.
5. In the **Summary** window, click **Finish**.
6. In the VS Properties window, go to **Mail Transfer Agent** in the navigation tree, and select **Enable as Mail Transfer Agent (MTA)**.
7. Add the MTA definitions to **Mail Forwarding**.
8. Click **OK**.
9. Install the Standard policy on the Virtual Systems (including VS0).

Threat Prevention CLI Commands

You can run commands from the CLI (Command Line Interface) to install Threat Prevention policy and for 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>`

Parameter	Description
`rulebase`	Name of the Rule Base
`targets`	Install the Threat Prevention policy on one or more of these Security Gateways

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`.

Syntax: `te_add_file  -f= <file path>  -d= <directory path>`

Parameter	Description
-f=	Specifies the path to the file. You must include the file name at the end of the path.
-d=	Specifies the path to a directory. The command takes all the files in the directory and sends them for emulation.

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.

Syntax: `tecli control sizing {enable|disable|status}`

Note: For more about using sizing mode, go to sk93598 http://supportcontent.checkpoint.com/solutions?id=sk93598.

tecli debug

Description: Enable and disable debug mode for Threat Emulation.

Syntax: `tecli debug {on|off|scan local {enable|disable}}`

Parameter	Description
`on`	Enables debug mode
`off`	Disables debug mode
`scan local enable`	Enables the appliance or Security Gateway to scan local connection
`scan local disable`	Disables the appliance or Security Gateway to scan local connection

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:

Command	Description
`tecli s s`	Shows emulation statistics
`tecli s c i`	Shows information about ThreatCloud emulation
`tecli s c q`	Shows the quota for ThreatCloud emulation
`tecli s e e`	Shows the current status of the emulation queue
`tecli s u a`	Shows all the parts of file emulation

tecli show cloud

Description: Shows data and statistics about your ThreatCloud account.

Syntax: `tecli show cloud {identity|info|quota}`

Parameter	Description
`identity`	Shows data about how the Security Gateway or Emulation appliance connects to the ThreatCloud
`info`	Shows data about your file emulation in the ThreatCloud
`quota`	Shows data about your ThreatCloud monthly emulation quota

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>}}`

Parameter	Description
`emulations`	Shows the current status of the emulation queue
`synopsis`	Shows a summary of the VMs
`detailed`	Shows data and details of the VMs
`id <ID>`	Shows data for the VM with this ID

Example:

`tecli s e e` or `tecli show emulator emulations`

`tecli s e v s` or `tecli show emulator vm synopsis`

tecli show downloads

Description: Shows data and statistics about files and rules that Threat Emulation is downloading.

Syntax: `tecli show downloads {all|images|dr|sa|raw|types}`

Parameter	Description
`all`	Shows the status of all downloads
`images`	Shows download status of operating system images
`dr`	Shows download status of malware detection rules
`sa`	Shows download status of static analysis rules
`raw`	Shows download status of general Threat Emulation files
`types`	Shows the file extensions that are being sent for emulation

Example:

`tecli s d a` or `tecli show downloads all`

`tecli s d i` or `tecli show downloads images`

tecli show remote

Description Shows data and statistics about the Emulation appliance

Syntax `tecli s r i` or `tecli show remote information`

tecli show statistics

Description: Shows statistics to the Emulation appliance or Security Gateway.

Syntax: `tecli s s` or `tecli show statistics`

Results:

```
gw> tecli s s
                                        Last day          Last week        Last 30 days|
General Information:
--------------------
Scanned files:                                0                262                 262
Malicious files:                              0                190                 190
Files filtered by static analysis:            0                  0                   0
Files error count:                            0                  0                   0
Files filtered by local cache:                0           241(91%)            241(91%)
Files no resource count:                      0                  0                   0
Average sample process time:                  0 sec.            57 sec.             57 sec.
Average sample size:                          0 bytes       213101 bytes        213101 bytes

Local Emulation Information:
----------------------------
Scanned files locally:                        0                  0                   0
Malicious files locally:                      0                  0                   0
Average process time for emulated files:      0 sec.           177 sec.            177 sec.
Average virtual machine usage:                0                  0                   0
Average queue size:                           0                  0                   0
Peak queue size:                              0                  0                   0

Cloud Emulation Information:
----------------------------
Scanned files on cloud:                       0                262                 262
Malicious files on Cloud:                     0                190                 190
Files filtered by cloud cache:                0                  4                   4
Average cloud process time:                   0 sec.           181 sec.            181 sec.

Remote Emulation Information:
-----------------------------
Scanned files remotely:                       0                  0                   0
Malicious files remotely:                     0                  0                   0
Files filtered by remote cache:               0                  0                   0
Average remote process time:                  0 sec.             0 sec.              0 sec.

Communication with Threat Cloud:
--------------------------------
Last Sharing succeeded:Thu Aug  8 03:01:00 2013
Last Sharing failed: -
Sharing Identifier:HASHED_7dc52293686f4edd6d6472632f019f3d-222c90527b6f0b1bebcef468b89edfca
gw>
```

tecli show throughput

Description: Shows data about file emulation for each time interval.

Syntax: `tecli show throughput {minute|hour|day|month}`

Parameter	Description
`minute`	Shows how many files completed emulation for each minute
`hour`	Shows how many files completed emulation for each hour
`day`	Shows how many files completed emulation for each day
`month`	Shows how many files completed emulation for each month

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)
```

Managing IPS gateways - CLI

You can use these CLI commands to manage IPS on your Security Gateways. You must be in expert mode to use the commands.

To see all available commands:

1. On the gateway, go to the expert mode.
2. Type **ips** and press **Enter**.

Command	Description
ips on|off [-n]	Enable or disable IPS on the Security Gateway. -n Empty templates table (applies **fwaccel off; fwaccel on** immediately). Otherwise, this command takes effect in a few minutes.
ips stat	Show the IPS status of the Security Gateway.
ips bypass stat	Show the Bypass Under Load status.

Command	Description
ips bypass on|off	Enable or disable Bypass Under Load.
ips bypass set cpu|mem low|high <threshold>	Set the Bypass Under Load threshold. threshold Valid range is 1 to 99. Unit is percent.
ips debug [-e filter] -o <output_file>	Create an IPS debug file. Filter valid values are the same as for **fw ctl debug**. Consult with Check Point Technical Support.
ips refreshcap	Refresh the sample capture repository.
ips stats [<ip_address> -m] [-g <seconds>] [<ip_address> <seconds>]	Print IPS and Pattern Matcher performance statistics. Without arguments, runs on current Security Gateway for 20 seconds. This is a resource intensive command. Do not run it on a system with a high load. -m Analyzes input statistics file from Security Gateway. Give IP address of the Security Gateway. Run from the management server. -g Collect statistics for current Security Gateway. seconds period in which statistics are gathered
ips pmstats reset	Reset pattern matcher statistics.
ips pmstats -o <output_file>	Print pattern matcher statistics.

Configuring Advanced Threat Emulation Settings

In This Section:

Updating Threat Emulation

Threat Emulation connects to the ThreatCloud to update the engine and the operating system images. The default setting for the Threat Emulation appliance is to automatically update the engine and images.

The default setting is to download the package once a day.

Best Practice - Configure Threat Emulation to download the package when there is low network activity.

Update packages for the Threat Emulation operating system images are usually more than 2GB. The actual size of the update package is related to your configuration.

To enable or disable Automatic Updates for Threat Emulation:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **Updates**.
   The **Updates** page opens.
3. Under Threat Emulation, click **Schedule Update**.
4. Select or clear these settings:
   - **Enable Threat Emulation engine scheduled update**
   - **Enable Threat Emulation images scheduled update**
5. Click **Configure** to configure the schedule for Threat Emulation engine or image updates.
6. Configure the automatic update settings to update the database:
   - To update once a day, select **At** and enter the time of day
   - To update multiple times a day, select **Every** and set the time interval
   - To update once or more for each week or month:

   a) Select **At** and enter the time of day.

   b) Click **Days**.

   c) Click **Days of week** or **Days of month**.

   d) Select the applicable days.

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

Threat Emulation Images

To update the operating system image for Threat Emulation on a gateway:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **Updates**.
   The **Updates** page opens.
3. Under Threat Emulation, click **Update Images**.
4. Select a gateway and click **OK**.
5. Install the Threat Prevention policy.

Handling Connections During Emulation

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

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.
3. Double-click the Threat Prevention profile.
4. From the navigation tree, select **Threat Emulation** > **Advanced**.
5. 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
6. Click **OK**.
7. Install the Threat Prevention policy.

Static Analysis

To disable static analysis for the Threat Prevention profile:

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.
3. Double-click the Threat Prevention profile.
4. From the navigation tree, select **Threat Emulation** > **Advanced**.
5. From the **Engine settings** section, select **Disable static analysis for filtering files**.
6. To enable static analysis, clear **Disable static analysis for filtering files**.
7. Click **OK**.
8. Install the Threat Prevention policy.

Threat Emulation Logs

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

1. In SmartConsole, select **Security Policies > Threat Prevention**.
2. From the **Threat Tools** section, click **Profiles**.
3. Double-click the Threat Prevention profile.
4. From the navigation tree, select **Threat Emulation** > **Advanced**.
5. From the **Logging** section, clear **Log every file scanned**.
6. To generate logs for each file after emulation is complete, select **Log every file scanned**.
7. Click **OK**.
8. Install the Threat Prevention policy.

Configuring MTA Advanced Settings

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

9. **Install Policy**.

Disabling the MTA

To disable the MTA:

1. Configure the network to disable the MTA.
2. Disable MTA on the Security Gateway.

Configuring the Network to Disable the MTA

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

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

1. Connect to the DNS settings for the network.
2. Change the MX records, and define the mail server as the next hop.
3. Wait for 24 hours.
4. Disable the MTA on the Security Gateway ("Disabling MTA on the Security Gateway" on page 116).

To disable MTA for email that is sent to a different MTA:

1. Connect to the SMTP settings on the MTA that sends SMTP traffic to the internal mail server.
2. Change the SMTP settings and define the mail server as the next hop.
3. Make sure that the MTA queue is empty.
4. Disable the MTA on the Security Gateway ("Disabling MTA on the Security Gateway" on page 116).

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 45).

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.

Emulation Limits

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

- Maximum file size
- Maximum time that the Software Blade does emulation
- Maximum time that a file waits for emulation in the queue (for Emulation appliance only)

If emulation is not done on a file for one of these reasons, the Fail Mode settings for Threat Prevention define if a file is allowed or blocked.

You can configure the maximum amount of time that a file waits for the Threat Emulation Software Blade to do emulation of a file. There is a different setting that configures the maximum amount of time that emails are held in the MTA.

If the file is waiting for emulation more than the maximum time:

- Threat Emulation Software Blade - The Threat Prevention profile settings define if a file is allowed or blocked
- MTA - The MTA settings define if a file is allowed or blocked

Configuring Emulation Limits

1. In SmartConsole, select **Manage & Settings > Blades > Threat Prevention > Advanced Settings**.

   The **Threat Emulation Engine Settings** window opens.
2. Click **Configure settings**.

   The **Threat Emulation Settings** window opens.
3. Configure the settings for the emulation limits.
   - From When limit is exceeded traffic is accepted with track, select the action if a file is not sent for emulation:
   - None - No action is done
   - Log - The action is logged
   - Alert - An alert is sent to SmartView Monitor
4. Click **OK** and then install the policy.

Changing the Local Cache

When a Threat Emulation analysis finds that a file is clean, the file hash is saved in a cache. Before Threat Emulation sends a new file to emulation, it compares the new file to the cache. If there is a match, it is not necessary to send it for additional emulation. Threat Emulation uses the cache to help optimize network performance.

Best Practice - Do not change this setting.

Changing the Size of the Local Cache

1. In SmartConsole, select **Manage & Settings > Blades > Threat Prevention > Advanced Settings**.

   The **Threat Prevention Engine Settings** window opens.
2. Click **Configure Settings**.

   The **Threat Emulation Settings** window opens.
3. From **Number of file hashes to save in local cache**, configure the number of file hashes that are stored in the cache.
4. Click **OK** and then install the policy.

Optimizing System Resources

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

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 SmartConsole, select **Manage & Settings** > **Blades** > **Threat Prevention**.
2. Under **Threat Prevention**, click **Advanced Settings**.
3. Scroll down and from the **Threat Emulation Settings** section, click **Configure settings**.
   The **Threat Emulation Settings** window opens.
4. Enter the **Network** and **Mask** for the IP address for the virtual interface.
5. Click **OK** and then install the policy.

Using Threat Prevention with HTTPS Traffic

In This Section:

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

Configuring HTTPS Inspection

HTTPS Internet traffic uses the SSL (Secure Sockets Layer) protocol and is encrypted to give data privacy and integrity. However, HTTPS traffic has a possible security risk and can hide illegal user activity and malicious traffic. Security Gateways cannot inspect HTTPS traffic because it is encrypted. You can enable the HTTPS Inspection feature to let the Security Gateways create new SSL connections with the external site or server. The Security Gateways are then able to decrypt and inspect HTTPS traffic that uses the new SSL connections.

There are two types of HTTPS Inspection:

- **Outbound HTTPS Inspection** - To protect against malicious traffic that is sent from an internal client to an external site or server.
- **Inbound HTTPS Inspection** - To protect internal servers from malicious requests that arrive from the Internet or an external network.

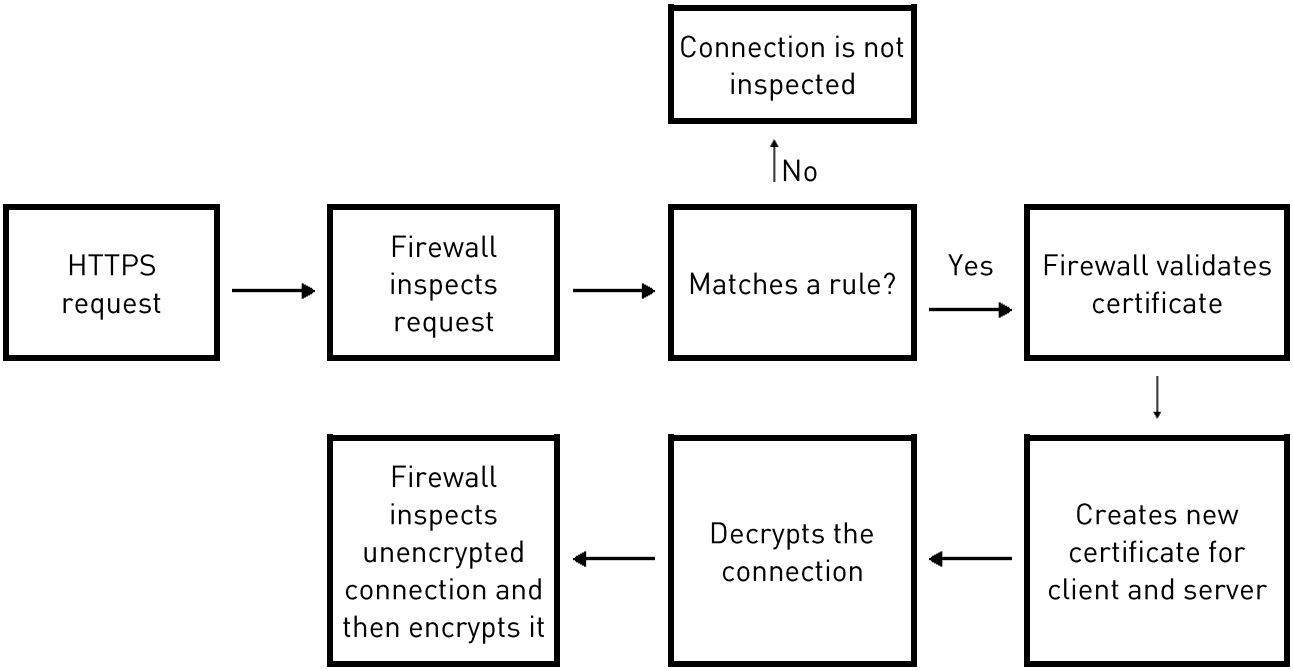
A Security Gateway uses certificates and becomes an intermediary between the client computer and the secure web site. All data is kept private in HTTPS Inspection logs. Only administrators with HTTPS Inspection permissions can see all the fields in such a log.

Inspecting HTTPS Packets

Outbound Connections

Outbound connections are HTTPS connections that arrive from an internal client and connect to the Internet. The Security Gateway compares the HTTPS request to the rules in the HTTPS Inspection Rule Base. If the request does not match any rule, the packet is not inspected and the connection is allowed.

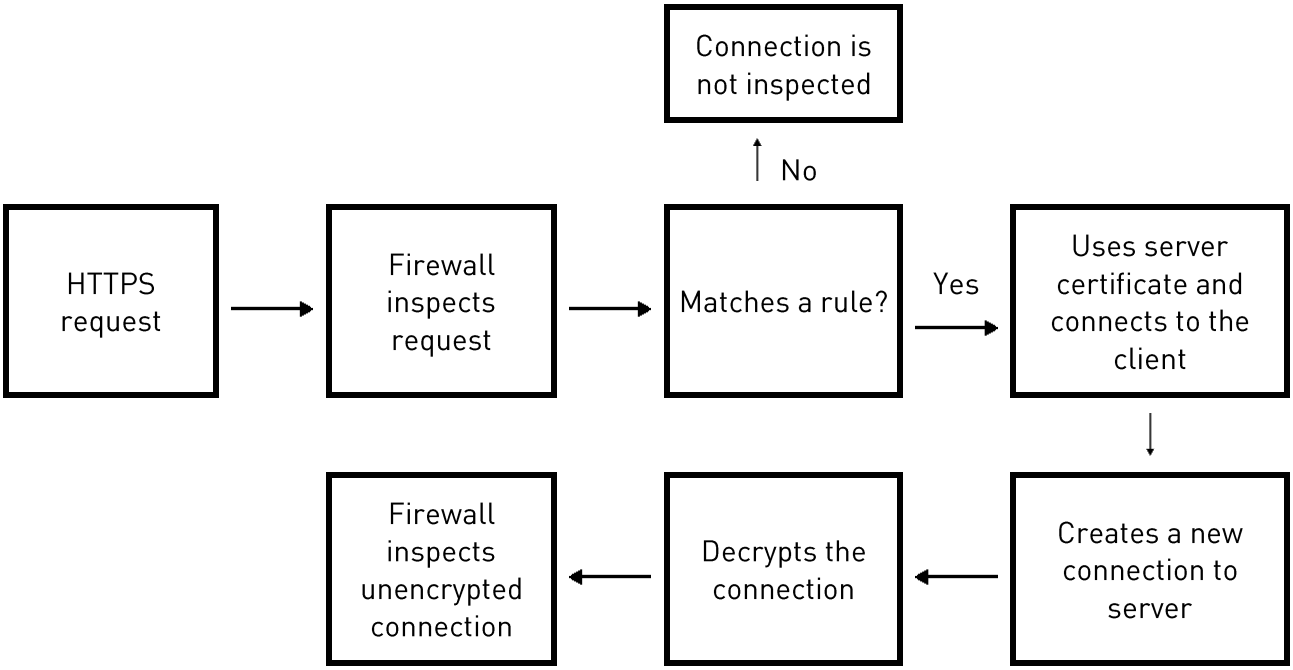
If the request matches an HTTPS Inspection rule, the Security Gateway validates the certificate from the server (on the Internet). The Security Gateway validates the certificate using the Online Certificate Status Protocol (OCSP) standard. OCSP is faster and uses much less memory than CRL Validation, which is used for certificate validation in releases lower than R80.10. For a new HTTPS connection to the server, the Security Gateway creates and uses a new certificate. There are two HTTPS connections, one to the internal client and one to the external server. It can then decrypt and inspect the packets according to the security policy. The packets are encrypted again and sent to the destination.



Inbound Connections

Inbound connections are HTTPS connections that arrive from an external client and connect to a server in the DMZ or the internal network. The Security Gateway compares the HTTPS request to the rules in the HTTPS Inspection Rule Base. If the request does not match any rule, the packet is not inspected and the connection is allowed.

If the request matches an HTTPS Inspection rule, the Security Gateway uses the certificate for the internal server to create an HTTPS connection with the external client. The Security Gateway creates a new HTTPS connection with the internal server. Since the Security Gateway has a secure connection with the external client, it can decrypt the HTTPS traffic. The decrypted traffic is inspected according to the security policy.



Configuring Gateways to inspect outbound and inbound HTTPS

This section gives an example of how to configure a Gateways to inspect outbound and inbound HTTPS traffic.

Workflow overview

1. Enable HTTPS Inspection on the Security Gateway.
2. Configure the Security Gateway to use the certificate.
   - Outbound Inspection - Generate a new certificate for the Security Gateway.
   - Inbound Inspection - Import the certificate for the internal server.
3. Configure the HTTPS Inspection Rule Base.
4. Install the Access Control Policy.

Enabling HTTPS Inspection

You must enable HTTPS inspection on each Security Gateway.

To enable HTTPS Inspection on a Security Gateway:

1. From the SmartConsole **Gateways & Servers** view, edit the Security Gateway object.
2. Click **HTTPS Inspection** > **Step 3**.
3. Select **Enable HTTPS Inspection**.

The first time you enable HTTPS inspection on one of the Security Gateways, you must create an outbound CA certificate for HTTPS inspection or import a CA certificate already deployed in your organization. This outbound certificate is used by all Security Gateways managed on the Security Management Server.

Creating an Outbound CA Certificate

The outbound CA certificate is saved with a P12 file extension and uses a password to encrypt the private key of the file. The Security Gateways use this password to sign certificates for the sites accessed. You must keep the password because it is also used by other Security Management Servers that import the CA certificate to decrypt the file.

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

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

To create an outbound CA certificate:

1. In SmartConsole Gateways & Servers view, right-click the Security Gateway object and select **Edit**.

   The **Gateway Properties** window opens.
2. In the navigation tree, select **HTTPS Inspection**.
3. In **Step 1** of the **HTTPS Inspection** page, click **Create**.

   The **Create** window opens.

4. Enter the necessary information:
   - **Issued by (DN)** - Enter the domain name of your organization.
   - **Private key password** - Enter the password that is used to encrypt the private key of the CA certificate.
   - **Retype private key password** - Retype the password.
   - **Valid from** - Select the date range for which the CA certificate is valid.
5. Click **OK**.
6. Export and deploy the CA certificate ("Exporting and Deploying the Generated CA" on page 125).

Importing an Outbound CA Certificate

You can import a CA certificate that is already deployed in your organization or import a CA certificate created on one Security Management Server to use on another Security Management Server.

Best Practice - Use *private* CA Certificates.

For each Security Management Server that has Security Gateways enabled with HTTPS inspection, you must:

- Import the CA certificate.
- Enter the password the Security Management Server uses to decrypt the CA certificate file and sign the certificates for users. Use this password only when you import the certificate to a new Security Management Server.

To import a CA certificate:

1. If the CA certificate was created on another Security Management Server, export the certificate from the Security Management Server on which it was created ("Exporting a Certificate from the Security Management Server" on page 124).
2. In the SmartConsole **Gateways & Servers** view, right-click the Security Gateway object and select **Edit**.

   The **Gateway Properties** window opens.
3. In the navigation tree, select **HTTPS Inspection**.
4. In **Step 1** of the **HTTPS Inspection** page, click **Import**.

   The **Import Outbound Certificate** window opens.
5. Browse to the certificate file.
6. Enter the **private key password**.
7. Click **OK**.
8. If the CA certificate was created on another Security Management Server, deploy it to clients ("Exporting and Deploying the Generated CA" on page 125).

Exporting a Certificate from the Security Management Server

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

Command syntax:

```
export_https_cert [-local] | [-s server] [-f certificate file name under FWDIR/tmp][-help]
```

To export the CA certificate:

On the Security Management Server, run this command:

```
$FWDIR/bin/export_https_cert -local -f [certificate file name under
FWDIR/tmp]
```

Example

```
$FWDIR/bin/export_https_cert -local -f mycompany.p12
```

Exporting and Deploying the Generated CA

To prevent users from getting warnings about the generated CA certificates that HTTPS inspection uses, install the generated CA certificate used by HTTPS inspection as a trusted CA. You can distribute the CA with different distribution mechanisms such as Windows GPO. This adds the generated CA to the trusted root certificates repository on client computers.

When users run standard updates, the generated CA will be in the CA list and they will not receive browser certificate warnings.

To distribute a certificate with a GPO:

1. From the **HTTPS Inspection** window of the Security Gateway, click **Export certificate**.
2. Save the CA certificate file.
3. Use the Group Policy Management Console ("Deploying Certificates by Using Group Policy" on page 125) to add the certificate to the Trusted Root Certification Authorities certificate store.
4. Push the Policy to the client computers in the organization.

   Note - Make sure that the CA certificate is pushed to the client computer organizational unit.
5. Test the distribution by browsing to an HTTPS site from one of the clients and verifying that the CA certificate shows the name you entered for the CA certificate that you created in the **Issued by** field.

Deploying Certificates by Using Group Policy

You can use this procedure to deploy a certificate to multiple client machines with Active Directory Domain Services and a Group Policy Object (GPO). A GPO can contain multiple configuration options, and is applied to all computers in the scope of the GPO.

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

To deploy a certificate using Group Policy:

1. On the Microsoft Windows Server, open the **Group Policy Management Console**.
2. Find an existing GPO or create a new GPO to contain the certificate settings. Make sure the GPO is associated with the domain, site, or organization unit whose users you want affected by the policy.
3. Right-click the GPO and select **Edit**.

   The **Group Policy Management Editor** opens and shows the contents of the policy object.
4. Open **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Publishers**.
5. Click **Action** > **Import**.

6. Do the instructions in the **Certificate Import Wizard** to find and import the certificate you exported from SmartConsole.
7. In the navigation pane, click **Trusted Root Certification Authorities** and repeat steps 5-6 to install a copy of the certificate to that store.

Configuring Inbound HTTPS Inspection

Configure the Security Gateway for inbound HTTPS Inspection.

To enable inbound HTTPS traffic inspection:

1. From the SmartConsole **Gateways & Servers** view, edit the Security Gateway object.
2. Click **HTTPS Inspection** > **Step 3**.
3. Select **Enable HTTPS Inspection**.
4. Import server certificates for servers behind the organization Security Gateways ("Assigning a Server Certificate for Inbound HTTPS Inspection" on page 126).
5. Define an HTTPS inspection policy:
   - Create rules
   - Add a server certificate to the **Certificate** column of each rule.

Assigning a Server Certificate for Inbound HTTPS Inspection

Add the server certificates to the Security Gateway. This creates a server certificate object

When a client from outside the organization initiates an HTTPS connection to an internal server, the Security Gateway intercepts the traffic. The Security Gateway inspects the inbound traffic and creates a new HTTPS connection from the gateway to the internal server. To allow HTTPS inspection, the Security Gateway must use the original server certificate and private key. The Security Gateway uses this certificate and the private key for SSL connections to the internal servers.

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

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

To add a server certificate for inbound HTTPS inspection:

1. In SmartConsole, go to **Security Policies** > **Shared Policies** > **HTTPS Inspection**.
2. Click **Open HTTPS Inspection Policy In SmartDashboard**.
   SmartConsole opens.
3. Click **Server Certificates**.
4. Click **Add**.
   The **Import Inbound Certificate** window opens.
5. Enter a **Certificate name** and a **Description** (optional).
6. Browse to the certificate file.
7. Enter the **Private key password**. Enter the same password that was used to protect the private key of the certificate on the server.
8. Click **OK**.

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

HTTPS Inspection Policy

The HTTPS Inspection rules define how the Security Gateways inspect HTTPS traffic. The HTTPS Inspection rules can use the URL Filtering categories to identify traffic for different websites and applications. For example, to protect the privacy of your users, you can use a rule to ignore HTTPS traffic to banks and financial institutions.

The HTTPS Inspection rules are applied to all the Software Blades that have HTTPS Inspection enabled. These are the Software Blades that support HTTPS Inspection:

- Access Control
  - Application Control
  - URL Filtering
  - Content Awareness
- Threat Prevention
  - IPS
  - Anti-Virus
  - Anti-Bot
  - Threat Emulation
- Data Loss Prevention

To open the HTTP Inspection Policy

1. In SmartConsole, go to **Security Policies** > **Shared Policies** > **HTTPS Inspection**.
2. Click **Open HTTPS Inspection Policy In SmartDashboard**.

HTTPS Inspection rules in SmartConsole

These are the fields that manage the rules for the HTTPS Inspection security policy.

Field	Description
No.	Rule number in the HTTPS Inspection Rule Base.
Name	Name that the system administrator gives this rule.
Source	Network object that defines where the traffic starts.
Destination	Network object that defines the destination of the traffic.
Services	The network services that are inspected or bypassed. By default, the services `HTTPS` on port 443 and `HTTP_and_HTTPS proxy` on port 8080 are inspected. You can add or delete services from the list.
Site Category	Categories for applications or web sites that are inspected or bypassed.
Action	Action that is done when HTTPS traffic matches the rule. The traffic is inspected or ignored (**Bypass**).

Field	Description
Track	Tracking and logging action that is done when traffic matches the rule.
Install On	Network objects that will get the HTTPS Inspection rule. You can only select Security Gateways that have HTTPS Inspection enabled.
Certificate	The certificate that is used for this rule. • Inbound HTTPS inspection - Select the certificate that the internal server uses. • Outbound HTTPS inspection - Select the Outbound Certificate object that you are using for the computers in the network. When there is a match to a rule, the Security Gateway uses the selected server certificate to communicate with the source client. You can create server certificates from **HTTPS Inspection > Server Certificates > Add**.
Comment	An optional field that lets you summarize the rule.

Configuring HTTPS Inspection Rules

Create different HTTPS Inspection rules for outbound and inbound traffic.

The outbound rules use the certificate that was generated for the Security Gateway.

The inbound rules use a different certificate for each internal server.

You can also create bypass rules for traffic that is sensitive and is not inspected. Make sure that the bypass rules are at the top of the HTTPS Inspection Rule Base.

After creating the rules, install the Access Control Policy.

Sample HTTPS Inspection Rule Base

This table shows a sample HTTPS Inspection Rule Base for a typical policy. (The **Track** and **Install On** columns are not shown. **Track** is set to **None** and **Install On** is set to **Any**.)

No	Name	Source	Destination	Services	Site Category	Action	Blade	Certificate
1	Inbound traffic	Any	WebCalendar Server	HTTPS	Any	Inspect	Any	WebCalendarServer CA
2	Financial sites	Any	Internet	HTTPS HTTP_HTTPS_proxy	Financial Services	Bypass	Any	Outbound CA
3	Outbound traffic	Any	Internet	HTTPS HTTP_HTTPS_proxy	Any	Inspect	Any	Outbound CA

1. **Inbound traffic** - Inspects HTTPS traffic to the network object WebCalendarServer. This rule uses the WebCalendarServer certificate.
2. **Financial sites** - This is a bypass rule that does not inspect HTTPS traffic to websites that are defined in the Financial Services category. This rule uses the Outbound CA certificate.
3. **Outbound traffic** - Inspects HTTPS traffic to the Internet. This rule uses the Outbound CA certificate.

Bypassing HTTPS Inspection for Software Update Services

Check Point dynamically updates a list of approved domain names of services from which content is always allowed. This option makes sure that Check Point updates or other 3rd party software updates are not blocked. For example, updates from Microsoft, Java, and Adobe.

To bypass HTTPS inspection for software updates:

1. In SmartConsole, go **Manage & Settings** > **Blades** > **HTTPS Inspection** > **Configure In SmartDashboard**.
2. In SmartDashboard, click the **HTTPS Inspection** tab.
3. Click **Policy**.
4. In the Policy pane, select **Bypass HTTPS Inspection of traffic to well known software update services (list is dynamically updated)**. This option is selected by default.
5. Click **list** to see the list of approved domain names.

Managing Certificates by Gateway

The **Gateways** pane lists the gateways with HTTPS Inspection enabled. Select a gateway and click **Edit** to edit the gateway properties.

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

If the Security Management Server which manages the selected Security Gateway does not have a generated CA certificate installed on it, you can add it with **Import certificate from file**.

- You can import a CA certificate already deployed in your organization.
- You can import a CA certificate from another Security Management Server. Before you can import it, you must first export ("Exporting a Certificate from the Security Management Server" on page 124) it from the Security Management Server on which it was created.

Adding Trusted CAs for Outbound HTTPS Inspection

When a client initiates an HTTPS connection to a web site server, the Security Gateway intercepts the connection. The Security Gateway inspects the traffic and creates a new HTTPS connection from the Security Gateway to the designated server.

When the Security Gateway establishes a secure connection (an SSL tunnel) to the designated web site, it must validate the site server certificate.

HTTPS Inspection comes with a preconfigured list of trusted CAs. This list is updated by Check Point when necessary and is automatically downloaded to the Security Gateway. The system is configured by default to notify you when a Trusted CA update file is ready for installation. The notification in SmartConsole shows as a pop-up notification or in the **Trusted CAs** window in the **Automatic Updates** section. After you install the update, make sure to install the policy. You can select to disable the automatic update option and manually update the Trusted CA list.

If the Security Gateway receives a non-trusted server certificate from a site, by default the user gets a self-signed certificate and not the generated certificate. A page notifies the user that there is a problem with the website security certificate, but lets the user continue to the website.

You can change the default setting to block untrusted server certificates.

Saving a CA Certificate

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

To export a CA certificate:

1. In SmartConsole, open **HTTPS Inspection** > **Trusted CAs**.
2. Click **Actions** > **Export to file**.

3. Browse to a location, enter a file name and click **Save**.
   A CER file is created.

HTTPS Validation

In the **HTTPS Validation** page of SmartConsole you can set options for

- Fail mode
- HTTPS site categorization mode
- Server validation.
- Certificate blacklisting
- Troubleshooting

To learn more about these options, see the Help. Click **?** in the **HTTPS Validation** page.

Showing HTTPS Inspection Logs

The predefined log query for HTTPS Inspection shows all HTTPS traffic that matched the HTTPS Inspection policy, and was configured to be logged.

To see HTTPS Inspection Logs:

1. In the SmartConsole **Logs & Monitor** > **Logs** tab, click **Favorites**.
2. Select the **HTTPS Inspection** query.

The logs includes an **HTTP Inspection Action** field. The field value can be *inspect* or *bypass*. If HTTPS Inspection was not done on the traffic, this field does not show in the log.

HTTP Inspection on Non-Standard Ports

Applications that use HTTP normally send the HTTP traffic on TCP port 80. Some applications send HTTP traffic on other ports also. You can configure some Software Blades to only inspect HTTP traffic on port 80, or to also inspect HTTP traffic on non-standard ports.

When selected, the Threat Prevention policy inspects all HTTP traffic, even if it is sent using nonstandard ports. This option is selected by default. You can configure this option in the **Manage & Settings** view > **Blades** > **Threat Prevention** > **Advanced Settings**.

Using Anti-Spam and Mail

In This Section:

Introduction to Anti-Spam and Mail Security

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

Feature	Explanation
Content based Anti-Spam	The core of the Anti-Spam functionality is the content based classification engine.
IP Reputation Anti-Spam	Using an IP reputation service, most of the incoming spam is blocked at connect time.
Block List Anti-Spam	Block specific senders based on IP address or sender's address.
Mail Anti-Virus	Scan and filter mail for malware.
Zero Hour Malware Protection	Filter mail using rapid response signatures.
IPS	Intrusion prevention system for mail protection.

Mail Security Overview

On the **Anti-Spam & Mail** tab:

- Select gateways that enforce Anti-Virus checking
- Select gateways that enforce Anti-Spam protection
- Enable automatic updates
- View settings and logs

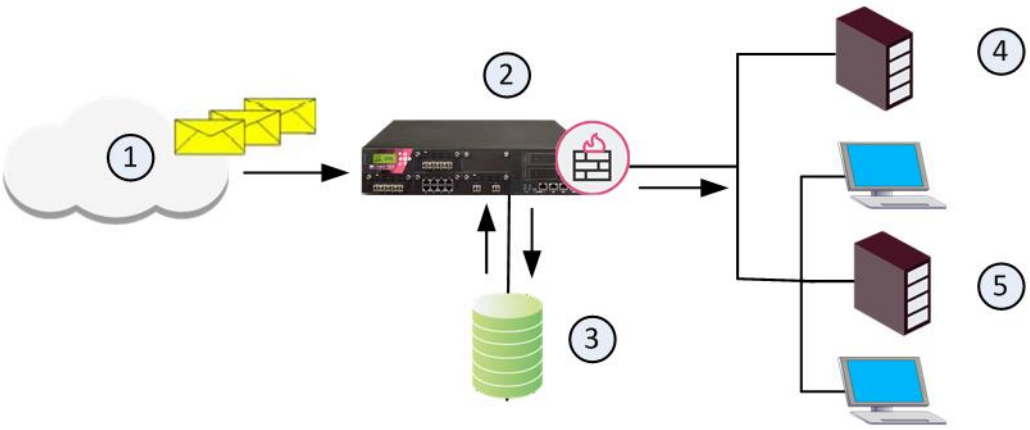
Anti-Spam

The Anti-Spam functionality employs unique licensed technology. Unlike many Anti-Spam applications that rely on searching for keywords and a lexical analysis of the content of an email message, Check Point Anti-Spam identifies spam by analyzing known and emerging distribution patterns. By avoiding a search for key words and phrases that might classify a legitimate email as spam and instead focusing on other message characteristics, this solution offers a high spam detection rate with a low number of false positives.

To preserve personal privacy and business confidentiality, only select characteristics are extracted from the message envelope, headers, and body (no reference to actual content or attachments are included). Hashed values of these message characteristics are sent to a Detection Center for pattern analysis. The Detection Center identifies spam outbreaks in any language, message format, or encoding type. Responses are returned to the enterprise gateway within 300 milliseconds.

Once identified, the network of spam generating machines is blacklisted. If the network changes its behavior, it is removed from the black list.

This figure illustrates the Anti-Spam workflow:



Item	Description
1	Internet
2	Proxy SMTP server
3	Detection Center
4	Enterprise front-end mail server in DMZ
5	Internal network

1. Proxy SMTP server on the gateway receives incoming mail.
2. The SMTP proxy uses the Anti-Spam daemon to extract selected message characteristics, and produce a hash fingerprint.
3. The Anti-Spam daemon queries the Detection Center with a special Anti-Spam protocol. The hashed fingerprint is compared to other fingerprints in the pattern repository to determine whether the email is spam.
4. The Detection Center classifies the email as spam or not spam, and returns the result to the gateway.
5. If the Detection Center classified the email as spam, the email is flagged as such (in the header or subject) and forwarded to the enterprise mail server.
6. The mail server forwards the email to its recipient on the network. Because the header or subject were flagged as spam, recipients can use that tag or marker to set up filtering rules in their native mail program — for example, in **Microsoft Outlook** you can configure a rule to delete all emails with the word SPAM in the subject line or the header.

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

Adaptive Continuous Download

To prevent delays, *Adaptive Continuous Download* starts delivering the email to the recipient while Anti-Spam scanning is still in progress. If the email is designated as Spam, it is flagged as spam before it is completely transferred to the recipient. Both the SMTP and POP3 protocols support Adaptive Continuous Download for the entire email message.

Configuring Anti-Spam

Configuring a Content Anti-Spam Policy

To configure a content Anti-Spam policy:

1. In SmartConsole, select **Manage & Settings** > **Blades** > **Anti-Spam & Mail** > and click **Configure in SmartConsole**.

   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. On the **Overview** page, under **Content based Anti-Spam**, click **Settings**.
3. Use the slider to select an Anti-Spam policy protection level.
4. Select flagging options.
5. In the **Security Gateway Engine settings** section, set a maximum data size to scan.
6. In the **UTM-1 Edge Engine settings** section, set a confidence level for spam and suspected spam.

   A spam confidence level is a grade or rating (usually between zero and a hundred) used decide whether a particular email message should be treated as spam. For example, if the confidence level is set to 70, then all email messages rated at 70 or above will be treated as spam.
7. Select **Tracking Options** for **Spam**, **Suspected Spam**, or **Non Spam**. Tracking options include:
   - None (no logging)
   - Log
   - Popup Alert
   - Mail Alert
   - SNMP trap alert
   - Three custom user-defined scripts.
8. Click **Save** and then close SmartDashboard.
9. From SmartConsole, install the Access Control policy.

Configuring an IP Reputation Policy

1. In SmartConsole, select **Manage & Settings** > **Blades** > **Anti-Spam & Mail** > and click **Configure in SmartConsole**.

   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. On the **Overview** page, under **IP Reputation Anti-Spam**, click **Settings**.
3. Use the slider to select an IP Reputation Policy:
   - **Off** - IP Reputation service is disabled
   - **Monitor** - Monitors known and suspected spam but does not block it
   - **Medium Protection** - Blocks known spam and monitors suspected spam
   - **High Protections** - Blocks known and suspected spam
4. Select tracking options for **Spam**, **Suspected Spam**, or **Non spam**. Tracking options include
   - None (no logging)
   - Log
   - Popup Alert
   - Mail Alert
5. Click **Save** and then close SmartDashboard.

6. From SmartConsole, install the Access Control policy.
   - SNMP trap alert
   - Three custom user-defined scripts.

Configuring a Block List

1. In SmartConsole, select **Manage & Settings** > **Blades** > **Anti-Spam & Mail** > and click **Configure in SmartConsole**.

   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. On the **Overview** page, under **Block List Anti-Spam**, click **Settings**.
3. Use the slider to select a Block Policy:
   - **Off** - Not blocked
   - **Monitor Only** - Not Blocked, but monitors senders by IP address and email address
   - **Block** - Blocks senders by IP address and email address
4. In the **Blocked senders\domains** section, click **Add** and enter the name of a sender or domain to be rejected.
5. In the **Blocked IPs** section, click **Add** and enter an IP address that should be blocked.
6. From the drop-down list in the **Tracking** section, select a tracking option for blocked mail or non-spam.
7. Click **Save** and then close SmartDashboard.
8. From SmartConsole, install the Access Control policy.

Configuring Anti-Spam SMTP

1. In SmartConsole, select **Manage & Settings** > **Blades** > **Anti-Spam & Mail** > and click **Configure in SmartConsole**.

   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. From the navigation tree, click **Advanced** > **SMTP**.
3. Make sure that **Scan SMTP traffic with Anti-Spam engine for Anti-Spam, IP reputation and Block list protection** is selected.
4. Select to scan SMTP traffic **By Mail Direction** or **By IPs**.
5. If you selected scan **By IPs**, click **Add Rule** to configure rules for IP addresses to scan.
6. If you selected scan **By Mail Direction**, select a scanning direction for:
   - Incoming files
   - Outgoing files
   - Internal files through the gateway
7. Select **Activate Continuous Download** to avoid client time-outs when large files are scanned.
8. Click **Save** and then close SmartDashboard.
9. From SmartConsole, install the Access Control policy.

Configuring Anti-Spam POP3

1. In SmartConsole, select **Manage & Settings** > **Blades** > **Anti-Spam & Mail** > and click **Configure in SmartConsole**.

   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. From the navigation tree click **Advanced** > **POP3**.

3. Make sure that **Scan POP3 traffic with Anti-Spam engine for Anti-Spam, IP reputation and Block list protection** is selected.
4. Select to scan POP3 traffic **By Mail Direction** or **By IPs**.
5. If you selected scan **By IPs**, click **Add Rule** to configure rules for IP addresses to scan.
6. If you selected scan **By Mail Direction**, select a scanning direction for:
   - Incoming mail
   - Outgoing mail
   - Internal mail
7. Select **Activate Continuous Download** to avoid client time-outs when large files are scanned.
8. Click **Save** and then close SmartDashboard.
9. From SmartConsole, install the Access Control policy.

Configuring Network Exceptions

To exclude sources and destinations:

1. In SmartConsole, select **Manage & Settings** > **Blades** > **Anti-Spam & Mail** > and click **Configure in SmartConsole**.

   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. From the navigation tree click **Advanced** > **Network Exceptions**.
3. Select **Enforce the Anti-Spam policy on all traffic except for traffic between the following sources and destinations**.
4. Click **Add**. The **Network Exception** window opens.
5. For **Source** and **Destination**, select **Any**, or select **Specific** and one gateway from each list.
6. Click **OK**.
7. Click **Save** and then close SmartDashboard.
8. From SmartConsole, install the Access Control policy.

Configuring an Allow List

1. In SmartConsole, select **Manage & Settings** > **Blades** > **Anti-Spam & Mail** > and click **Configure in SmartConsole**.

   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. From the navigation tree click **Advanced** > **Allow List**.
3. In the **Allowed Senders / Domains** section, click **Add** and enter the name of a sender or domain to be allowed.
4. In the **Allowed IPs** section, click **Add** and enter an allowed IP address.
5. From the drop-down list in the **Tracking** section, select a tracking option.
6. Click **Save** and then close SmartDashboard.
7. From SmartConsole, install the Access Control policy.

Selecting a Customized Server

To select a data center:

1. In SmartConsole, select **Manage & Settings** > Blades > **Anti-Spam** & Mail > and click **Configure in SmartConsole**.

SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. From the navigation tree click **Advanced** > **Customized Server**.
3. Select **Use Customized Server**.
4. From the drop-down list, select a server.
5. Click **Save** and then close SmartDashboard.
6. From SmartConsole, install the Access Control policy.

Anti-Spam on UTM-1 Edge Devices

Anti-Spam protection is available on UTM-1 Edge devices.

To configure Anti-Spam on UTM-1 Edge devices:

1. Open the **General Properties** window of the UTM-1 Edge gateway.
2. Select **Anti-Spam**.

Bridge Mode and Anti-Spam

If an UTM-1 appliance is configured to run in bridge mode, Anti-Spam is supported providing that:

- The bridge interface has an IP address
- The bridge interface has a default gateway

Configuring Anti-Virus Protection for Mail

Configuring Mail Anti-Virus

To configure a mail Anti-Virus policy:

1. In SmartConsole, select **Manage & Settings** > **Blades** > **Anti-Spam & Mail** > and click **Configure in SmartConsole**.
   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. From the navigation tree, select **Traditional Anti-Virus** > **Security Gateway** > **Mail Protocols > Mail Anti-Virus**.
3. Set the slider to **Block**.
4. Select tracking options for either all POP3 and SMTP mail, or just blocked mail. Tracking options include:
   - None (no logging)
   - Log
   - Popup alert
   - Mail alert
   - SNMP trap alert
   - Three custom user-defined scripts
5. Click **Save** and then close SmartDashboard.
6. From SmartConsole, install the Access Control policy.

Configuring Zero Hour Malware Protection

1. In SmartConsole, select **Manage & Settings** > **Blades** > **Anti-Spam & Mail** > and click **Configure in SmartConsole**.

   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. From the navigation tree, select **Traditional Anti-Virus** > **Security Gateway** > **Mail Protocols > Zero Hour Malware Protection**.
3. With the slider, select a Zero hour malware protection level:
   - Off
   - Monitor Only
   - Block
4. Select tracking options for blocked, SMTP and POP3 mail. Tracking options include:
   - None (no logging)
   - Log
   - Popup alert
   - Mail alert
   - SNMP trap alert
   - Three custom user-defined scripts
5. Click **Save** and then close SmartDashboard.
6. From SmartConsole, install the Access Control policy.

Configuring SMTP and POP3

1. Using the slider, select a protection level:
   - Off
   - Monitor Only - SMTP and HTTP are the only protocols that support this protection level
   - Block
2. When you scan by File Direction, select a scanning direction for:
   - Incoming files
   - Outgoing files
   - Internal files through the gateway
3. When you scan by IPs, create rules for the Rule Base to define the source and destination of the data to be scanned.
4. 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 143) for further information. FTP and POP3 are set to Proactive Detection mode automatically.
5. If Proactive Detection was configured, select the **Activate Continuous Download** checkbox to prevent client time-outs when large files are scanned.

   See Continuous Download (on page 144) for further information.
6. In SmartConsole, select **Manage & Settings** > **Blades** > **Anti-Spam & Mail** > and click **Configure in SmartConsole**.

   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
7. From the navigation tree, select **Traditional Anti-Virus** > **Security Gateway** > **Mail Protocols > SMTP** or **POP3**.

8. Click **Save** and then close SmartDashboard.
9. From SmartConsole, install the Access Control policy.

Configuring File Types

1. In SmartConsole, select **Manage & Settings** > **Blades** > **Anti-Spam & Mail** > and click **Configure in SmartConsole**.

   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. From the navigation tree, select **Traditional Anti-Virus** > **Security Gateway** > **File Types.**
3. Configure the file types.
4. Optional: Click **Update** to select a file to use to update the list.
5. Click **Save** and then close SmartDashboard.
6. From SmartConsole, install the Access Control policy.

Configuring Settings

1. In SmartConsole, select **Manage & Settings** > **Blades** > **Anti-Spam & Mail** > and click **Configure in SmartConsole**.

   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. From the navigation tree, select **Traditional Anti-Virus** > **Security Gateway** > **Settings.**
3. In the **Scan Failure** section, select the default behavior if there are problems with the scan.
4. In the **File Handling** section, select the maximum file size to scan and the default behavior if the file exceeds the size limit.
5. In the Archive Handling section, select the maximum nesting level to scan, the compression ratio, and the default behavior if the file exceeds the limits or cannot be extracted.
6. Click **Save** and then close SmartDashboard.
7. From SmartConsole, install the Access Control policy.

Configuring a Disclaimer

1. In SmartConsole, select **Manage & Settings** > **Blades** > **Anti-Spam & Mail** > and click **Configure in SmartConsole**.

   SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2. From the navigation tree, select **Advanced** > **Disclaimer**.
3. Select **Add disclaimer to email scanned by Anti-Virus and Anti-Spam engines**.
4. In the text box, type your disclaimer notice.
5. Click **Save** and then close SmartDashboard.
6. From SmartConsole, install the Access Control policy.

Anti-Spam Logging and Monitoring

Anti-Spam logging and monitoring options are available in the **Logs & Monitor** view in SmartConsole.

Logs derived from Anti-Spam scanning are sent to Security Management Server, and show in the **Logs & Monitor** > **Logs** view. In the **Logs & Monitor** view, you can see detailed views (on page 72) and reports (on page 73) of the Anti-Spam activity, customize these views and reports, or generate new ones.

Using Traditional Anti-Virus

In This Appendix

Managing Traditional Anti-Virus

Traditional Anti-Virus inspection uses these detection modes:

- Proactive mode - a file-based solution where the kernel traps the traffic for the selected protocols and forwards the traffic 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 - the kernel processes the traffic for the selected protocols 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. You can configure the SMTP and HTTP protocols to work in Proactive or Stream mode. Anti-Virus scanning is applied only to accepted traffic that was allowed by the security policy.

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

Database Updates

The following kinds of database updates are available:

- **Automatic Update**: Updates of the virus signature can be scheduled at a predefined interval.
- **Manual Update**: 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

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 set file scanning according to the file's (and not necessarily the connection's) origin and destination.

Scan by IPs enables you to set 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 scanned, select **Scan by File Direction**.

If you want a connection or part of a connection's source or destination to be scanned, select **Scan by IPs**.

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.

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 SmartConsole 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 though 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 142).

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 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. With 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.

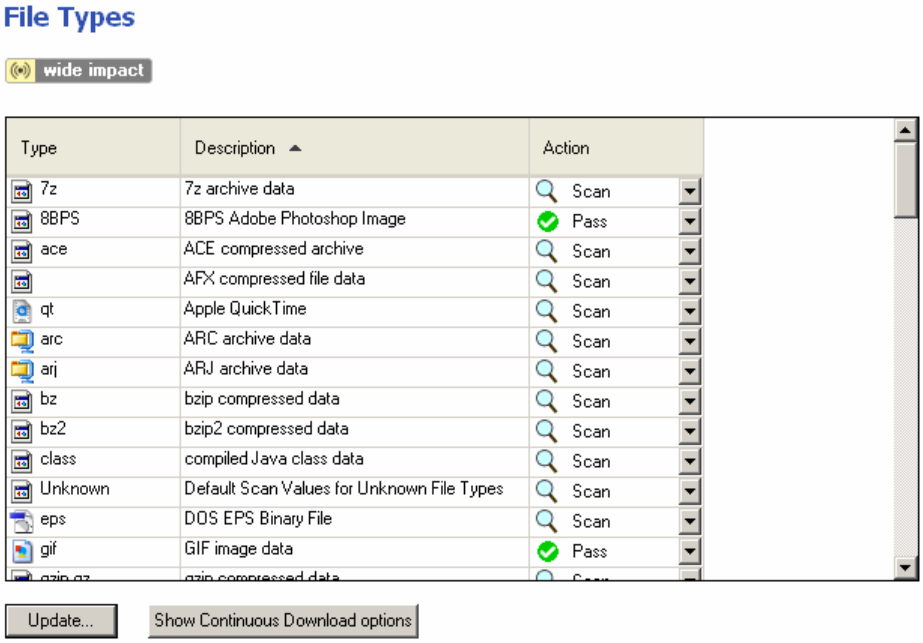
1. In the **Traditional Anti-Virus** tab, click **Traditional Anti-Virus** > **Security Gateway** > **Mail Protocols** > **SMTP, POP3, FTP** or **HTTP**.

2. With the slider, select a protection level:
   - Off
   - Monitor Only - SMTP and HTTP are the only protocols that support this protection level
   - Block
3. For a scan by File Direction, select a scanning direction for:
   - Incoming files
   - Outgoing files
   - Internal files through the gateway
4. For a scan by IPs, create rules for the Rule Base to set the source and destination of the data to be scanned.
5. For SMTP and HTTP, select **Activate Proactive Detection (impacts performance)** 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 143) for further information. FTP and POP3 are set to Proactive Detection mode automatically.
6. If Proactive Detection was configured, select **Activate Continuous Download** to prevent client time-outs when large files are scanned.

   See Continuous Download (on page 144) for further information.

Configuring File Types

You can set an action to take place when a file of a specified type passes through the gateway, so that it is not 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** tab, click **Traditional Anti-Virus** > **Security Gateway** > **File Types** page and set the actions. See File Type Recognition (on page 144) for more information.

In this window, you can also configure **Continuous Download options**. **Continuous Download options** are only relevant if the scan is set to Proactive Detection. See Continuous Download (on page 144) 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

These scan failure options are available:

- **When Traditional Anti-Virus engine is overloaded or scan fails**: Defines if the gateway passes or blocks the files.
- **When Traditional Anti-Virus engine fails to initialize**: Defines if the gateway passes or blocks the files.

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 a file exceeds size 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

These 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 nesting or compression exceeds limit or extraction fails**: Defines if the gateway passes or blocks the files.

Logging and Monitoring

Traditional Anti-Virus logging and monitoring options are available in the **Logs & Monitor** tab in SmartConsole.

Logs derived from Traditional Anti-Virus scanning are sent to Security Management Server, and show in the **Logs & Monitor** > **Logs** tab. In the **Logs & Monitor** tab, you can see detailed views (on

page 72) and reports (on page 73) of the Traditional Anti-Virus activity, customize these views and reports, or generate new ones.

UTM-1 Edge Traditional Anti-Virus

You can now enable Traditional Anti-Virus protection within UTM-1 Edge. When you select the **Enable Traditional Anti-Virus** option, the Traditional Anti-Virus protection is installed and updates are sent to the specified gateway.

With 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 or destination is scanned. Files set for scanning are defined in the classic Rule Base, which defines the source and destination of the connection to be scanned.

Best Practice - 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.

Appendix: Regular Expressions

In This Section:

Regular Expression Syntax

This table shows the Check Point implementation of standard regular expression metacharacters.

Metacharacter	Name	Description
\	Backslash	escape metacharacters non-printable characters character types
[ ]	Square Brackets	character class definition
( )	Parenthesis	sub-pattern, to use metacharacters on the enclosed string
{min[,max]}	Curly Brackets	min/max quantifier {n} - exactly n occurrences {n,m} - from n to m occurrences {n,} - at least n occurrences
.	Dot	match any character
?	Question Mark	zero or one occurrences (equals {0,1})
*	Asterisk	zero or more occurrences of preceding character
+	Plus Sign	one or more occurrences (equals {1,})
|	Vertical Bar	alternative
^	Circumflex	anchor pattern to beginning of buffer (usually a word)
$	Dollar	anchor pattern to end of buffer (usually a word)
-	hyphen	range in character class

Using Non-Printable Characters

To use non-printable characters in patterns, escape the reserved character set.

Character	Description
\a	alarm; the BEL character (hex 07)
\cx	"control-x", where x is any character
\e	escape (hex 1B)
\f	formfeed (hex 0C)
\n	newline (hex 0A)
\r	carriage return (hex 0D)
\t	tab (hex 09)
\ddd	character with octal code ddd
\xhh	character with hex code hh

Using Character Types

To specify types of characters in patterns, escape the reserved character.

Character	Description
\d	any decimal digit [0-9]
\D	any character that is not a decimal digit
\s	any whitespace character
\S	any character that is not whitespace
\w	any word character (underscore or alphanumeric character)
\W	any non-word character (not underscore or alphanumeric)

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):

Regular Expression	`.*\.example\.com`	
Wildcard	`*.example.com`	**Important!** If you use this string as a regular expression, policy install fails. The gateway cannot resolve the regular expression to a URL, because there is no preceding character to find.

More examples of regular expressions:

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

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