QUANTUM

02 February 2025

THREAT PREVENTION

R81.20

Administration Guide

CHECK POINT™

Check Point Copyright Notice

Important Information

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

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

Check Point R81.20
For more about this release, see the R81.20 home page.

Latest Version of this Document in English
Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

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

Revision History

Date	Description
21 January 2025	Updated *"MITRE ATT&CK" on page 490*
5 January 2025	Updated *"The Check Point Threat Prevention Solution" on page 26*
22 November 2024	Added *"Malware Prevention Using IP and Port Indicators" on page 81*
09 July 2024	Updated *"Configuring Anti-Bot Settings" on page 76*
11 March 2024	Updated: ■ *"Configuring IPS Protections for Custom Threat Prevention" on page 66* ■ *"Threat Prevention API " on page 391*
04 December 2023	Updated *"Configuring Threat Emulation Settings on the Security Profile" on page 96*
27 November 2023	Updated *" SSH Deep Packet Inspection - Custom Threat Prevention" on page 283*
18 October 2023	Updated *"Configuring Anti-Virus Settings" on page 83*
01 September 2023	Updated *"Configuring the Security Gateway as a Mail Transfer Agent" on page 170*
14 August 2023	Updated *"Configuring Zero Phishing Settings - Custom Threat Prevention" on page 125*
1 August 2023	Updated *"Exception Rules" on page 130*
8 June 2023	Updated: ■ *"Threat Prevention and UserCheck - Custom Threat Prevention" on page 246* ■ *"Threat Prevention and UserCheck - Autonomous Threat Prevention" on page 327*

Date	Description
15 May 2023	Updated: - *"Threat Prevention and UserCheck - Autonomous Threat Prevention" on page 327* - *"Threat Prevention and UserCheck - Custom Threat Prevention" on page 246*
2 May 2023	Updated: - *"Configuring IPS Protections for Custom Threat Prevention" on page 66* - *"IPS Protections" on page 321*
22 February 2023	Added: - *"Cyber Attack View - Gateway" on page 433* - Cyber Attack View - Mobile - *"MITRE ATT&CK" on page 490* - *"Log Fields" on page 496* Updated: - *"Monitoring Threat Prevention - Autonomous Threat Prevention" on page 370* - *"Monitoring Threat Prevention - Custom Threat Prevention" on page 271*
January 31, 2023	Updated *"The Threat Prevention Policy" on page 42*
January 2, 2023	General Updates
20 November 2022	First release of this document

Table of Contents

About This Guide

There are two ways to configure Threat Prevention:

- Custom Threat Prevention - In Custom Threat Prevention, you create your own Security Policy and configure the policy rules manually.
- Autonomous Threat Prevention - Autonomous Threat Prevention includes pre-defined security profiles. When you select a security profile, the Security Policy is created automatically.

You can install either Autonomous Threat Prevention or Custom Threat Prevention on each gateway, but not both.

This guide is divided into three chapters:

- Custom Threat Prevention configuration (*"Custom Threat Prevention" on page 34*).
- Autonomous Threat Prevention configuration (*"Autonomous Threat Prevention" on page 299*).
- Common configuration - which includes configurations that are common for both Custom Threat Prevention and Autonomous Threat Prevention (*"Common Features in Custom Threat Prevention and Autonomous Threat Prevention" on page 381*

The Check Point Threat Prevention Solution

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 protections 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 protection 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 protection is continuously updated from ThreatCloud. It detects and blocks malware by correlating multiple detection engines before users are affected.

- **SandBlast**

  Protection against infections from undiscovered exploits, zero-day and targeted attacks using:

  Threat Emulation

  This innovative solution quickly inspects files and runs them in a virtual sandbox to discover malicious behavior. Discovered malware is prevented from entering the network. The Emulation service reports to the ThreatCloud and automatically shares the newly identified threat information with other customers.

Threat Extraction

Protection against incoming malicious content. The extraction capability removes exploitable content, including active content and embedded objects, reconstructs files to eliminate potential threats, and promptly delivers sanitized content to users to maintain business flow. To remove possible threats, Threat Extraction creates a safe copy of the file, while the inspects the original file for potential threats.

Zero Phishing

Zero Phishing prevents unknown zero-day and known phishing attacks on websites in real-time, by utilizing industry leading Machine-Learning algorithms and patented inspection technologies.

Each protection is unique. When combined, they supply a strong Threat Prevention solution. Data from malicious attacks are shared between the Threat Prevention protections 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 protections.

IPS

The IPS protection 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

The IPS protection includes:

- Detection and prevention of specific known exploits
- Detection and prevention of vulnerabilities, including both known and unknown exploit tools, for example protection from specific CVEs
- Detection and prevention of protocol misuse which in many cases indicates malicious activity or potential threat. Examples of commonly manipulated protocols are HTTP, SMTP, POP, and IMAP
- Detection and prevention of outbound malware communications
- Detection and prevention of tunneling attempts. These attempts may indicate data leakage or attempts to circumvent other security measures such as web filtering

- Detection, prevention or restriction of certain applications which, in many cases, are bandwidth consuming or may cause security threats to the network, such as Peer to Peer and Instant Messaging applications
- Detection and prevention of generic attack types without any pre-defined signatures, such as Malicious Code Protector

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

Capabilities of IPS

The unique capabilities of the Check Point IPS engine include:

- Clear, simple management interface
- Reduced management overhead by using one management console for all Check Point products
- Integrated management with SmartConsole
- Easy navigation from business-level overview to a packet capture for a single attack
- #1 security coverage for Microsoft and Adobe vulnerabilities
- Resource throttling so that high IPS activity does not impact other Threat Prevention 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 does the following

- 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 protection scans incoming and outgoing files to detect and prevent these threats, and provides pre-infection protection from malware contained in these files. The Anti-Virus protection is also supported by the Threat Prevention API (see *"Threat Prevention API " on page 391*).

The Anti-Virus protection

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

SandBlast

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

Threat Emulation

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

Threat Emulation receives files through these methods of delivery

- E-mail attachments transferred using the SMTP or SMTPS protocols
- Web downloads

- Files sent to Threat Emulation through the Threat Prevention API (see *"Threat Prevention API " on page 391*)
- Files transferred using FTP and SMB protocols
- E-mail attachments transferred using the IMAP protocol

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.

To learn more about Threat Emulation (see *"The Threat Emulation Solution" on page 88*).

Threat Extraction

Threat Extraction is supported on R77.30 and higher.

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

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

Threat Extraction receives files through these methods of delivery

- E-mail attachments received through the Mail Transfer Agent (see *"Configuring the Threat Prevention Profile and Rules" on page 59*)
- Web downloads (see *"Configuring Threat Extraction Settings" on page 112*)
- Files sent to Threat Extraction through the Threat Prevention API (see *"Threat Prevention API " on page 391*)

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 above.

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

Zero Phishing

Zero Phishing is a new technology and a Threat Prevention protection introduced in R81.20.

Zero Phishing prevents unknown zero-day and known phishing attacks on websites in real-time, by utilizing industry leading Machine-Learning algorithms and patented inspection technologies.

Phishing attacks continue to play a dominant role in the digital threat landscape, which is becoming more mature and sophisticated. Most cyber-attacks start with a phishing attempt.

The Check Point Zero Phishing protection scans the web traffic on the Security Gateway and sends it to the Check Point Cloud for scanning. This way, the Zero Phishing protection prevents access to the most sophisticated phishing websites, both known and completely unknown (zero-day phishing websites).

Because the protection is initiated on the network Security Gateway, the protection is browser-agnostic and platform-agnostic and it does not depend on an email security solution.

Protections usually provided by endpoint or email solutions are now available through the Security Gateway, with no need to install and maintain clients on any device.

The Zero Phishing protection uses two main engines:

1. **Real-time phishing prevention based on URLs**

   The engine prevents both known and unknown zero-day phishing attacks, by analyzing various features on the URL in real-time. The engine sends the URL information to the URL-reputation cloud service to perform the analysis. For example: brand similarity, non-ASCII characters and time of registration.

   Using Machine-Learning, the risk is calculated and URLs are classified as phishing and blocked.

2. **In-browser Zero Phishing**

   The Security Gateway performs patented Java Script injection to scan HTML forms when they are loaded on the browser (including dynamic forms).

   When the end-user clicks the input fields in the form, all HTML components are scanned in real-time, and the information is sent to the Check Point Zero Phishing cloud service for AI-based analysis.

   The risk is calculated and the phishing site is blocked accordingly.

Notes -

- If both SandBlast Agent for Browsers and Zero Phishing protections are active for the same user, the SandBlast Agent for Browsers protection takes precedence over the Zero Phishing protection.
- Zero Phishing is supported with VSX, ClusterXL High Availability and ClusterXL Load Sharing.
- Site scanning in Internet Explorer is not supported.
- JavaScript injection for HTTP 2.0 connections is not supported.
- In-browser Zero Phishing for mirrored traffic is not supported.
- When the Security Gateway is configured as the HTTP/HTTPS Proxy in the "Non Transparent" mode, internal users must have a direct access to the UserCheck Portal on the Security Gateway. In their web-browsers, internal users must add the FQDN of the Zero Phishing Portal to the Proxy Bypass List.

Custom Threat Prevention

Custom Threat Prevention lets you plan your policy independently based on the needs of your organization. With Custom Threat Prevention, you create your own Security Policy and configure the policy rules manually. If you prefer to create your Threat Prevention policy automatically and not manually, see *"Autonomous Threat Prevention" on page 299*.

Getting Started with Custom Threat Prevention

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.

1. Enable Custom Threat Prevention Software Blades in the Security Gateway / Cluster object.

Enabling the IPS Software Blade

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

Enabling the Anti-Bot Software Blade

Step	Instructions
1	In the **Gateways & Servers** view, double-click the Security Gateway / Cluster object. The **General Properties** window opens.
2	In the **General Properties** > **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** - Packet are allowed, but the traffic is logged according to the settings in the Threat Prevention Rule Base.
4	Click **OK**.

Enabling the Anti-Virus Software Blade

Step	Instructions
1	In the **Gateways & Servers** view, double-click the Security Gateway / Cluster object. The **General Properties** window opens.
2	In the **General Properties** > **Network Security** tab, select **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**.

Enabling the Threat Emulation Software Blade

When you enable Threat Emulation, the wizard automatically gives you the option to enable Threat Extraction.

Step	Instructions
1	In the **Gateways & Servers** view, double-click the Security Gateway / Cluster object. The **Gateway Properties** window opens.
2	In the **General Properties** > **Network Security** tab, select **SandBlast Threat Emulation**. The Threat Emulation wizard opens and shows the **Emulation Location** page.
3	Select the **Emulation Location:** ■ **ThreatCloud Emulation Service** ■ **Locally on this Threat Emulation appliance** ■ **Other Threat Emulation appliances**

Step	Instructions
4	Click **Next**. The **Activate Threat Extraction** window opens, with this checkbox selected: **Clean potentially malicious parts from files (Threat Extraction)** ■ To activate Threat Extraction, keep this checkbox selected: ■ If you do not want to activate Threat Extraction, clear this checkbox.
5	Click **Next**. The **Summary** page opens. **Note** - If you selected the **Emulation Location** as **Locally on this Threat Emulation appliance** or **Other Threat Emulation appliances**, and you want to share Threat Emulation information with ThreatCloud, select **Share attack information with ThreatCloud**.
6	Click **Finish** to enable Threat Emulation (and if selected, Threat Extraction), and then close the First Time Configuration Wizard.
7	Click **OK**. The **Gateway Properties** window closes.

Note - When a trial license is installed on the Security Gateway, a green "V" incorrectly appears next to the Threat Emulation Software Blade (in SmartConsole, go to the **Gateways & Servers** view > right-click the Security Gateway / Cluster object > click **Monitor**) > the **Device and License Information** window opens > **Device Status** > **Threat Emulation**).
To see the correct license status, go to the **License Status** tab in the **Device and License Information** window.

Using Cloud Emulation

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

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

Enabling the Threat Extraction Software Blade

Step	Instructions
1	In the **Gateways & Servers** view, double-click the Security Gateway / Cluster object. The **General Properties** window opens.
2	In the **General Properties** > **Network Security** tab, and select **Threat Extraction**. **Note** - In a ClusterXL High Availability environment, do this once for the cluster object.

Notes:

- When you enable Threat Extraction, web download scan is automatically enabled.
- For Threat Extraction to scan e-mail attachments, configure the Security Gateway as a Mail Transfer Agent (MTA) (see *"Configuring the Security Gateway as a Mail Transfer Agent" on page 170*).
- For Threat Extraction API support, in the Security Gateway Properties, go to **Threat Extraction > Web API > Enable API**.

Enabling the Zero Phishing Software Blade

Step	Instructions
1	In the **Gateways & Servers** view, double-click the Security Gateway / Cluster object. The **General Properties** window opens.
2	In the **General Properties** > **Network Security** tab, select **Zero Phishing**. The Zero Phishing First Time Configuration Wizard opens
3	If **HTTPS Inspection** is enabled, enter the Fully Qualified Domain Name (FQDN) for the Security Gateway / Cluster, and click **Next**. If HTTPS Inspection is disabled, this page does not appear. **Notes:** ▪ For In-browser Zero Phishing protection to work, you must have a certificate on the Zero Phishing portal and configure a Fully Qualified Domain Name (FQDN) on the Security Gateway / each Cluster Member. The First Time Configuration Wizard generates a certificate automatically using the HTTPS Inspection certificate. If HTTPS Inspection is not active, the certificate is not required and cannot be generated. ▪ The FQDN must be in the DNS records of your DNS server.

Step	Instructions
4	The Zero Phishing Software Blade is now active. **Notes:** ■ If HTTPS Inspection is disabled, we recommend to enable it. ■ For Zero Phishing to work, you must install both the Access Control and the Threat Prevention policies.

Notes:

- Make sure that Zero Phishing portal is configured to work on a public IP address. For more information, see sk178769.
- To ensure that the configuration was applied successfully, visit this page both with HTTP and HTTPS:

  ```
  http://zp-demo.com/verification/zphi_check.html
  https://zp-demo.com/verification/zphi_check.html
  ```

  If the test is successful, this message appears: **In-Browser Zero Phishing feature is working properly**

2. Optional: Create your Custom Threat Prevention profiles based on the default Custom Threat Prevention profiles.

   See *"Threat Prevention Profiles" on page 52*.

3. Optional: Configure advanced Threat Prevention settings:

   - **Security Gateway** / **Cluster** object - Settings for Threat Prevention Software Blades and features.
   - **Security Policies** view > **Threat Prevention** > **Exceptions**
   - **Security Policies** view > **Threat Prevention** > click **Custom Policy** > refer to the **Custom Policy Tools** section
   - **Security Policies** view > **HTTPS Inspection**
   - **Manage & Settings** view > **Blades** > **Threat Prevention** > **Advanced Settings**
   - **Security Gateway** / each **Cluster Member** command line - Configuration commands and files (for example, for SSH Deep Inspection)

4. Configure the Custom Threat Prevention policy.

   Procedure

   If the default rule is not enough for your environment, configure the required rules. See *"Configuring the Threat Prevention Profile and Rules" on page 59*.

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 value equals any, see *"Protected Scope" on page 47*) is inspected for all protections according to the **Optimized** profile (see *"Profiles Pane" on page 53*). By default, logs are generated and the rule is installed on all Security Gateways that use a Threat Prevention Software Blade.

Name	Protected Scope	Action	Track	Install On

Out-of-the-box Threat Prevention policy	`*Any`	**Optimized**	`Log`
			`Packet Capture`
				`*Policy Targets`

Notes:

- The **Optimized** profile is installed by default (see *"Optimized Protection Profile Settings" on page 53*).
- The **Protection/Site** column is used only for protection exceptions (see *"Protection" on page 49*).

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

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

5. Install the Custom Threat Prevention policy.

Procedure

The Custom Threat PreventionSoftware 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.

Step	Instructions
1	From the Global toolbar, click **Install Policy**. The **Install Policy** window opens showing the installation targets (Security Gateways).
2	Select **Threat Prevention**.
3	Select the **Install Mode**: ■ **Install on each selected gateway independently** Install the policy on the selected Security Gateways without reference to the other targets. A failure to install on one Security Gateway does not affect policy installation on other gateways. If the gateway is a member of a cluster, install the policy on all the members. The Security Management Server makes sure that it can install the policy on all the members before it installs the policy on one of them. If the policy cannot be installed on one of the members, policy installation fails for all of them. ■ **Install on all selected gateways, if it fails do not install on gateways of the same version** Install the policy on all installation targets. If the policy fails to install on one of the Security Gateways, the policy is not installed on other targets of the same version.
4	Click **OK**.

Disabling the Threat Prevention Blades

When you disable all the Threat Prevention Software Blades in a Security Gateway object, you must click the "**Install Policy**" button and then click the "**Uninstall Threat Prevention Policy**" link.

Monitoring

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

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

Step	Instructions
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 Policy Packages.
4	Optional: For each Policy Package, create Threat Prevention Policy Layers. **Note** - For each Policy Layer, configure a Threat Prevention Rule Base with the Threat Prevention profile as the *Action* of the rule.
5	Install the Threat Prevention policy.

Assigning Administrators for Threat Prevention

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

To Learn More about Policy Packages

To learn more about Policy Packages, see the *R81.20 Security Management Administration Guide*.

Threat Prevention Policy Layers

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

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

Important - When the Threat Prevention blades run in MTA mode, the gateway enforces the automatic MTA rule, which is created when MTA is enabled on the gateway.

Action Enforcement in Multiple-Layered Security Policies

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

Example 1

The Layers "IPS" and "Threat Prevention" are pre-defined.

	IPS Layer	Threat Prevention Layer
Rule matched	Rule 3	Rule 1
Profile action	Prevent	Detect

Enforced action: Prevent

Example 2

The Layers "IPS" and "Threat Prevention" are pre-defined.

	IPS Layer	Threat Prevention Layer
Rule matched	Rule 3	Rule 1
Profile action	Prevent	Detect
Exception for protection X	Inactive	-

Enforced action for protection X: Detect

Example 3

These Layers are user-defined.

	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

These Layers are user-defined.

	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:

Allow combined with the maximum nesting level/scanning time,

OR

Block combined with the minimum nesting level/scanning time,

OR

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

Example 6

This example is for UserCheck.

These Layers are user-defined.

The first Layer with the strictest action is enforced.

Enforced Action: Prevent with UserCheck Page B.

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

Creating a New Policy Layer

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

To create a new Threat Prevention Layer

Step	Instructions
1	In SmartConsole, go to **Security Policies** > **Threat Prevention**.
2	Right-click **Policy** and select **Edit Policy**.
3	In the **General** tab, go to **Threat Prevention** and click the **+** sign.
4	Select **New Layer**. The **New Threat Prevention Layer** window opens.
5	Enter the Layer Name.
6	Optional: In the **General** tab, in the **Sharing** area, you can configure reuse of the layer in different policy packages. Select **Multiple policies and rules can use this layer**.
7	In the **Permissions** tab, select the permission profiles that can edit this layer. **Note** - There is no need to add permission profiles that are configured to edit all layers.
8	Click **OK**.

Threat Prevention Layers in Pre-R80 Gateways

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

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

- For pre-R80 gateways with IPS and Threat Prevention Software Blades enabled, the policy is split into two parallel layers: IPS and Threat Prevention.

  To see which Security Gateway enforces which IPS profile, look at the **Install On** column in the IPS Layer.

- R80.XX gateways are managed separately, based on the R80 or higher Policy Layers (see *"Threat Prevention Policy Layers" on page 43*).

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

Threat Prevention Rule Base

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

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

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

Parts of the Rules

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

Number (No.)

The sequence of rules is important because the first rule that matches traffic according to a protected scope (see *"Protected Scope" on the next page*) 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

1. Give the rule a descriptive name. The name can include spaces.
2. Double-click in the **Name** column of the rule to add or change a name.
3. 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. From R80.10, dynamic objects and domain objects are also supported in the Threat Prevention Policy.
- Network object groups
- Updatable objects (from R80.40)
- IP address ranges
- Roles
- Zones
- Data Center

For more details on the various types of objects, see the *R81.20 Security Management Administration Guide*.

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.

- The "`fw ctl set int`" command - Changes current **Protected Scope** settings for SPAN and TAP, does not survive reboot
- The `$FWDIR/module/fwkern.conf` file - 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/boot/modules/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 or lower, 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

Step	Instructions
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

Step	Instructions
1	Put your mouse cursor 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 (see *"Profiles Pane" on page 53*).
- For **rule exceptions** and **exception groups**, the action can be set to **Prevent** or **Detect**.

To select a profile for a rule

Step	Instructions
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

Tracking options and their description

Track Option	Description
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 (see *"Packet Capture" on page 275*).
Forensics	Adds fields to the Threat Prevention logs. The extra information gives you a deeper understanding of an attack (see *"Advanced Forensics Details" on page 276*).

Install On

1. Select the Security Gateways, on which to install the rule. The default is *All* (all Security Gateways that have a Threat Prevention blade enabled).
2. Put your mouse in the column and a plus sign shows.
3. Click the plus sign to open the list of available Security Gateways and select the applicable Security Gateway.

If you right-click a column in the table, you can add more columns to the table from the list that shows.

Concurrent Install Policy

Starting from R81, one administrator or more can run *different* policy installation tasks on multiple gateways at the same time. In earlier versions, you can only run the *same* policy installation task on multiple gateways at the same time.

Concurrent Install Policy only supports the Access Control and Threat Prevention policies. It does not support the Desktop and QoS policies.

The maximum number of policy installation tasks (of different policies) that can run at the same time is 5. If more than 5 policy installation requests are sent, any request beyond the first 5 gets in a queue.

The running and the queued tasks appear in the **Recent Tasks** window at the bottom left of your screen.

Note - In the first installation, you cannot install both the Access Control and Threat Prevention policies on the same gateway at the same time. You must install one and then the other.

Threat Prevention Profiles

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 following

- 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.

Profile

A profile is a set of configurations based on these:

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

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

Profile	Description
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.
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 or lower
- Very 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
- Critical

Activation Settings

Setting	Description
Ask	The Software Blade blocks the file or traffic until the user makes sure that the Security 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 from passing through the Security Gateway. It also logs the traffic, or tracks it, according to configured settings in the Rule Base.
Detect	The Software Blade allows identified file or traffic to pass through the Security Gateway. It also logs the traffic, or tracks it, according to configured settings in the Rule Base.
Inactive	The Software Blade 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 Security Gateway, Threat Emulation, Anti-Bot, and Anti-Virus can analyze the applicable HTTPS traffic.

To create a new Threat Prevention profile

Step	Instructions
1	In SmartConsole, select **Security Policies > Threat Prevention**.
2	From the **Custom Policy Tools** section, click **Profiles**. The **Profiles** page opens.
3	Right-click a profile and select **New**.

Step	Instructions
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

Step	Instructions
1	In SmartConsole, select **Security Policies > Threat Prevention**.
2	From the **Custom Policy 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 SmartConsole session.

Editing Profiles

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

To edit a profile

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

Deleting Threat Prevention Profiles

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

To delete a profile

Step	Instructions
1	In SmartConsole, select **Security Policies > Threat Prevention**.
2	From the **Custom Policy 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	In SmartConsole, install the policy.

To show the objects that use a profile

Step	Instructions
1	From the **Profiles** page, select the profile. The **Summary** page opens.
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**.

Viewing Changes to a Threat Prevention Profile

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

To view the Audit log for a Threat Prevention profile

Step	Instructions
1	In **SmartConsole**, click **Logs & Monitor**.
2	Click the **Audit** tab, or press **CTRL + T**, and then click **Open Audit Logs View**.
3	In **Enter search query**, enter the name of the profile.

Step	Instructions
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.

Assigning Profiles to Gateways

When you enable the IPS Software Blade on a pre-R80 gateway, a default IPS rule is automatically created in the IPS policy layer of the Security Policy. The Action of this rule is set according to the IPS setting of the assigned Threat Prevention Profile. You can change the profile from the Action column.

Note - Only the IPS settings from the Threat Prevention Profile apply to the IPS Policy.

To assign a profile to a gateway

Step	Instructions
1	In SmartConsole, select **Security Policies > Threat Prevention > Policy > IPS**.
2	Click the **Action** cell, and select the Threat Prevention profile.
3	Install the Access Control policy.

Configuring the Threat Prevention Profile and Rules

Create and manage the policy for the Threat Prevention:

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

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

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

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

Configuring Mail Settings

General

Options

- **Emulate emails for malicious content (requires Threat Emulation)** - When this option and the Threat Emulation blade are enabled, the Threat Emulation blade scans SMTP traffic.
- **Scan emails for viruses (requires Anti-Virus)** - When this option and the Anti-Virus blade are enabled, the Anti-Virus blade scans SMTP traffic.
- **Extract potentially malicious attachments (requires Threat Extraction)** - When this option and the Threat Extraction blade are enabled, the Threat Extraction blade scans SMTP traffic.

Malicious Email Policy on MTA Gateways

In this section you can decide whether to block or allow an email which was found malicious.

If you allow the email, you can select any or all of these options

- **Remove attachments and links** - This option is selected by default. You can replace a link or an attachment found malicious with a neutralized version of the links and attachments. The neutralized email version is sent to the recipient with a customizable template.

Click "Configure" to edit the template

Malicious Attachments - Replaced by a neutralized *txt* file. You can customize the message which the user receives. To add more file-related information to your message, click **Insert Field**(for example: file name or MD5 hash).

Failed to Scan Attachments - If the scanning of the attachment fails and fail mode is set to fail-close, the attachment is replaced with a *txt* attachment. If fail mode is set to fail-open, the original attachment is allowed. To add more file-related information to your message, click **Insert Field** (for example: file name or MD5 hash).

Malicious Links - Replaced by a neutralized link. To add more link-related information to your message, for example, neutralized URL.

- **Add an X-Header to the email** - Tag the email found malicious with an X-Header. The X-Header format is: "`X-Check Point-verdict: <`*`verdict`*` >; confidence: <`*`confidence`*`>`".

  Example

  "`X-Check Point-verdict: malicious; confidence: high`". With this option, you can configure the MTA Next Hop to quarantine all emails with a specific X-Header.

- **Add a prefix to the email subject** - Adds a prefix to the subject of an email found malicious.

  Example

  You can add a warning message that the email is malicious. Click **Configure** to edit the prefix.

- **Add customized text to the email body** - This option adds a section at the beginning of the email body, based on a customizable template, with an optional placeholder for the verdicts of the links and attachments found malicious or failed to be scanned. The links are given in their neutralized versions, and attachments are only given by file names. Click **Configure** to edit the template.

Send a copy to the following list - This option is available both if you allow or block the malicious email. With this option, the original email (with the malicious attachments and links) is attached to a new email, which contains: the verdict list with the neutralized links and attachment file names, and the SMTP envelope information. You can configure the email content on the gateway. You can use this option for research purposes.

Example

The *Check Point Incident Response Team* needs to inquire the emails received in the organization for improved security and protection.

Use Case

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

To configure external quarantine for malicious emails

Step	Instructions
1	Enable MTA on your gateway (see *"Configuring the Security Gateway as a Mail Transfer Agent" on page 170*).
2	Clone the Profile you wish to configure and rename it.
3	In the new profile, go to **Mail** > **General** > **Malicious Email Policy on MTA Gateways** and select **Allow the email**.
4	Clear **Remove attachments and links**.
5	Select **Add an X-Header** to the email. **Note** - When you add an X-Header to the email, the rest of the email is kept in the email's original form. The other options: **Remove attachments and links**, **Add a prefix to the email subject** and **Add customized text to the email body**, change the email, and therefore must be cleared.
6	Click **OK**.
7	Install Policy.

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

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

Exceptions

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

To exclude emails from Threat Emulation

Step	Instructions
1	In **Emulation Exceptions**, click **Configure**.
2	In the **Recipients** section, click the **+** button to enter one or more emails. Emails and attachments that are sent to these recipients will not be sent for emulation.
3	In the **Senders** section, click the **+** button to enter one or more emails. Emails and attachments that are received from these senders will not be sent for emulation. **Note** - You can use a wildcard character to exclude more than one email address from a domain.
4	Click **OK**.

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

To exclude emails from Threat Extraction

Step	Instructions
1	In **Extraction Exclusion/Inclusion**: 1. Select **Scan all emails** (selected by default) and click **Exceptions**. 2. Click the **+** button to exclude specific recipients, users, groups or senders. 3. Select **Scan mail only for specific users or groups** and click **Configure**. 4. Click the Add button to exclude specific User Groups, Recipients, or Senders.
2	Click **OK**.

Examples

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

Important - In the main SmartConsole menu > **Global Properties** > **User Directory**, make sure that you selected **Use User Directory for Security Gateways**.

Signed Email Attachments

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

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

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

MIME Nesting

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

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

Configuring IPS Profile Settings

To configure IPS settings for a Threat Prevention profile

Important - To ensure IPS protections are enforced on HTTPS traffic, you must enable HTTPS Inspection in the Security Gateway/Security Cluster properties in SmartConsole, with inspection enabled for the respective traffic. See *HTTPS Inspection*.

Step	Instructions
1	In SmartConsole, select **Security Policies > Threat Prevention**.
2	From the **Custom Policy 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 (see *"Additional Activation Fields" on the next page*).
6	From the navigation tree, click **IPS** > **Pre-R80 Settings**.
7	Configure the settings for newly downloaded IPS protections (see *"Updates" on the next page*).
8	**If you import IPS profiles from a pre-R80 deployment** 1. From the navigation tree, click **IPS** > **Pre-R80 Settings**. 2. Activate the applicable **Client** and **Server** protections (see *"Pre-R80 Settings" on page 66*). 3. Configure the IPS protection categories to exclude from this profile (see *"Pre-R80 Settings" on page 66*). **Note** - These categories are different from the protections in the **Additional Activation** page.
9	Click **OK**.
10	Click **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 Security Gateways enforce activated protections, and do not enforce deactivated protections, regardless of the general profile protection settings.

Activate IPS protections according to the following additional properties - When selected, the categories configured on this page modify the profile's IPS protections.

- **Protections to activate** - The IPS protection categories in this section are enabled on the Security Gateways that use this Threat Prevention profile.
- **Protections to deactivate** - The IPS protection categories in this section are NOT enabled on the Security Gateways that use this Threat Prevention profile.

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

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

Updates

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

In the Threat Prevention profile, you can configure an updates policy for IPS protections that were newly updated. You can do this with the **IPS** > **Updates** page in the **Profiles** navigation tree.

Select one of these settings for Newly Updated Protections

- **Active - According to profile settings** -Selected by default. Protections are activated according to the settings in the **General** page of the Profile. This is the Check Point recommended configuration.

  Set activation as staging mode - Newly updated protections remain in staging mode until you change their configuration. The default action for protections in staging mode is Detect. You can change the action manually in the IPS **Protections** page (see *"Activating Protections" on page 71*).

  Click **Configure** to exclude specific protections from staging mode.

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

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

Pre-R80 Settings

The pre-R80 settings are relevant for the pre-R80 Security 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 Security Gatewayperformance by deactivation of protections. If you select Client Protections and Server Protections, all protections are activated, except for those that are:

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

Excluded Protections Categories

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

Configuring IPS Protections for Custom Threat Prevention

IPS Protections

Protection Browser

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

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

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 Security Gateway. 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 Security Gateways on which they are activated.

Important - The **Performance Impact** of protections is rated based on how they affect Security Gateways that run R80.30 version and above. The Performance Impact on other Security 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 Security 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 Security 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 (see *"Updating IPS Protections" on the next page*). 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

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

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

To filter the protections

Step	Instructions
1	From the **IPS Protections** window, click the **Filter** icon. The **Filters** pane opens and shows IPS protections categories.

Step	Instructions
2	To add more categories 1. Click the **Add filter** button. A window opens and shows the IPS protections categories. 2. 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.

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.

Notes:

- To enforce the IPS updates, you must install the Threat Prevention Policy.
- When you assign or reassign a global configuration while an IPS update runs on a Domain, you may get an "Internal error occurred" error. To resolve this issue:
  1. Connect with SmartConsole to the Domain Management Server.
  2. Run the IPS update.
  3. Close the SmartConsole which is connected to the Domain Management Server.
  4. In the global SmartConsole, assign or reassign the global configuration.

To update IPS Protections

In SmartConsole, click the **Security Policies** view > **Threat Prevention** > in the **Custom Policy Tools** section, click **Updates**.

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

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

Scheduling IPS Updates

You can configure a schedule for downloading the latest IPS protections and protection descriptions (see *"Threat Prevention Scheduled Updates - Custom Threat Prevention" on page 279*).

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

Step	Instructions
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**. Click **OK**.
3	Install the Threat Prevention Policy.

Reviewing New Protections

To see newly downloaded protections

In SmartConsole, go to **Security Policies > Threat Prevention** > **Custom Policy Tools**

Step	Instructions
1	Go to **IPS Protections**.

Step	Instructions
2	The **Update Date** column sorts the protections by date. By default, the latest protections are shown first. If not, click the column so that the latest protections are presented first.

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:

In SmartConsole, click the **Security Policies** view > **Threat Prevention** > in the **Custom Policy Tools** section, click **IPS Protections**.

Step	Instructions
1	Right-click 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**.
2	Click **OK**.
3	Close the Threat Prevention profile window.
4	Install the Threat Prevention policy.

Editing Protections for a Specific Profile

To edit a protection for a specific profile

Step	Instructions
1	In the **Protections Browser**, find the protection to activate.
2	Click **Edit**.
3	Right-click the relevant profile and click **Edit**. You can activate the protection for one profile and deactivate it for another profile. It will be active for some gateways and inactive for others. If the protection is inactive according to the policy, you can override the policy preference or change the policy criteria.

Step	Instructions
4	To override the settings for the specific protection, click **Override with**.
5	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.
6	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.
7	Configure **Additional Settings** if relevant. For example, for the protection **Web Login Form Password Brute Force Attempt**, click **Customize** > **Configure**, to configure these settings: - Number of login attempts from the same IP. - Time (seconds) in which login attempts occur. - Time (seconds) in which the source IP will be blocked.
8	Install the Threat Prevention 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

Step	Instructions
1	In SmartConsole, select **Security Policies > Threat Prevention**.
2	From the **Custom Policy Tools** section, click **IPS Protections**. The **IPS Protections** page opens.
3	Click the protections in the applicable profile column. **Note** - Press CTRL to select more than one protection.
4	Right-click the highlighted cell or cells and select **Restore to profile settings**.

Step	Instructions
5	Select **All Profiles** or **Displayed Profiles**. A warning message opens.
6	Click **Yes**.
7	Install the Threat Prevention Policy.

To remove IPS protection overrides from all protections

Step	Instructions
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 the Threat Prevention Policy.

Editing Core IPS Protections

To edit core protections

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

IPS Protections Follow Up

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

To view protections marked for follow up

In SmartConsole, go to **Security Policies** > **Threat Prevention** > **Custom Policy Tools**

Step	Instructions
1	Go to **IPS Protections** > **Filters**.
2	Select **Follow Up**.

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

Manually Marking Protections for Follow Up

You can mark individual protections for Follow Up, which lets you quickly review the identified protections in the **IPS Protections** page. To make the Follow Up feature efficient, make sure to keep the list of marked protections as short as possible.

Mark newly downloaded protections and any protection that you want to monitor, but remember to remove protections from this list when you are more confident that you configured them in the best way for your environment. The longer the Follow Up list is, the more difficult it is to use it as a workable task list

To manually mark protections for follow up:

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

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

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

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

Automatically Marking New Protections for Follow Up

Check Point provides new and updated protections as they become available (see *"Updating IPS Protections" on page 69*). To give you complete control over the process of integrating new IPS protections, you can have them automatically marked for Follow Up. This gives you time to evaluate the impact the protections have on your environment.

To have new protections marked automatically

In SmartConsole, go to **Security Policies** > **Threat Prevention** > **Custom Policy Tools**

Step	Instructions
1	In SmartConsole, select **Security Policies**.
2	Choose **Threat Prevention > Custom Policy Tools > Updates > IPS**.
3	Select **Follow Protections**.

Configuring Anti-Bot Settings

Here you can configure the Anti-Bot **UserCheck Settings**:

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

Blocking Bots

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

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

To block bots in your organization

Step	Instructions
1	In SmartConsole, click **Gateways & Servers**.
2	Enable the **Anti-Bot** Software Blade on the Gateways that protect your organization. **For each Gateway** 1. Double-click the Gateway object. 2. In the **Gateway Properties** page, select the **Anti-Bot** Software Blade. The First Time **Activation** window opens. 3. Select **According to the Anti-Bot and Anti-Virus policy**. 4. Click **OK**.

Step	Instructions
3	Click **Security Policies > Threat Prevention > Custom Policy**. 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** 1. Click **Add Rule**. A new rule is added to the Threat Prevention Custom Policy. The Software Blade applies the first rule that matches the traffic. 2. 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 (see *"Profiles Pane" on page 53*). 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, on which to install the rule.

Step	Instructions
4	**Install the Threat Prevention Policy.** The IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction Software Blades have a dedicated Threat Prevention policy. You can install this policy separately from the policy installation of the Access Control Software Blades. Install only the Threat Prevention policy to minimize the performance impact on the Security Gateways. **To install the Threat Prevention policy** 1. From the Global toolbar, click **Install Policy**. The Install Policy window opens showing the installation targets (Security Gateways). 2. Select **Threat Prevention**. 3. Select **Install Mode**: ■ Install on each selected gateway independently - Install the policy on the selected Security Gateways without reference to the other targets. A failure to install on one Security Gateway does not affect policy installation on other gateways. If the gateway is a member of a cluster, install the policy on all the members. The Security Management Server makes sure that it can install the policy on all the members before it installs the policy on one of them. If the policy cannot be installed on one of the members, policy installation fails for all of them. ■ Install on all selected gateways, if it fails do not install on gateways of the same version - Install the policy on all installation targets. If the policy fails to install on one of the Security Gateways, the policy is not installed on other targets of the same version. 4. Click **OK**.

Note - From R81.20 Jumbo Hotfix Accumulator **Take 70**, there is an enhanced protection against zero-day attacks. It detects and blocks advanced malware variants by automatically analyzing and identifying communication patterns. The feature is disabled by default. To enable it, refer to *"Malware Prevention Using IP and Port Indicators" on page 81*.

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: Go to the **General Policy** pane > **Activation Mode** section, and set all **Confidence** levels to **Detect**.	`Log`	`*Policy Targets`

To monitor all bot activity

Step	Instructions
1	In SmartConsole, select **Security Policies > Threat Prevention**.
2	**Create a new profile** a. From the **Custom Policy 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** 1. Go to Security Policies > **Threat Prevention > Custom Policy**. 2. Add a rule to the Rule Base. The first rule that matches is applied. 3. Make a rule that includes these components. ■ **Name** - Give the rule a name such as **Monitor 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 (see *"Profiles Pane" on page 53*). 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, on which to install the rule.

Step	Instructions
4	**Install the Threat Prevention Policy.** The IPS, Anti-Bot, Anti-Virus, Threat Emulation and Threat Extraction Software Blades have a dedicated Threat Prevention policy. You can install this policy separately from the policy installation of the Access Control Software Blades. Install only the Threat Prevention policy to minimize the performance impact on the Security Gateways. **To install the Threat Prevention policy** 1. From the Global toolbar, click **Install Policy**. The Install Policy window opens showing the installation targets (Security Gateways). 2. Select **Threat Prevention**. 3. Select **Install Mode**: ■ Install on each selected gateway independently - Install the policy on the selected Security Gateways without reference to the other targets. A failure to install on one Security Gateway does not affect policy installation on other gateways. If the gateway is a member of a cluster, install the policy on all the members. The Security Management Server makes sure that it can install the policy on all the members before it installs the policy on one of them. If the policy cannot be installed on one of the members, policy installation fails for all of them. ■ Install on all selected gateways, if it fails do not install on gateways of the same version - Install the policy on all installation targets. If the policy fails to install on one of the Security Gateways, the policy is not installed on other targets of the same version. 4. Click **OK**.

Malware Prevention Using IP and Port Indicators

IP Reputation Protection inspects traffic and blocks suspicious connections based on IP addresses. This protection enforces security policies through advanced IP and port-based analysis, which identifies and blocks malicious traffic across multiple protocols. The system loads the latest threat intelligence from its cloud service to maintain an up-to-date reputation feed.

This protection enables organizations to defend against well-known botnets, including Emotet, Dridex, Qbot, and others.

Important - This feature is available from R81.20 Jumbo Hotfix Accumulator **Take 70**.

Known limitations

- Only IPv4 is supported.
- The feature is disabled when the Security Gateway operates in offline mode.

How to Enable IP Reputation Protection

To enable IP Reputation Protection, modify the `ip_port_feed.conf` file on the Security Gateway. The following steps to configure the file and apply the changes to activate the protection.

1. To enable the protection change the `ip_port_feed.conf` file on the Security Gateway. Open the file with `vi` or another text editor:

   ```
   vi $FWDIR/conf/ip_port_feed.conf
   ```

2. Locate the line with the value `enabled`.
3. Set the value to `true`.
4. Save the file.
5. Apply the changes:
   - Wait 5 minutes for the scheduled task to apply the changes automatically.
   - Alternatively, run the following command to apply the changes immediately:

     ```
     ipp_feeder -f
     ```

Note - To disable the protection, set the `enabled` value to `false` in the configuration file.

Feed Verification

This process ensures that the feed configuration is correct and that any associated errors, such as `MALWARE_IP_REP` issues, are identified and resolved. Follow these steps to verify the feed, troubleshoot errors, and ensure proper functionality.

1. Run `tp_collector_cli` and look for **MALWARE_IP_REP** errors.
2. To gather additional error details, run `ipp_feeder -d -f` on the Security Gateway to fetch feeds in debug mode. Verify error details in `$FWDIR/log/ipp_feeder.elg`.
3. Ensure the `$FWDIR/conf/ip_port_feed.conf` configuration file exists and remains uncorrupted. If the file is corrupt, replace its content with the following:

```
{
  "enabled": true,
  "url": "https://ipport.iaas.checkpoint.com/ip-port-feed.csv",
  "feed_size_limit": 10000,
  "policy_enabled": false,
  "ssl_validation_enabled": false
}
```

4. Install the policy.
5. Confirm observables were fetched to the kernel table by running the following command:

```
fw tab –t mal_ip_port_reputation
```

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 check DMZ interface configuration

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

Step	Instructions
1	In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway. The Security Gateway properties 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 Security Gateway editor. Perform this procedure for each interface that goes to the DMZ.

In a Threat Prevention profile, you can configure these settings in the Anti-Virus page

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

- **Inspect incoming files from**:

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

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

- **Inspect incoming and outgoing files** - Sends all incoming and outgoing files for inspection.

- **Protocol**:
  - **Web (HTTP/HTTPS))**
  - **FTP**
  - **SMB**
  - **Mail (SMTP)** - Click **Mail** to configure the SMTP traffic inspection. This opens the **Mail** page of the Profile settings (see *"Configuring Mail Settings" on page 59*).

- **File Types**:
  - **Process file types known to contain malware** - Select this option to scan the files configured by default. To see the default list of files, go to **Process specific file type families**, and click **Configure**.
  - **Process all file types** -Select **Enable deep inspection scanning (impacts performance)**, if needed.
  - **Process specific file types families**

    To configure the specific file type families:

Step	Instructions
1	Click **Configure**.
2	In the **File Types Configuration** window, for each file type, select the Anti-Virus action for the file type.
3	Click **OK** to close the **File Types Configuration** window.

- **Archives**:

You can select **Enable Archive scanning (impacts performance)**. See *"Enabling Archive Scanning" below*.

Enabling Archive Scanning

You can configure the Anti-Virus settings to enable archive scanning. The Anti-Virus engine unpacks archives and applies proactive heuristics. The use of this feature impacts network performance.

Select **Enable Archive scanning (impacts performance)** and click **Configure:**

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

Blocking Viruses

To block viruses and malware in your organization

Step	Instructions
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**. Click **OK**.
4	Click **OK** to close the Security Gateway Properties window.
5	Publish the SmartConsole session.
6	Click **Security Policies > Threat Prevention > Custom Policy**.
7	Click **Add Rule**. A new rule is added to the Threat Prevention policy. The Software Blade applies the first rule that matches the traffic.

Step	Instructions
8	Configure a rule that includes these columns: ▪ **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 (see *"Profiles Pane" on page 53*). 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 Security Gateways, on which to install the rule.
9	Install 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 for the Access Control Software Blades. **Best Practice** - Install only the Threat Prevention policy to minimize the performance impact on the Security Gateways.

Additionally Supported Protocols for Anti-Virus

In addition to HTTP, FTP, SMB and SMTP protocols, which you can select in the SmartConsole GUI, the Anti-Virus Software Blade also supports the IMAP and POP3 protocols.

Procedure to activate Anti-Virus inspection for IMAP and POP3 protocols

Step	Instructions
1	Connect to the command line on your Security Gateway.
2	Log in to the Expert mode.
3	Back up the `$FWDIR/conf/malware_config` file: `cp -v $FWDIR/conf/malware_config{,_BKP}`
4	Edit the `$FWDIR/conf/malware_config` file: `vi $FWDIR/conf/malware_config`
5	Change the value of the applicable parameter: ■ To activate IMAP protocol support: In the "`[imap]`" section, change the value of the parameter "`imap_av_policy_on`" from "`0`" to "`1`". ■ To activate POP3 protocol support: In the "`[temp_for_av_profile]`" section, change the value of the parameter "`pop3_enabled`" from "`0`" to "`1`".
6	Save the changes in the file and exit the editor.
7	In SmartConsole, install Threat Prevention Policy.

The Threat Emulation Solution

Getting Started with Threat Emulation

1. **If you use a Threat Emulation appliance, prepare the network and the Threat Emulation appliance, for local or remote emulation in the internal network**

Step	Instructions
1	In SmartConsole, create the Security Gateway object for the Threat Emulation appliance.
2	If you run emulation on HTTPS traffic, configure the settings for HTTPS Inspection (see *"HTTPS Inspection " on page 393*).
3	Make sure that the traffic is sent to the appliance according to the deployment: ■ Local Emulation - The Threat 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 Threat Emulation appliance.

2. **Enable the Threat Emulation Software Blade on the Security Gateway**

Step	Instructions
1	In the **Gateways & Servers** view, double-click the Security Gateway / Cluster object. The **Gateway Properties** window opens.
2	In the **General Properties** > **Network Security** tab, select **SandBlast Threat Emulation**. The **Threat Emulation First Time Configuration Wizard** opens and shows the **Emulation Location** page.
3	Select the **Emulation Location:** ■ **ThreatCloud Emulation Service** ■ **Locally on this Threat Emulation appliance** ■ **Other Threat Emulation appliances -** Click the **+** sign to add emulation appliances (you can select more than one appliance for the emulation)**.**

Step	Instructions
4	Click **Next**. The **Activate Threat Extraction** window opens, with this checkbox selected: **Clean potentially malicious parts from files (Threat Extraction)** ■ To activate Threat Extraction, keep this checkbox selected: ■ If you do not want to activate Threat Extraction, clear this checkbox.
5	Click **Next**. The **Summary** page opens. ⓘ **Note** - If you selected the **Emulation Location** as **Locally on this Threat Emulation appliance** or **Other Threat Emulation appliances**, and you want to share Threat Emulation information with ThreatCloud, select **Share attack information with ThreatCloud**.
6	Click **Finish** to enable Threat Emulation (and if selected, Threat Extraction), and then close the First Time Configuration Wizard.
7	Click **OK**. The **Gateway Properties** window closes.

ⓘ **Note** - When a trial license is installed on the Security Gateway, a green "V" incorrectly appears next to the Threat Emulation Software Blade (in SmartConsole, go to the **Gateways & Servers** view > right-click the Security Gateway / Cluster object > click **Monitor**) > the **Device and License Information** window opens > **Device Status** > **Threat Emulation**).
To see the correct license status, go to the **License Status** tab in the **Device and License Information** window.

Using Cloud Emulation

Files are sent to the Check Point ThreatCloud over a secure TLS 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**.

3. Select deployment. See *"Selecting the Threat Emulation Deployment" on page 93*.

4. Configure Threat Emulation settings on the Threat Prevention profile. See *"Configuring Threat Emulation Settings on the Security Profile" on page 96*.
5. Optional: Configure Threat Emulation settings on the Security Gateway. See *"Configuring Threat Emulation on the Security Gateway - Custom Threat Prevention" on page 103*
6. Configure advanced Threat Emulation settings. See *"Configuring Advanced Threat Emulation Settings - Custom Threat Prevention" on page 108*.
7. Install the Threat Prevention policy on the Security Gateway. If you use a Threat Emulation appliance, install the Threat Prevention policy on the Threat Emulation appliance as well.

For information about Private ThreatCloud, see the following Secure Knowledge articles:

- sk149692: Private ThreatCloud
- sk113332: Private ThreatCloud - Engine Updates
- sk161534: How to configure Private ThreatCloud (PTC) on Scalable Platform Appliances

ThreatCloud Emulation

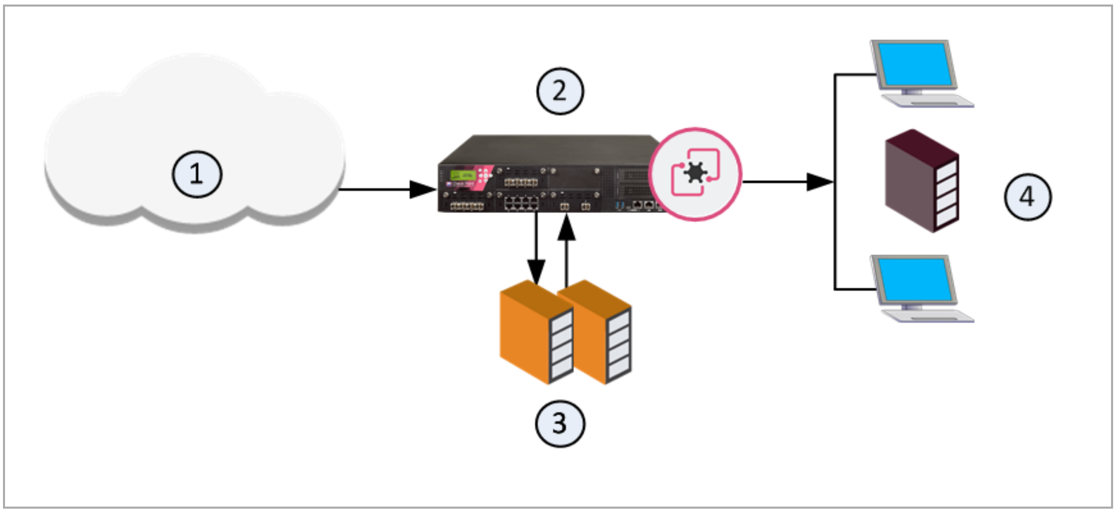
You can securely send files to the Check Point ThreatCloud for emulation. The ThreatCloud is always up-to-date with the latest Threat Emulation releases.

The new Threat Emulation engine uses Internet-connected sandboxes to prevent multi-stage attacks at the earliest stage. The full infection chain is analyzed and is presented in the MITRE ATT&CK Matrix visualization in the Threat Emulation report. The Internet-connected sandbox capability is supported on Threat Emulation AWS cloud platform and all Threat Emulation vectors: Web download, Mail Transfer Agent, CloudGuard SaaS, SandBlast Agent and APIs.

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 a TLS 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	Internet and external networks
2	Perimeter Security Gateway
3	Check Point ThreatCloud servers
4	Computers and servers in the 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 Appliance in the Internal network** - You can use a Threat Emulation appliance to run emulation on the files, whether locally or on a remote appliance.

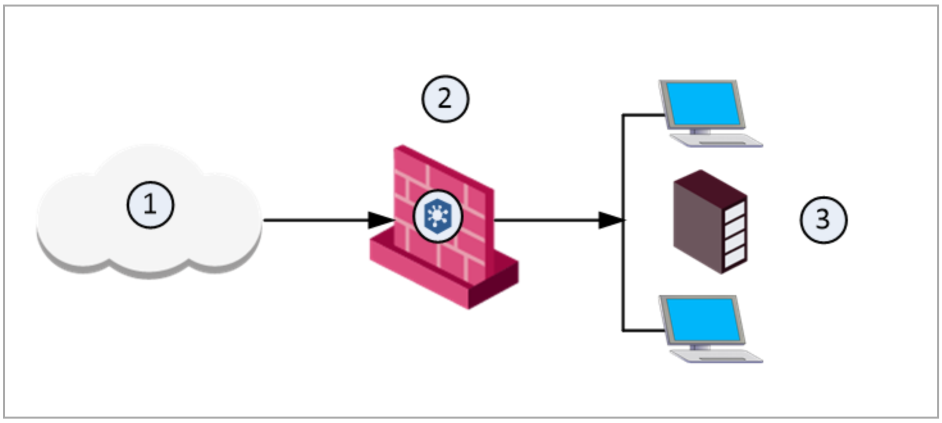
Local or Remote Emulation

You can install a Threat Emulation appliance in the internal network.

Sample workflow for local Threat Emulation

1. The Security Gateway receives the traffic, and aggregates the files.
2. The Security Gateway compares the cryptographic hash of the file with the database.

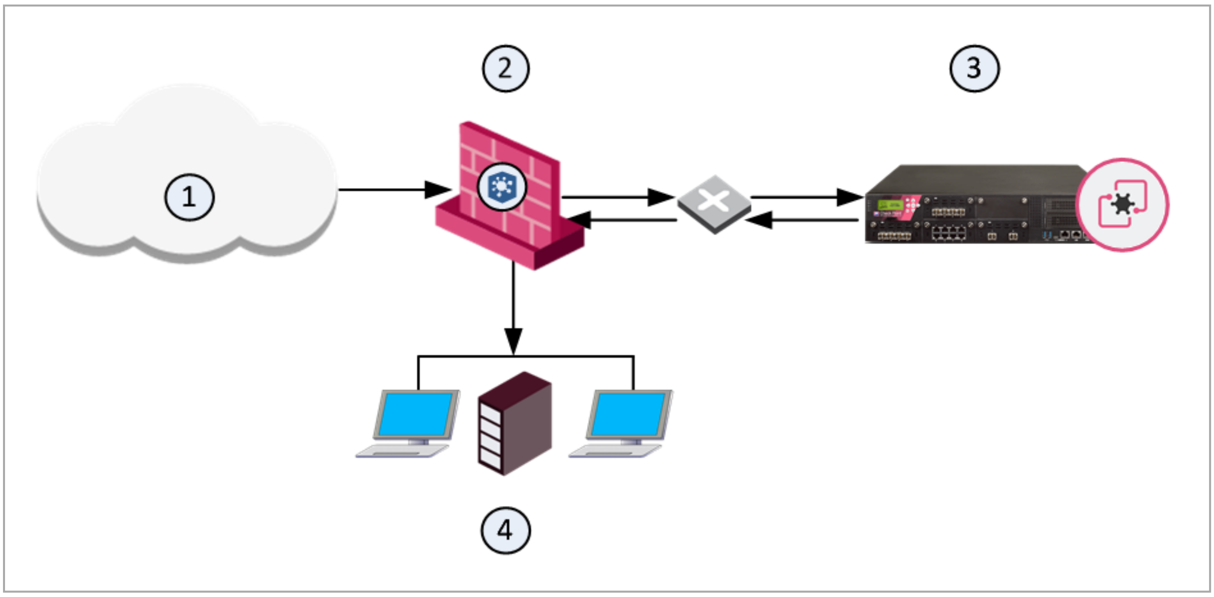
- The file is already in the database, no emulation is needed.
- If the file is not in the database, the virtual computers in the Security Gateway run full emulation on the file.



Item	Description
1	Internet and external networks
2	Security Gateway/Threat Emulation appliance
3	Computers and servers in the internal network

Sample workflow for Threat Emulation on a remote appliance

1. The Security Gateway aggregates the files, and the files are sent to the Threat Emulation appliance.
2. The Threat Emulation appliance compares the cryptographic hash of the file with the database. Files have unique cryptographic hashes. These file hashes are stored in a database after emulation is complete
   - If the file is already in the database, no emulation is needed.
   - If the file is not in the database, the virtual computers in the Threat Emulation appliance run full emulation on the file.



Item	Description
1	Internet and external networks
2	Perimeter Security Gateway
3	Threat Emulation Appliance
4	Computers and servers in the internal network

Selecting the Threat Emulation Deployment

What are my options to send traffic for emulation?

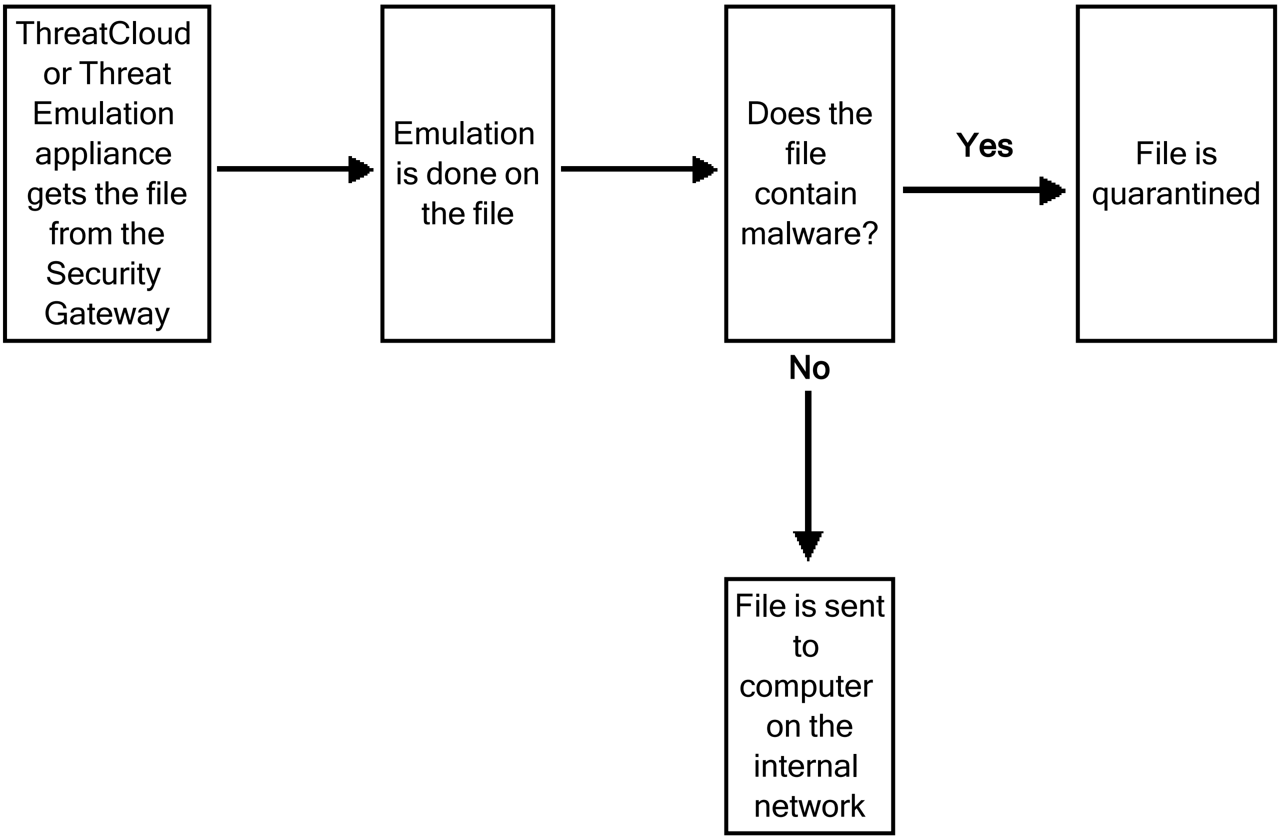
Option	Description
Inline	Traffic is sent for emulation before it is allowed to enter the internal network. You can use the Threat Prevention policy to block malware.
Monitor (SPAN/TAP)	You can use a mirror or TAP port to duplicate network traffic. Files are sent to the computer in the internal network. If Threat Emulation discovers that a file contains malware, the appropriate log action is done.
MTA (see *"Configuring the Security Gateway as a Mail Transfer Agent" on page 170*)	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.

To switch between the Inline and Monitor modes, see the *R81.20 Gaia Administration Guide*

Inline Deployments

The ThreatCloud or Threat Emulation appliance gets a file from the Security Gateway. After emulation is done on the file, if the file is safe, it is sent to the computer in the internal network. If the file contains malware, it is quarantined and logged. The computer in the internal network is not changed.

Sample Inline Emulation Workflow (Prevent Action)

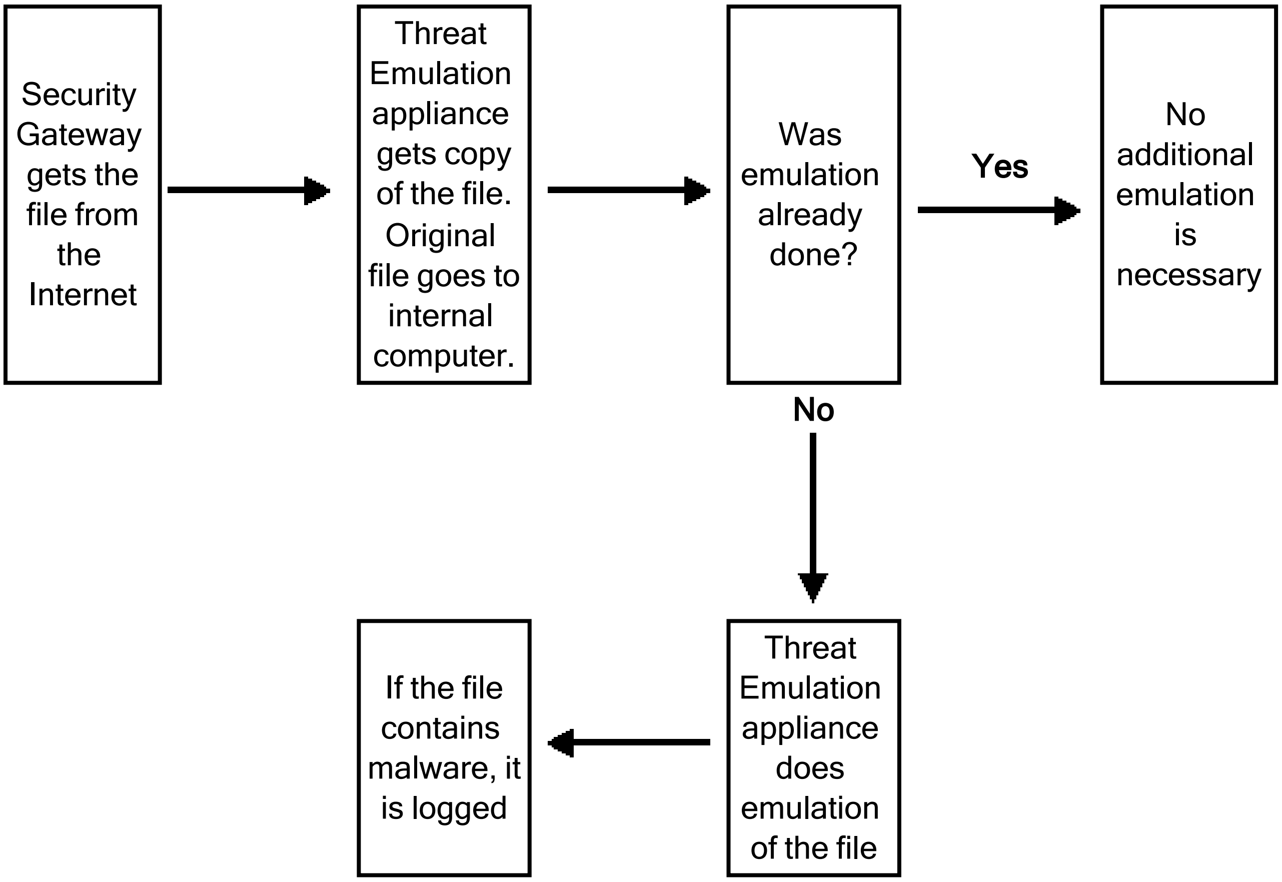

ThreatCloud or Threat Emulation appliance gets the file from the Security Gateway
Emulation is done on the file
Does the file contain malware?
Yes
File is quarantined
No
File is sent to computer on the internal network

Monitor (SPAN/TAP) Deployments

The Security Gateway gets a file from the Internet or an external network and lets it enter the internal network. The Threat Emulation appliance receives a copy of the file and the original file goes to the computer in the internal network. The Threat Emulation appliance compares the cryptographic the file with the database. If the file is already in the database, then no additional emulation is necessary. If the file is not in the database, the virtual computers in the Threat Emulation appliance do emulation of the file.

If the file is identified as malware, it is logged according to the Track action of the Threat Prevention rule. Monitor deployments support only the **Detect** action.

Sample Monitor Emulation Workflow


Security Gateway gets the file from the Internet
Threat Emulation appliance gets copy of the file. Original file goes to internal computer.
Was emulation already done?
Yes
No additional emulation is necessary
No
Threat Emulation appliance does emulation of the file
If the file contains malware, it is logged

Threat Emulation Deployments with a Mail Transfer Agent

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

For more information on how to work with the Mail Transfer Agent, see *"Configuring the Security Gateway as a Mail Transfer Agent" on page 170*.

Configuring Threat Emulation Settings on the Security Profile

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

To verify DMZ interface configuration

Step	Instructions
1	From the left navigation panel, click **Gateways & Servers**.
2	Double-click the Security Gateway object.
3	From the left navigation tree, click **Network Management**.
4	Double-click a DMZ interface.
5	In the **General** page of the **Interface** window, click **Modify**.
6	In the **Topology Settings** window, click **Override** and select **Interface leads to DMZ**.
7	Click **OK**.

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

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

To configure Threat Emulation settings for a Threat Prevention profile

Step	Instructions
1	In SmartConsole, select **Security Policies > Threat Prevention**.
2	From the **Custom Policy Tools** section, click **Profiles**. The **Profiles** page opens.
3	Right-click the profile, and click **Edit**.
4	From the navigation tree, go to **Threat Emulation** and configure these settings: a. *"Threat Emulation General Settings" on the next page* b. *"Threat Emulation Environment" on page 99* c. *"Threat Emulation Advanced Settings" on page 99*
5	Click **OK** and close the Threat Prevention profile window.
6	Install the Threat Prevention policy.

Important - To emulate a file, the Security Gateway must receive the full file. Threat Emulation does not work on a file if only a part of it was downloaded.

Threat Emulation General Settings

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

UserCheck Settings

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

Protected Scope

Select an interface type and traffic direction option

- **Inspect incoming files from the following interfaces**:

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

  - **External** - Inspect incoming files from external interfaces. Files from the DMZ and internal interfaces are not inspected.

    Example: A company's firewall is configured to inspect files received from external sources, such as emails or cloud services, while not interfering with internal file transfers.

  - **External and DMZ** - Inspect incoming files from external and DMZ interfaces. Files from internal interfaces are not inspected.

    Example: An organization's perimeter security system inspects files entering through both external connections and the Demilitarized Zone (DMZ), ensuring a thorough evaluation of potential threats.

  - **All** - Inspect all incoming files from all interface types.

    Example: A highly secure environment demands inspection of files from all possible interfaces, including both external and internal sources, to maintain a comprehensive defense against any potential malicious activity.

- **Inspect incoming and outgoing files** - Sends all incoming and outgoing files for inspection.

  Example: In a scenario where bidirectional traffic monitoring is crucial, a network security system is configured to inspect both incoming and outgoing files, ensuring end-to-end protection against potential threats.

Protocols

Protocols to be emulated

- **Web (HTTP/HTTPS)**
- **FTP**
- **SMB**
- **Mail (SMTP/POP3)** - Click **Mail** to configure the SMTP traffic inspection by the Threat Emulation Software Blade. This links you to the **Mail** page of the Profile settings (see *"Configuring Mail Settings" on page 59*).

File Types

Here you can configure the Threat Emulation **Action** and **Emulation Location** for each file type scanned by the Threat Emulation Software Blade.

Select one of these file types

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

  Note - You can find this list of supported file types also in **Manage & Settings** view > **Blades > Threat Prevention > Advanced Settings > Threat Emulation > File Type Support**.

- **Process specific file type families** - Click **Configure** to change the action or emulation location for the scanned file types.

  To change the emulation action for a file type, click the applicable action in the **Action** column and select one of these options:

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

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

  - **According to gateway** - The **Emulation Location** is according to the settings defined in the **Gateway Properties** window of each gateway.
  - **Locally** - Emulation for these file types is done on the gateway. This option is not supported for R80.40.
  - **ThreatCloud** - These file types are sent to the ThreatCloud for emulation.

> **Note** - If the emulation location selected in the profile is different than the emulation location configured on the Security Gateway, then the profile settings override.

Archives

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

Threat Emulation Environment

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

- The **Analysis Locations** section lets you select: where the emulation is done.
  - To use the Security Gateway settings for the location of the virtual environment, click **According to the gateway**.
  - To configure the profile to use a different location of the virtual environment, click **Specify** and select the applicable option.
- The **Environments** section lets you select the operating system images on which the emulation is run. If the images defined in the profile and the Security Gateway or Threat Emulation appliance are different, the profile settings are used.

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

Threat Emulation Advanced Settings

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

  Emulation Connection Handling Mode lets you configure Threat Emulation to allow or block a connection while it finishes the analysis of a file. The handling mode you select affects the form of the file that the user receives and the timing at which the user receives it. This section explains the difference between the Threat Emulation handling modes and the interaction between the Threat Emulation and Threat Extraction components with regards to the handling mode selected.

The first part of the section explains what happens when Threat Emulation works with Threat Extraction disabled and the second part explains how the Threat Emulation and the Threat Extraction components work together. You can also specify a different mode for SMTP and HTTP services. To configure the settings for the Threat Emulation handling mode, go to **Security Policies** > **Threat Prevention** > **Policy** > right-click a profile > **Threat Emulation** > **Advanced**.

Selecting an Emulation connection handling mode when Threat Extraction is disabled

If Threat Emulation reaches a verdict regarding a file within 3 seconds or less:

- If the file is benign, the gateway sends the original file to the user.
- If the file is malicious, the gateway blocks the page.

If Threat Emulation takes longer than 3 seconds to check the file:

- In **Rapid Delivery** mode - The gateway sends the original file to the user (even if it turns out eventually that the file is malicious).
- In **Maximum Prevention** mode - The user waits for Threat Emulation to complete. If the file is benign, the gateway sends the original file to the user. If the file is malicious, the gateway presents a Block page and the user does not get access to the file. Maximum Prevention mode gives you more security, but may cause time delays in downloading files.

In **Custom** mode- You can set a different handling mode for SMTP and HTTP. For example: you can set HTTP to Rapid Delivery and SMTP to Maximum Prevention.

Selecting an Emulation connection handling mode when Threat Extraction is enabled

With Threat Extraction, the gateway removes potentially malicious parts from downloaded/attached files and delivers them instantly to the user. Threat Emulation continues to run in the background, and examine the original files. Threat Extraction supports certain file types, primarily Microsoft Office files and PDFs, but not all file types, for example, executables.

- If Threat Emulation rules that the file is benign, the user gets access to the original file, using the link in the file itself or the email body banner, , without help desk overhead.
- If Threat Emulation rules that the file is malicious, the original file is blocked and the user only gets access to the cleaned file.

This way administrators can ensure maximum security, while not harming end-user productivity.

This behavior would be the same for both the Rapid Delivery and Maximum Prevention modes. Nevertheless, if you select Maximum Prevention, In CLI, you can configure an even more restrictive mode, such that:

- The user always waits for Threat Emulation to complete, even if the file is supported by Threat Extraction.
- The user receives the file only if the file is deemed benign, and if the file is supported by Threat Extraction, it will also be cleaned. To configure this mode, see sk146593.

When Threat Extraction is enabled, but the file is not supported by Threat Extraction, the user is not able to receive a cleaned version of the file. The behavior therefore, will be the same as when Threat Extraction is disabled. In Rapid Delivery mode, the user gets the original file and in Maximum Prevention mode, the user waits for the Threat Emulation verdict.

Best Practice:
If Threat Extraction is enabled, use Maximum Prevention as your handling mode (without the extra preventive CLI configuration). Because most files that users work with on a daily basis are documents, that are supported by Threat Extraction, the time penalty for waiting for the non-supported files is manageable. Users will be able to receive most files in a timely manner. If Threat Extraction is disabled, select the handling mode based on balancing your security needs versus time constraints.

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

- **Static Analysis** optimizes file analysis by doing an initial analysis on files. If the analysis finds that the file is simple and cannot contain malicious code, the file is sent to the destination without additional emulation. Static analysis significantly reduces the number of files that are sent for emulation. If you disable it, you increase the percentage of files that are sent for full emulation. The Security Gateways do static analysis by default, and you have the option to disable it.
- **Logging** lets you configure the system to generate logs for each file after emulation is complete. If **Log every file scanned** is enabled, then every file that is selected in **Threat Emulation** > **General** > **File Types** is logged, even if no operation is performed on it. If **Log every file scanned** is disabled, malicious files are still logged.

Use Case

Configuring Threat Emulation location

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

To configure the Threat Emulation analysis location

Step	Instructions
1	In the **Gateways & Servers** view, double-click a Security Gateway, go to **Threat Emulation** > **Analysis Location**.
2	Select: ▪ **Locally** (not supported for R80.40 OR ▪ **Remote Emulation Appliances**. Click the **+** sign to select the applicable Security Gateways from the drop-down list.
3	Click **OK**.

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

Configuring Threat Emulation on the Security Gateway - Custom Threat Prevention

Changing the Analysis Location

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

Note - The Threat Prevention policy defines the analysis location that is used for emulation (see *"Threat Emulation Environment" on page 99*).

To select the location of the emulation analysis

Step	Instructions
1	Double-click the Security Gateway object of the **Threat Emulation appliance**. The **Gateway Properties** window opens.
2	From the navigation tree, select **Threat Emulation**. The **Threat Emulation** page opens.
3	From the **Analysis Location** section, select the emulation location: ▪ **According to the gateway** - According to the gateway configuration. ▪ Specify: • **Check Point ThreatCloud** - Files are sent to the Check Point ThreatCloud for emulation. • **Local Gateway** - This Security Gateway does the emulation. • **Remote Emulation Appliances** - Remote appliances do the emulation. You can select one or more appliances on which the emulation is performed.
4	**Optional:** Select **Emulate files on ThreatCloud if not supported locally**. If files are not supported on the Threat 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 Threat Emulation appliance.

Setting the Activation Mode

You can change the Threat Emulation protection **Activation Mode** of the Security Gateway or Threat 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

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

Optimizing System Resources

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

You can configure the settings for these system resources:

- Minimum available hard disk space (If no emulation is done on a file, the Threat Prevention **Fail Mode** settings determine if the file is allowed or blocked.
- Maximum available RAM that can be used for Virtual Machines.

If you plan to change the available RAM, these are the recommended settings:

- If the appliance is only used for Threat Emulation, increase the available RAM.
- If the appliance is also used for other Software Blades, decrease the available RAM.

To optimize the system resources for the Threat Emulation appliance

Step	Instructions
1	Double-click the Security Gateway object of the **Threat Emulation appliance**. The **Gateway Properties** window opens.
2	From the navigation tree, select **Threat Emulation** > **Advanced**. The **Advanced** page opens.
3	Stopping the emulation is determined when the Log storage mechanism automatically deletes log files. Therefore, in order to change the relevant configured value (**Note** - It also affects the Log's files deletion). Navigate to **Logs** > **Local Storage** >. And from When disk space is below `<value>`**Start deleting old files**, you can change the `<value>`.
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: 1. Click **Configure**. The **Memory Allocation Configuration** window opens. 2. 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 512 MB - 1000 GB. 3. 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**.
8	Install the Threat Prevention Policy.

Managing Images for Emulation

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

To manage the images that the appliance uses for emulation

Step	Instructions
1	Double-click the Security Gateway object of the **Threat 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.

Additionally Supported Protocols for Threat Emulation

In addition to HTTP, FTP and SMTP protocols, which you can select in the SmartConsole, the Threat Emulation Software Blade also supports the IMAP and POP3 protocols:

To activate IMAP protocol support

Step	Instructions
1	Connect to the command line on your Security Gateway.
2	Log in to the Expert mode.
3	Back up this file: `$FWDIR/conf/malware_config` Run: `cp -v $FWDIR/conf/malware_config{,_BKP}`
4	Edit this file: `$FWDIR/conf/malware_config` Run: `vi $FWDIR/conf/malware_config`

Step	Instructions
5	In the `[imap]` section, change the value of this parameter: `imap_av_policy_on` from "`0`" to "`1`"
6	Save the changes in the file and exit the Vi editor.
7	Install the Threat Prevention Policy.

To activate POP3 protocol support

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Log in to the Expert mode.
3	Back up the file: `$FWDIR/conf/malware_config` Run: `cp -v $FWDIR/conf/malware_config{,_BKP}`
4	Edit the file: `$FWDIR/conf/malware_config` Run: `vi $FWDIR/conf/malware_config`
5	In the `[temp_for_av_profile]` section, change the value of the parameter `pop3_enabled` from "`0`" to "`1`".
6	Save the changes in the file, and then exit the Vi editor.
7	Install the Threat Prevention Policy.

Configuring Advanced Threat Emulation Settings - Custom Threat Prevention

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

In SmartConsole, go to **Security Policies > Threat Prevention** > **Custom Policy** > **Custom Policy Tools**.

Step	Instructions
1	Go to **Updates**. The **Updates** page opens.
2	Under **Threat Emulation**, click **Schedule Update**.
3	Select or clear these settings: ■ **Enable Threat Emulation engine scheduled update** ■ **Enable Threat Emulation images scheduled update**
4	To configure the schedule for Threat Emulation engine or image updates, click **Configure**.
5	Configure the automatic update settings to update the database: ■ To update every few hours, select **Update every**, and configure the number of hours, minutes, and seconds. ■ To update daily, select **Update at** > **Daily** and select the hour of update. ■ To update once or more for each week or month: 1. Select **At** and enter the time of day. 2. Click **Days**. 3. Click **Days of week** or **Days of month**. 4. Select the applicable days.
6	Click **OK**, and install the Threat Prevention policy.

Updating Threat Emulation Images Manually

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

The default setting is to download the package once a week on Sunday. If Sunday is a work day, we recommend that you change the update setting to a non-work day.

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

In SmartConsole, go to **Security Policies > Threat Prevention** >**Custom Policy** > **Custom Policy Tools**.

Step	Instructions
1	Go to **Updates**. The **Updates** page opens.
2	Under **Threat Emulation**, click **Update Images**.
3	Select a gateway. Click **OK**.
4	Install the Threat Prevention policy.

Fine-Tuning the Threat Emulation Appliance

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

Configuring the Emulation Limits

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

- Maximum file size (up to 100,000 KB)
- Maximum time that the Software Blade does emulation
- Maximum time that a file waits for emulation in the queue (for Threat 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:

- **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.

If the Security Gateway is enabled as a Mail Transfer Agent - The Mail Transfer Agent settings define if a file is allowed or blocked (see *"Configuring the Security Gateway as a Mail Transfer Agent" on page 170*).

To configure the emulation limits

Step	Instructions
1	In SmartConsole, go to **Manage & Settings** > **Blades** > **Threat Prevention** > **Advanced Settings**. The **Threat Prevention Engine Settings** window opens.
2	Go to **Threat Emulation** tab > **Emulation Limits**.
3	Configure the **Maximum file size for emulation** and the **Maximum file time in queue**.
4	From **When limit is exceeded traffic is accepted with track**, select the action if a file is not sent for emulation: ■ **None** - No action is done ■ **Log** - The action is logged ■ **Alert** - An alert is sent to SmartView Monitor
5	Click **OK**, and then install the policy.

Changing the Size of the Local Cache

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

To change the size of the local cache

Step	Instructions
1	In SmartConsole, select **Manage & Settings** > **Blades** > **Threat Prevention** > **Advanced Settings**. The **Threat Prevention Engine Settings** window opens.
2	Go to the **Threat Emulation** tab > **Advanced Settings**.
3	In **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 install the policy.

Configuring Threat Extraction Settings

To configure Threat Extraction settings for a Threat Prevention profile

Step	Instructions
1	From the left navigation panel, click **Security Policies**.
2	In the **Custom Policy Tools** section, click **Profiles**.
3	Right-click a profile and select **Edit**. The **Profiles** properties window opens.
5	In the left pane navigation tree, go to **Threat Extraction**, and configure these settings: ■ *"Threat Extraction General Settings" below* ■ *"Threat Extraction Advanced Settings" on page 115*
6	Click **OK**.
7	Install the Threat Prevention policy.

Note - You can configure some of the Threat Extraction features in a configuration file, in addition to SmartConsole and the CLI. See sk114613.

Threat Extraction General Settings

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

UserCheck Settings

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

  Note - This option is only configurable when the Threat Emulation Software Blade is activated on the **General Properties** pane of the profile.

- **UserCheck Message**

  You can create or edit UserCheck messages on the UserCheck page (see *"Threat Prevention and UserCheck - Autonomous Threat Prevention" on page 327*).

  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.

Selecting the success or cancellation messages of the file download

Step	Instructions
1	Go to **Manage & Settings**.
2	Select **Blades** > **Threat Prevention**.
3	Select **Advanced Settings** > **UserCheck** (see *"Threat Prevention and UserCheck - Autonomous Threat Prevention" on page 327*).

You can customize a UserCheck message only for SMTP files. For HTTP files (supported on Security Gateways R80.30 and above), the message which the user gets is not customizable in SmartConsole. You can only customize it on the gateway.

Optional

To give the user access to the original email, you can add the **Send Original Mail** field in the Threat Extraction **Success Page**.

Step	Instructions
1	Go to **Threat Prevention**.
2	Select **Custom Policy Tools** > **UserCheck** > **Threat Extraction** > **Success Page**.
3	Right-click > **Clone**.
4	Click inside the message > **Insert Field**, and then select **Send Original Mail**. The **Send Original Mail** is added to the message body.

Protocol

- **Web (HTTP/HTTPS)** - Supported from Security Gateways R80.30 and above. To allow web support, enable HTTPS Inspection (see *"HTTPS Inspection " on page 393* > section "*Enabling HTTPS Inspection*"). By default, Threat Extraction web support works on these standard ports: HTTP - Port 80, HTTPS - Port 443, HTTPS Proxy - Port 8080.

  To enable web support on other ports, create a new TCP service. In **General** > **Protocol** select **HTTP**, and in **Match By**, select **Customize** and enter the required port number.

Notes:

- When you enable Threat Extraction, web support is enabled automatically. to disable web support, clear this checkbox.
- After a file is scanned by the Threat Extraction Software Blade, the user receives a message on the action that was done on the file. To customize the message, see sk142852.
- Threat Extraction web support applies to web downloads, but not web uploads.

- **Mail (SMTP)** - Click **Mail** to configure the SMTP traffic inspection by the Threat Extraction Software Blade. This links you to the Mail page of the Profile settings (see *"Configuring Mail Settings" on page 59*).

For information on storage of the original files, see *"Storage of Original Files" on page 122*.

Extraction Method

- **Extract potentially malicious parts from files** - Selected by default

  Click **Configure** to select which malicious parts the Software Blade extracts. For example, macros, JavaScript, images and so on.

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

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

Extraction Settings

- **Process all files**

  Selected by default.

- **Process malicious files when the confidence level is**

  Set a Low, Medium, or High confidence level. This option is only configurable when the Threat Emulation Software Blade is activated in the **General Properties** pane of the profile.

File Types

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

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

- **Process specific file type families**

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

Notes:

- Supported file types for web are: Word, Excel, PowerPoint and PDF.
- For e-mail attachments:
  - For `jpg`, `bmp`, `png`, `gif`, and `tiff` files - Threat Extraction supports only extraction of potentially malicious content.
  - For `hwp`, `jtd`, `eps` files - Threat Extraction supports only conversion to PDF.
  - For Microsoft Office and PDF files and all other file types on the list - Threat Extraction supports both extraction of potentially malicious content and conversion to PDF.
  - You can also configure supported file types in the configuration file. For explanation, see sk112240.

Protected Scope

Threat Extraction protects incoming files from external interfaces and DMZ. The user cannot configure the protected scope.

Threat Extraction Advanced Settings

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

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

- **Corrupted files**

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

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

  Allow lets the recipient receive the corrupted file.

- **Encrypted files**

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

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

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

  Allow lets the recipient receive the encrypted file.

Scenario 1: Excluding senders from scanning

Scanning takes time and resources, so if you know a source is safe, you may want to stop scanning the reports from this source.

Example:

- Control and Monitoring systems that send daily reports to IT departments.
- Reports sent by a Mail Relay server about spam emails that it stopped.

In SmartConsole, you can exclude specific senders from the Threat Extraction scanning.

To exclude a sender from the Threat Extraction scanning:

Step	Instructions
1	Go to **Security Policies > Threat Prevention > Profiles**.
2	Right-click the profile name and select **Clone**. The **Clone Object** window opens.
3	Enter a name for the cloned profile.
4	Click **OK**.

Step	Instructions
5	In the new profile, go to **Mail** > **Exceptions** > **Extraction Exclusion/Inclusion** > **Scan all emails**, and click **Exceptions**. The **Exclude/Include Users** window opens.
6	In the **Senders** section, click the **+** sign to add the senders to exclude from the Threat Extraction scan.

Scenario 2: Allowing digitally signed emails without scanning

The attorneys at the legal department in Corp X send and receive contracts and other legal documents signed with a digital signature. According to Corp X's Security Policy, the Threat Extraction blade scans all files received by the legal department. A digital signature must show the authenticity of a document. If the Threat Extraction blade scans the document, the digital signature can no longer prove the document's authenticity. The configuration, therefore, must allow digitally signed emails.

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

Scenario 3:

For security reasons, the IT department in Corp X changed the default extraction method in the Threat Prevention profile from **Extract potentially malicious parts from files** to **Convert to PDF**.

The economists in the Finance Department in Corp X receive certain files by email in excel formats, or download excel files from the Web, and must work on them in the files' original format. To keep the excel files in their original formats you must set the Threat Extraction to clean the files and not convert them to PDF.

To override the profile web extraction method

Step	Instructions
1	Go to **File Types**, select **Process specific file type families** and click **Configure**. The **Threat Extraction Supported File Types** window opens.
2	Go to the `xslx` row. Right-click the **Mail Extraction Method** and select **Clean**. Do the same for the **Web Extraction Method**.

Configuring Threat Extraction on the Security Gateway - Custom Threat Prevention

To configure the Threat Extraction blade on the Security Gateway

Step	Instructions
1	Make sure Threat Extraction is enabled on the gateway. For more information, see *"Getting Started with Custom Threat Prevention" on page 35*.
2	In the **Gateways & Servers** view, double-click the Security Gateway object and click the **Threat Extraction** page.
3	Make sure the **Activation Mode** is set to **Active**.
4	In the **Resource Allocation** section, configure the resource settings.
5	Click **OK**.
6	Install the Access Control Policy.

In addition to configuring Threat Extraction on the gateway:

Enable Threat Extraction to scan one or all of these types of documents

- For Threat Extraction to scan e-mail attachments, enable the gateway as a Mail Transfer Agent (MTA) (see *"Configuring the Security Gateway as a Mail Transfer Agent" on page 170*).
- When Threat Extraction is enabled on the gateway, it is automatically enabled to scan web downloads. To disable web download scan:

Step	Instructions
1	Go to the **Security Policies** view > **Threat Prevention > Custom Policy Tools > Profiles**.
2	Double-click a profile > **Threat Extraction > General > Protocol**.
3	Clear this checkbox: **Web (HTTP/HTTPS)**.

- For Threat Extraction API support, in the gateway editor, go to **Threat Extraction** > **Web API** > **Enable API**.

Threat Extraction and Endpoint Security

When both the Threat Extraction blade and the SandBlast Agent for Browsers are activated on the network Security Gateway, a special configuration is required. Without this configuration, when you download a file, it can be cleaned twice, both by the Threat Extraction blade and by the SandBlast Agent.

To prevent this, the Security Gateway adds a digital signature to all the files cleaned by the Threat Extraction blade. When the SandBlast Agent intercepts a downloaded file. If the digital signature is verified successfully, SandBlast Agent does not clean the file, so the file is not cleaned twice.

For details on how to configure the digital signature on the Security Gateway and how to configure the Endpoint management, see sk142732.

Configuring Threat Extraction in a Cluster

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

To configure Threat Extraction in a cluster

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

Notes:

- Only the High Availability mode is supported.
- The original files are synchronized between the Cluster Members. In case of a failure, there is still access to the original files.

Threat Extraction Statistics

To see Threat Extraction statistics

Step	Instructions
1	Connect to the command line on the Security Gateway with the Threat Extraction enabled.
2	Run these commands: ▪ `cpview` ▪ `cpstat scrub -f threat_extraction_statistics`

Using the Gateway CLI

The Security Gateway has a Threat Extraction menu

In this menu, you can:

- 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

Step	Instructions
1	Connect to the command line on the Security Gateway / each Cluster Member.
2	Log in to the Expert mode.
3	Run: `scrub`

The menu shows these options:

Option	Description
`debug`	Controls debug messages.

Option	Description
`queues`	Shows information on Threat Extraction queues. 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 `scrubd` (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.
`cache`	Shows and resets cache.
`backup_expired_mail`	Backs up expired mails to external storage.

Storage of Original Files

The Threat Extraction blade reconstructs files (cleans or converts files to PDF) to eliminate potentially malicious content. After the Threat Extraction blade reconstructs the files, the original files are saved on the gateway for a default period.

Mail attachments

Mail attachments are saved for a default period of 14 days.

To configure a different number of days for storage of mail attachments:

Step	Instructions
1	From the left navigation panel, click **Gateways & Servers**.
2	Open the Security Gateway / Cluster object.
3	From the left tree, click **Threat Extraction**.
4	Click **Resource Allocation** > **Delete stored original files older than x Days**.
5	Change the number of days as required. The maximum is 45 days.
6	Click **OK**.
7	Install the Threat Prevention Policy.

To save the files for a longer period, you must back them up to external storage (see *"Backup to External Storage" on the next page*).

Web downloads

Web downloads are saved for a default period of 2 days.

To configure a different number of days for storage of web downloads:

Step	Instructions
1	Connect to the command line on the Security Gateway / each Cluster Member.
2	Log in to the Expert mode.
3	Edit the `$FWDIR/conf/scrub_debug.conf` file.
4	Search for `http_keep_original_duration` and change the value as required. Value can be between 2 and 45 days.

Step	Instructions
5	Save the changes in the file and exit the editor.

To save the files for a longer period, you must back them up to external storage (see *"Backup to External Storage" below*).

Backup to External Storage

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

Notes:

- In a cluster, you must configure all Cluster Members in the same way.
- End-users cannot access files on external storage. Only the administrator can access these files.

To back up original files to external storage

Step	Instructions
1	Connect to the command line on the Security Gateway / each Cluster Member.
2	Log in to the Expert mode.

3	Create the backup folder:
	`mkdir /mnt/<local_backup_folder>`
	Example:
	`mkdir /mnt/MyLocalBackupFolder`

4	Mount the backup folder to the remote folder:
	`mount -t cifs <remote_folder> /mnt/<local_backup_folder>`
	Example:
	`mount -t cifs //MyServer/MyBackupFolder /mnt/MyLocalBackupFolder`
	Best Practice - To preserve the mount configuration after reboot, configure a Scheduled Job to run the applicable "`mount`" command at startup (in Gaia Portal, go to **System Management** > **Job Scheduler**).

5	Edit the `$FWDIR/conf/scrub_debug.conf` file: `vi $FWDIR/conf/scrub_debug.conf`

Step	Instructions

6	Search for this section:
	`:external_storage.`
	1. Change the `enabled` value from "`0`" to "`1`".
	2. In the `external_path` parameter, write the full path to the local backup folder.
	3. The `expired_in_days` parameter sets the backup date.
	The value you enter for this parameter specifies how many days before expiration the backup is performed.
	Example:
	`:external_storage (`
	`    :enabled (1)`
	`    :external_path ("/mnt/MyLocalBackupFolder")`
	`    :expired_in_days (5)`

7	Configure the applicable values:
	1. Change the `enabled` value from "`0`" to "`1`".
	2. In the `external_path` parameter, write the full path to the local backup folder.
	3. The `expired_in_days` parameter sets the backup date.
	The value you enter for this parameter specifies how many days before expiration the backup is performed.
	Example:
	`:external_storage (`
	`    :enabled (1)`
	`    :external_path ("/mnt/MyLocalBackupFolder")`
	`    :expired_in_days (5)`

8	Save the changes in the file and exit the editor.

To test the backup manually

Run this command:

```
scrub backup_expired_mail <days for expired entries> <external_path>
```

In "*<days for expired entries>*" enter "0".

Configuring Zero Phishing Settings - Custom Threat Prevention

Zero Phishing uses two main engines:

- Real-time phishing prevention based on URLs.
- In-Browser Zero Phishing.

For more information about these two engines, see *"The Check Point Threat Prevention Solution" on page 26*.

For information o how to enable Zero Phishing, see *"Getting Started with Custom Threat Prevention" on page 35*.

To disable the Zero Phishing protection:

1. In SmartConsole, go to **Security Policies** > **Threat Prevention** > **Custom Threat Prevention** > **Custom Policy Tools** > **Profiles**.
2. Select the required profile.
3. In the **General Policy** page, clear **Zero Phishing**

To disable In-browser Zero Phishing:

1. In SmartConsole, go to **Security Policies** > **Threat Prevention** > **Custom Threat Prevention** > **Custom Policy Tools** > **Profiles**.
2. Select the required profile.
3. In the profile, go to the Zero Phishing page.
4. Clear the **In-browser Zero Phishing** checkbox.

Limitations:

- In-browser Zero Phishing does not support Internet Explorer.
- In-browser Zero Phishing does not support mirrored traffic (Mirror Port, Span Port, Tap mode).

You can block or allow sites that the Cloud Service is unable to classify as Phishing or Benign.

To block unclassified sites, run this command on the Security Gateway CLI:

```
zph att set inbrowser_block_unclassified_sites 1
```

To allow unclassified sites (default), run this command on the Security Gateway CLI:

```
zph att set inbrowser_block_unclassified_sites 0
```

Configuring Zero Phishing UserCheck Settings

Starting from SmartConsole Build 646, you can select the UserCheck message that appears in case of a suspected phishing attempt.

Prevent - Select the UserCheck message that opens for the **Prevent** action. The default message is **Zero Phishing Blocked**.

You can create UserCheck messages of your own for the **Prevent** action and configure their settings. To do this , go to **Security Policies** > **Threat Prevention** > **Custom Threat Prevention** > **Custom Policy Tools** > **UserCheck**, and in the **UserCheck** page, click **New**. For more information, see *"Threat Prevention and UserCheck - Custom Threat Prevention" on page 246*.

Configuring Zero Phishing Exceptions

To skip unnecessary scans of popular sites, we recommend to configure the Zero Phishing blade to bypass specific popular sites.

To configure the Zero Phishing blade to bypass popular sites:

1. In SmartConsole, go to the **Security Policies** view > **Threat Prevention** > **Exceptions**.
2. Click **Add Exception** > **Below**.
3. Give a name to the rule.
4. In the **Protected Scope** column:
   a. Click the "Plus" (**+**) button.
   b. In the window that opens, go to **Import** > **Updatable Objects**.
   c. Search for **Zero Phishing Bypass** and select it.
   d. Click **OK**.
5. In the **Protection/Site/File/Blade** column:
   a. Click the "Plus" (**+**) button.
   b. From the drop-down menu in the window that opens, select **Blades**.
   c. From the list of blades, select **Zero Phishing**.
6. In the **Action** column, select **Inactive**.
7. Install Policy.

Notes -

- For proper enforcement, make sure that this rule is the last rule under Global Exceptions.
- For any exception rule that contains **Zero Phishing** in the **Protection/Site/File/Blade** column, in the **Install On** column, you must select Security Gateways with Zero Phishing enabled.

The list of bypassed sites dynamically changes. To see the list, go to sk179726.

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 Gateway external IP address as the DNS trap address but:

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

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

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

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

Configuring the Malware DNS Trap parameters for the profile

Step	Instructions
1	In SmartConsole, select **Security Policies > Threat Prevention**.
2	From the **Custom Policy 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.

Configuring the Malware DNS Trap parameters for a gateway

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

Exception Rules

If necessary, you can add an **exception** directly to a rule.

An exception sets a different **Action** to an object in the **Protected Scope** from the Action specified Threat Prevention rule.

In general, exceptions are designed to give you the option to reduce the level of enforcement of a specific protection and not to increase it.

Example

> The Research and Development (R&D) network protections are included in a profile with the **Prevent** action.
>
> You can define an exception which sets the specific R&D network to **Detect**.
>
> For some Anti-Bot and IPS signatures only, you can define exceptions which are stricter than the profile action.

You can add one or more exceptions to a rule. The exception is added as a shaded row below the rule in the Rule Base.

It is identified in the **No** column with the rule's number plus the letter E and a digit that represents the exception number.

For example, if you add two exceptions to rule number 1, two lines will be added and show in the Rule Base as E-1.1 and E-1.2.

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

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

To add an exception to a rule

Step	Instructions
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). Click **OK**.

Step	Instructions
5	Install the Threat Prevention Policy.

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

Disabling a Protection on One Server

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

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

Name	Protected Scope	Protection/Site	Action	Track	Install On
Monitor Bot Activity	`* Any`	`- N/A`	A profile based on the **Optimized** profile. Edit this profile > go to the **General Policy** pane> in the **Activation Mode** section, set every **Confidence** to **Prevent**.	Log	Policy Targets
Exclude	Server_1	`Backdoor.Win32.Agent.AH`	**Detect**	Log	Server_1

To add an exception to a rule

Step	Instructions
1	In SmartConsole, go to Security Policies > **Threat Prevention > Custom Policy**.

Step	Instructions
2	Click the rule that contains the scope of Server_1.
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 Allow List files. When you add EICAR files through Exceptions in Policy rules, the gateway still blocks them, if archive scanning is enabled. ■ **Action** - Keep it as **Detect**. ■ **Track** - Keep it as **Log**. ■ **Install On** - Keep it as **Policy Targets** or select specified gateways, on which to install the rule.
6	Install the Threat Prevention Policy.

Software Blade Exceptions

You can configure an exception for an entire blade.

To configure a blade exception

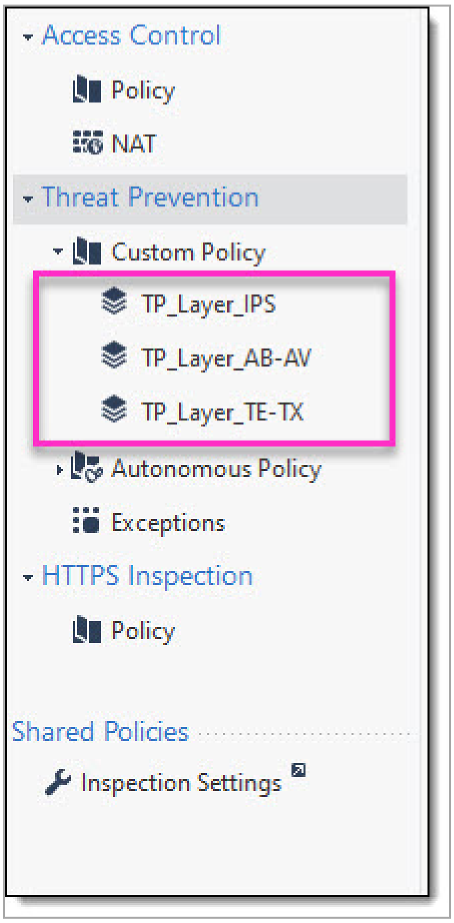
Step	Instructions
1	In the **Policy**, select the Layer rule to which you want to add an exception.
2	Click **Add Exception**.
3	Select the **Above**, **Below**, or **Bottom** option according to where you want to place the exception.
4	In the **Protection/Site** column, select **Blades** from the drop-down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

You can create a rule or exception for a specific blade for a specific website/URL because the Security Gateway is always the destination in non-transparent proxy mode.

In a transparent proxy mode, or while the traffic is inspected by a Security Gateway, this setup is not a challenge because the destination is configured in the Destination column, and the excluded blade is configured in the Protection/Site/File/Blade column. This is not possible in non-transparent mode because the destination is always the Security Gateway itself.

To create an exception for a specific Threat Prevention blade for a specific website in non-transparent proxy mode

1. Create a separate layer with a separate profile for each blade or a pair of blades (for example: Anti-Virus and Anti-Bot, or Threat Emulation and Threat Extraction):

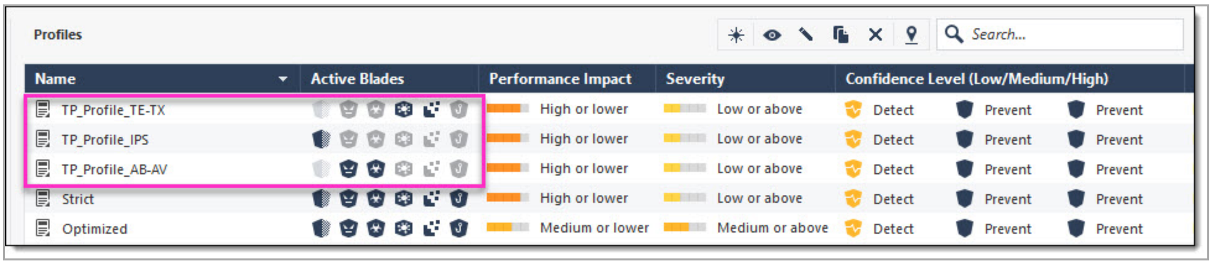


- Access Control
  - Policy
  - NAT
- Threat Prevention
  - Custom Policy
    - TP_Layer_IPS
    - TP_Layer_AB-AV
    - TP_Layer_TE-TX
  - Autonomous Policy
  - Exceptions
- HTTPS Inspection
  - Policy

Shared Policies

- Inspection Settings

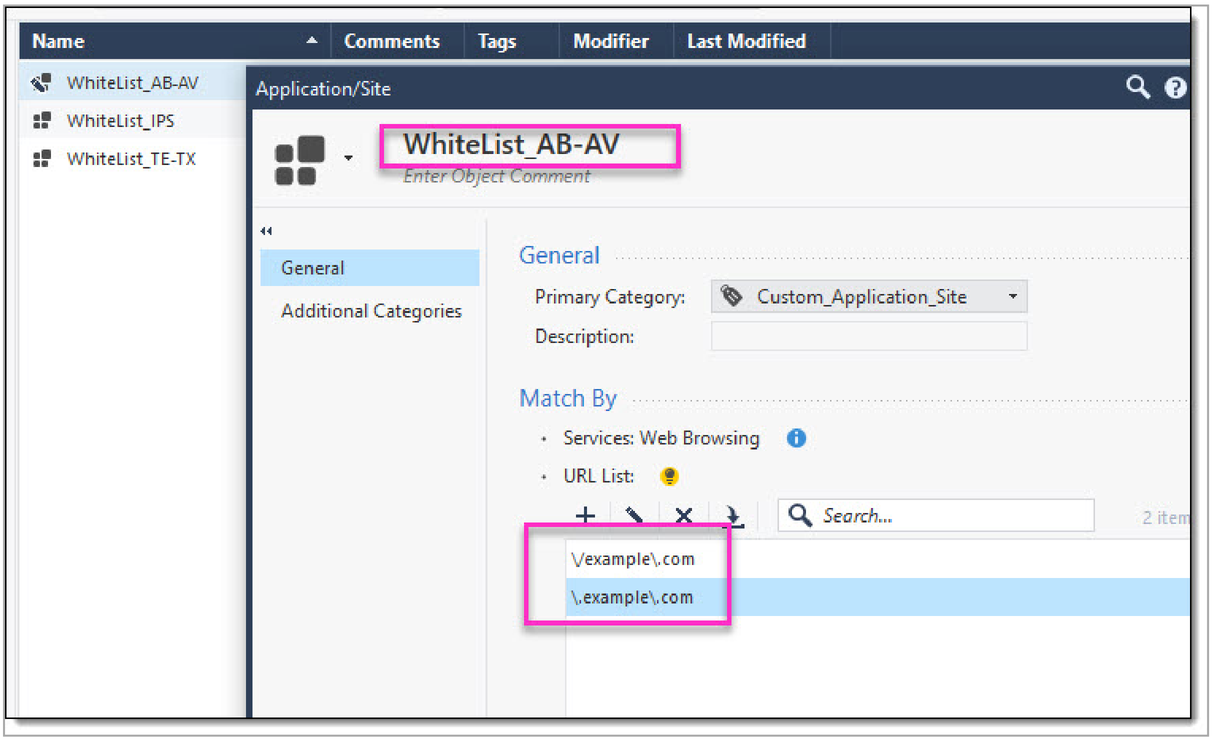
2. Create a separate profile for each layer and enable only the specific blade:



Profiles

Name	Active Blades	Performance Impact	Severity	Confidence Level (Low/Medium/High)		
TP_Profile_TE-TX		High or lower	Low or above	Detect	Prevent	Prevent
TP_Profile_IPS		High or lower	Low or above	Detect	Prevent	Prevent
TP_Profile_AB-AV		High or lower	Low or above	Detect	Prevent	Prevent
Strict		High or lower	Low or above	Detect	Prevent	Prevent
Optimized		Medium or lower	Medium or above	Detect	Prevent	Prevent

3. Create a custom Application/Site for each layer. For instructions, refer to sk165094:



Name	Comments	Tags	Modifier	Last Modified
WhiteList_AB-AV				
WhiteList_IPS				
WhiteList_TE-TX				

Application/Site

WhiteList_AB-AV

Enter Object Comment

General

Primary Category: Custom_Application_Site

Description:

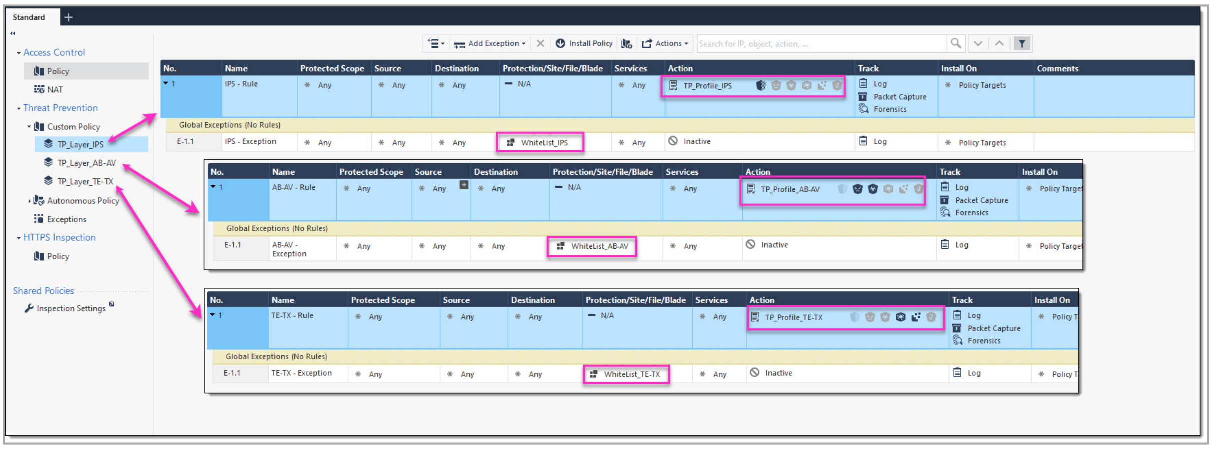
Match By

- Services: Web Browsing
- URL List:

\/example\\.com

\\.example\\.com

4. Create a Rule Base for each layer, and a different exception rule with the created Custom Application/Site in Protection/Site/File/Blade:



No.	Name	Protected Scope	Source	Destination	Protection/Site/File/Blade	Services	Action	Track	Install On	Comments
1	IPS - Rule	Any	Any	Any	N/A	Any	TP_Profile_IPS	Log Packet Capture Forensics	Policy Targets	
Global Exceptions (No Rules)										
E-1.1	IPS - Exception	Any	Any	Any	WhiteList_IPS	Any	Inactive	Log	Policy Targets	

No.	Name	Protected Scope	Source	Destination	Protection/Site/File/Blade	Services	Action	Track	Install On
1	AB-AV - Rule	Any	Any	Any	N/A	Any	TP_Profile_AB-AV	Log Packet Capture Forensics	Policy Target
Global Exceptions (No Rules)									
E-1.1	AB-AV - Exception	Any	Any	Any	WhiteList_AB-AV	Any	Inactive	Log	Policy Target

No.	Name	Protected Scope	Source	Destination	Protection/Site/File/Blade	Services	Action	Track	Install On
1	TE-TX - Rule	Any	Any	Any	N/A	Any	TP_Profile_TE-TX	Log Packet Capture Forensics	Policy T
Global Exceptions (No Rules)									
E-1.1	TE-TX - Exception	Any	Any	Any	WhiteList_TE-TX	Any	Inactive	Log	Policy T

5. In the **Action** column, select **Detect** or **Inactive** to disable the applicable Threat Prevention Blade for the applicable websites/URLs.

Notes -

- You must make changes to a Threat Prevention profile on all applicable profiles. For example: if you change the action for medium confidence protections on Threat Prevention blades, you must make the change in all profiles.
- We recommend to have as few layers as possible.
- When HTTPS Inspection and non-transparent proxy are enabled, the proxy IP address of the Security Gateway is matched as the destination in the HTTPS Inspection Rule Base.
- For a detailed explanation of the enforcement in Multiple-Layered Security Policies, see *Threat Prevention Policy Layers* .
- For information on how to configure a Security Gateway as HTTP/HTTPS proxy, see sk110013.

Creating Exceptions from IPS Protections

To create an exception from an IPS protection

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

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 appear below **Global Exceptions**.

To update a rule exception or global exception from a log

Step	Instructions
1	Click **Logs & Monitor** > **Logs** tab.

Step	Instructions
2	Right-click the log and select **Add Exception**.
3	Configure the settings for the exception.
4	In the **New Exception Rule** window: ▪ To show the exception in the policy, click **Go to**. ▪ Otherwise, click **Close**.
5	Install the Threat Prevention Policy.

Exception Groups

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

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

The Exceptions Groups pane contains these options

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 the Global Exceptions group are automatically added to every rule in the Rule Base. For other exception groups, you can decide to which rules to add them.

Exception Groups in the Rule Base

Global exceptions and other exception groups are added as shaded rows below the rule in the Rule Base. Each exception group is labeled with a tab that shows the exception group's name. The exceptions within a group are identified in the **No** column using the syntax: `E - <rule number>.<exception number>`, where `E` identifies the line as an exception.

For example

> If there is a Global Exceptions group that contains two exceptions, all rules show the exception rows in the Rule Base **No** column as E-1.1 and E-1.2. **Note** - that the numbering of exception varies when you move the exceptions within a rule.

To view exception groups in the Rule Base:

Click the plus or minus sign next to the rule number in the **No**. column to expand or collapse the rule exceptions and exception groups.

Creating Exception Groups

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

Procedure

Step	Instructions
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 policy.

To use exception groups, you must add exception rules to them.

To add exceptions to an exception group

Step	Instructions
1	In SmartConsole, select **Security Policies > Threat Prevention > Exceptions**.

Step	Instructions
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 Exceptions to Exception Groups

To use exception groups, you must add exception rules to them.

Procedure

Step	Instructions
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**.

Procedure

Step	Instructions
1	Click **Security Policies > Threat Prevention > Custom Policy**.
2	Right-click the rule and select **Add Exception Group** > **<Group Name>**.
3	Install the Threat Prevention policy.

Configuring Advanced Threat Prevention Settings

Threat Prevention Engine Settings - Custom Threat Prevention

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.

By default, all Security Gateways that are controlled by a single Security Management Server, act the same according to t fail mode configuration of the Security Management Server.

Starting from R81.20, you can control the fail mode configuration for each individual Security Gateway by using the *malware_config* file.

Valid Values

Value	Description
by_policy	This is the default value. Fail mode is determined by the policy.
open	All connections to the specific Security Gateway are allowed in a situation of engine overload or failure.
close	All connections to the specific Security Gateway are blocked in a situation of engine overload or failure.

To set fail mode on a specific Security Gateway:

1. Connect to the command line on the Security Gateway.
2. Log in to the Expert mode.
3. Backup the current `$FWDIR/conf/malware_config` file:

   ```
   [Expert@HostName]# cp $FWDIR/conf/malware_config
   $FWDIR/conf/malware_config_ORIGINAL
   ```

4. Set the required fali mode for the specific Security Gateway:

   To set the fail mode to be controlled by the policy, run:

   ```
   [Expert@HostName]# sed -ie 's/^fail_close=.*$/fail_close=by_
   policy/' $FWDIR/conf/malware_config
   ```

   To set the fail mode to "open", run:

   ```
   [Expert@HostName]# sed -ie 's/^fail_close=.*$/fail_close=open/'
   $FWDIR/conf/malware_config
   ```

   To set fail mode to "close", run:

   ```
   [Expert@HostName]# sed -ie 's/^fail_close=.*$/fail_close=close/'
   $FWDIR/conf/malware_config
   ```

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. Access to the cloud is required if the response is not cached. Resource classification mode determines if the connection is allowed or suspended while the Security Gateway queries the Check Point Online Web Service.

- 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.

  These settings are relevant for Anti-Virus, Anti-Bot and Zero Phishing.

- **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, and in the background, the Check Point Online Web Service continues the categorization procedure. After the classification is complete, a "Detect" log is generated. The log includes this description: "Connection was allowed because background classification mode was set". 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-Virus, Anti-Bot and Zero Phishing. For example, click **Customize** to set Anti-Bot to Hold mode and Anti-Virus and Zero Phishing to Background mode.

If you change Background mode to Hold mode, the Security Gateway holds the file and does not send it to the client browser. The Browser shows the file as still being downloaded, but the download is stuck at some point. The Security Gateway continues the download only after the scan is complete or if a timeout occurred at the Security Gateway. If the file is malicious, the Security Gateway stops sending the file.

Note - If the "Prevent" action is used in the Threat Prevention policy, then a file that Threat Emulation identified as malware in the past, is blocked. The file will not be sent to the destination even in the "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 the Anti-Bot, Threat Emulation, and Anti-Virus, the default session is 10 hours (600 minutes).

To adjust the length of a session

Step	Instructions
1	Go to **Manage & Settings > Blades > Threat Prevention > Advanced Settings > General > Connection Unification > Session unification timeout (minutes)**.
2	Enter the required value.
3	Click **OK**.

Configuring Anti-Bot Whitelist

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

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

Step	Instructions
1	Go to the **Manage & Settings > Blades > Threat Prevention > Advanced Settings > Anti-Bot**.
2	Click the **+** sign.

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

Selecting Emulation File Types

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

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

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

Configuring Advanced Engine Settings for Threat Extraction

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

To configure file type support

Step	Instructions
1	Click the **Manage & Settings** view > **Blades > Threat Prevention > Advanced Settings**. The **Threat Prevention Engine Settings** window opens.
2	In Threat Extraction, click **Configure File Type Support**. The **Threat Extraction Supported File Types** window opens.
3	From the list select the file types which the Threat Extraction blade supports.
4	Click **OK**.

To configure mail signatures

Step	Instructions
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 mail that has had threats extracted. A link to the original files is added if the email recipient is allowed to access it. The link opens the UserCheck Portal. The portal shows a list of attachments the recipient can download. ■ **Mail signatures for unmodified attachments** You can click the **Insert Field** button to insert a reference ID into the signature text. Use this ID to send the file to the recipient. You can also find the ID in the logs. On the Security Gateway, run the command: `scrub send_orig_email`
2	Click **OK**.

SNORT Signature Support

SNORT is a popular, open source, Network Intrusion Detection System (NIDS). For more information about SNORT see snort.org.

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

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

To perform these actions on a Check Point Management Server

Step	Instructions
1	Import existing SNORT rules from a file.
2	After important and conversion: 1. SNORT Protection names are SNORT imported: `<Value of the 'msg' field in the original SNORT rule>` See *"Creating SNORT Rule Files" on page 154*. 2. SNORT Protections get these attributes automatically: - Performance Impact - **High** - Severity - **High** - Confidence Level - **Low** or **Medium**
3	Delete the existing SNORT rules.

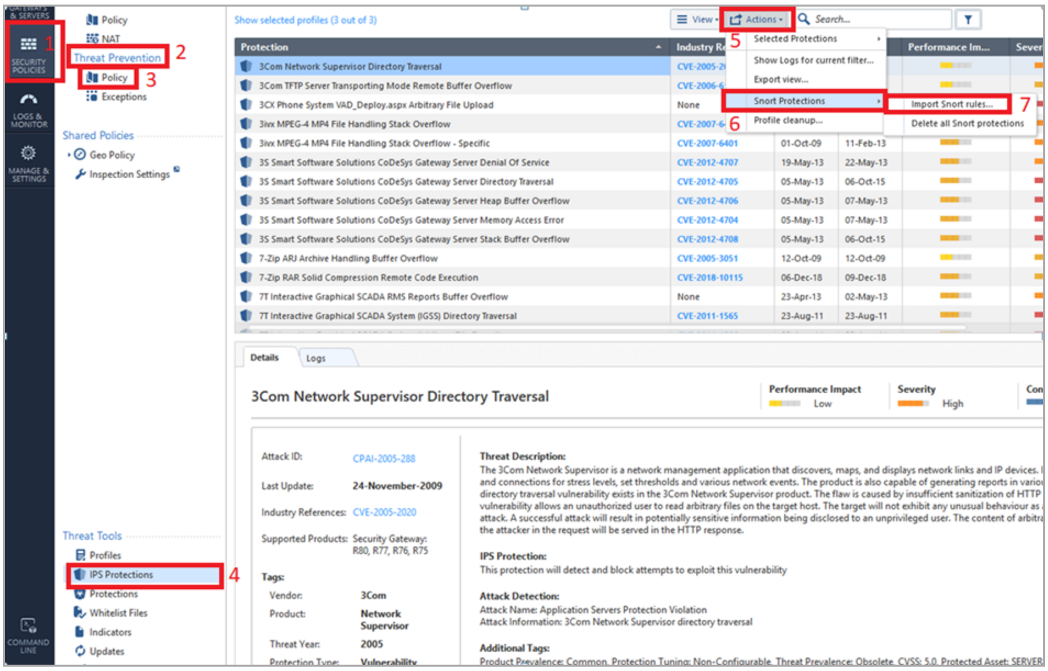
Importing SNORT Protection Rules to the Security Management Server

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

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

To import SNORT Protection rules to the Security Management Server

Step	Instructions
1	Connect with SmartConsole to the Security Management Server that manages the applicable Security Gateway or Security Cluster.
2	In SmartConsole, go to **Security Policies** > **Threat Prevention** > **Custom Policy**

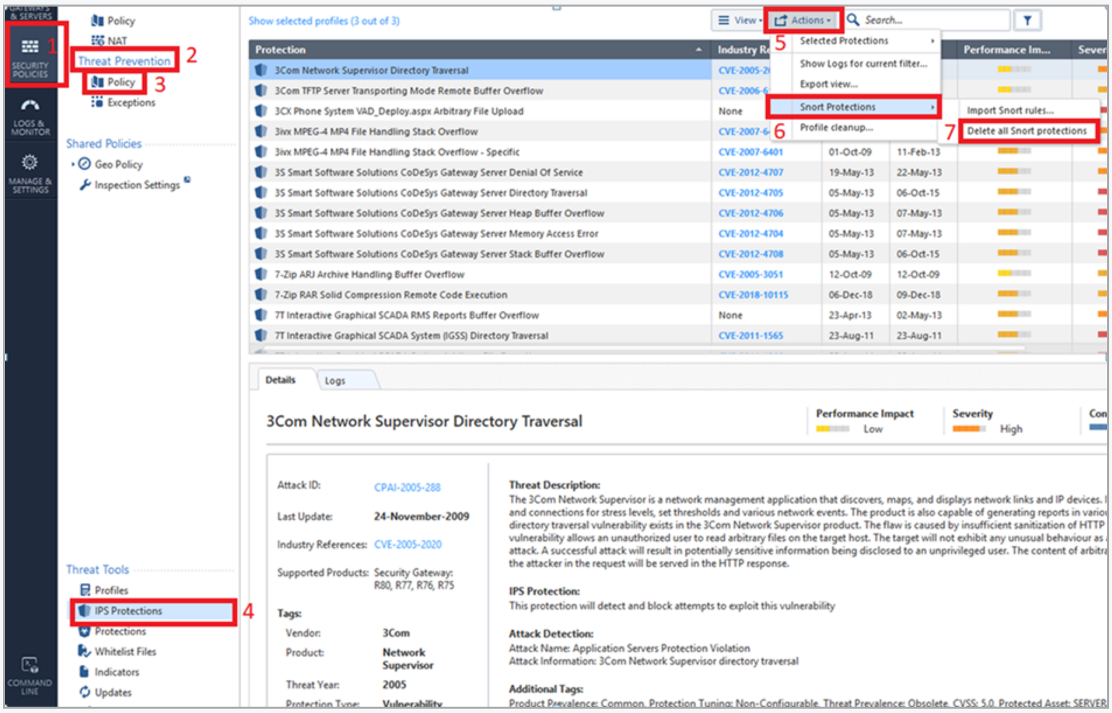
Step	Instructions
3	In the bottom section **Custom Policy Tools**, click **IPS Protections**.
4	From the top toolbar, click **Actions** > **Snort Protections** > **Import Snort rules**.
5	Select the file with the SNORT rules and click Open. The tool converts the rules to Check Point syntax and updates the protections database. **Important** - SmartConsole shows the converted SNORT rules as IPS protections whose names start with "**Snort imported**".  GATEWAYS & SERVERS SECURITY POLICIES 1 Policy NAT Threat Prevention 2 Policy 3 Exceptions Shared Policies Geo Policy Inspection Settings LOGS & MONITOR MANAGE & SETTINGS Threat Tools Profiles IPS Protections 4 Protections Whitelist Files Indicators Updates COMMAND LINE Show selected profiles (3 out of 3) View Actions 5 Search... Selected Protections Show Logs for current filter... Export view... Snort Protections 6 Profile cleanup... Import Snort rules... 7 Delete all Snort protections Details Logs Protection · Industry Re... · Performance Im... · Sever... 3Com Network Supervisor Directory Traversal · CVE-2005-2 3Com TFTP Server Transporting Mode Remote Buffer Overflow · CVE-2006-6 3CX Phone System VAD_Deploy.aspx Arbitrary File Upload · None 3ivx MPEG-4 MP4 File Handling Stack Overflow · CVE-2007-6 3ivx MPEG-4 MP4 File Handling Stack Overflow - Specific · CVE-2007-6401 · 01-Oct-09 · 11-Feb-13 3S Smart Software Solutions CoDeSys Gateway Server Denial Of Service · CVE-2012-4707 · 19-May-13 · 22-May-13 3S Smart Software Solutions CoDeSys Gateway Server Directory Traversal · CVE-2012-4705 · 05-May-13 · 06-Oct-15 3S Smart Software Solutions CoDeSys Gateway Server Heap Buffer Overflow · CVE-2012-4706 · 05-May-13 · 07-May-13 3S Smart Software Solutions CoDeSys Gateway Server Memory Access Error · CVE-2012-4704 · 05-May-13 · 07-May-13 3S Smart Software Solutions CoDeSys Gateway Server Stack Buffer Overflow · CVE-2012-4708 · 05-May-13 · 06-Oct-15 7-Zip ARJ Archive Handling Buffer Overflow · CVE-2005-3051 · 12-Oct-09 · 12-Oct-09 7-Zip RAR Solid Compression Remote Code Execution · CVE-2018-10115 · 06-Dec-18 · 09-Dec-18 7T Interactive Graphical SCADA RMS Reports Buffer Overflow · None · 23-Apr-13 · 02-May-13 7T Interactive Graphical SCADA System (IGSS) Directory Traversal · CVE-2011-1565 · 23-Aug-11 · 23-Aug-11 3Com Network Supervisor Directory Traversal Performance Impact: Low Severity: High Attack ID: CPAI-2005-288 Last Update: 24-November-2009 Industry References: CVE-2005-2020 Supported Products: Security Gateway: R80, R77, R76, R75 Tags: Vendor: 3Com Product: Network Supervisor Threat Year: 2005 Protection Type: Vulnerability Threat Description: The 3Com Network Supervisor is a network management application that discovers, maps, and displays network links and IP devices. I and connections for stress levels, set thresholds and various network events. The product is also capable of generating reports in vario directory traversal vulnerability exists in the 3Com Network Supervisor product. The flaw is caused by insufficient sanitization of HTTP vulnerability allows an unauthorized user to read arbitrary files on the target host. The target will not exhibit any unusual behaviour as attack. A successful attack will result in potentially sensitive information being disclosed to an unprivileged user. The content of arbitra the attacker in the request will be served in the HTTP response. IPS Protection: This protection will detect and block attempts to exploit this vulnerability Attack Detection: Attack Name: Application Servers Protection Violation Attack Information: 3Com Network Supervisor directory traversal Additional Tags: Product Prevalence: Common, Protection Tuning: Non-Configurable, Threat Prevalence: Obsolete, CVSS: 5.0, Protected Asset: SERVER
6	Publish the SmartConsole session.
7	Install the Threat Prevention Policy on the applicable Security Gateway or Security Cluster.

To override the profile settings for a specific SNORT protection, see Action on SNORT Protection Rules, see *"Action on SNORT Protection Rules" on page 149*.

Deleting SNORT Protection Rules from the Security Management Server

To delete SNORT protection rules from the Security Management Server

Step	Instructions
1	Connect with SmartConsole to the Security Management Server that manages the applicable Security Gateway or Security Cluster.

Step	Instructions
2	From the left navigation panel, go to **Security Policies** > **Threat Prevention** > **Custom Policy**.
3	In the bottom section **Custom Policy Tools**, go to **IPS Protections**.
4	From the top toolbar, click **Actions** > **Snort protections** > **Delete all snort protections**. 
5	Publish the SmartConsole session.
6	Install the Threat Prevention Policy on the applicable Security Gateway or Security Cluster.

Protection	Industry R			Performance Im...	Sever
3Com Network Supervisor Directory Traversal	CVE-2005-2				
3Com TFTP Server Transporting Mode Remote Buffer Overflow	CVE-2006-6				
3CX Phone System VAD_Deploy.aspx Arbitrary File Upload	None				
3ivx MPEG-4 MP4 File Handling Stack Overflow	CVE-2007-6				
3ivx MPEG-4 MP4 File Handling Stack Overflow - Specific	CVE-2007-6401	01-Oct-09	11-Feb-13		
3S Smart Software Solutions CoDeSys Gateway Server Denial Of Service	CVE-2012-4707	19-May-13	22-May-13		
3S Smart Software Solutions CoDeSys Gateway Server Directory Traversal	CVE-2012-4705	05-May-13	06-Oct-15		
3S Smart Software Solutions CoDeSys Gateway Server Heap Buffer Overflow	CVE-2012-4706	05-May-13	07-May-13		
3S Smart Software Solutions CoDeSys Gateway Server Memory Access Error	CVE-2012-4704	05-May-13	07-May-13		
3S Smart Software Solutions CoDeSys Gateway Server Stack Buffer Overflow	CVE-2012-4708	05-May-13	06-Oct-15		
7-Zip ARJ Archive Handling Buffer Overflow	CVE-2005-3051	12-Oct-09	12-Oct-09		
7-Zip RAR Solid Compression Remote Code Execution	CVE-2018-10115	06-Dec-18	09-Dec-18		
7T Interactive Graphical SCADA RMS Reports Buffer Overflow	None	23-Apr-13	02-May-13		
7T Interactive Graphical SCADA System (IGSS) Directory Traversal	CVE-2011-1565	23-Aug-11	23-Aug-11		

3Com Network Supervisor Directory Traversal

Performance Impact: Low

Severity: High

Con

Attack ID: CPAI-2005-288

Last Update: 24-November-2009

Industry References: CVE-2005-2020

Supported Products: Security Gateway: R80, R77, R76, R75

Tags:

Vendor: 3Com

Product: Network Supervisor

Threat Year: 2005

Protection Type: Vulnerability

Threat Description:
The 3Com Network Supervisor is a network management application that discovers, maps, and displays network links and IP devices. I and connections for stress levels, set thresholds and various network events. The product is also capable of generating reports in vario directory traversal vulnerability exists in the 3Com Network Supervisor product. The flaw is caused by insufficient sanitization of HTTP vulnerability allows an unauthorized user to read arbitrary files on the target host. The target will not exhibit any unusual behaviour as attack. A successful attack will result in potentially sensitive information being disclosed to an unprivileged user. The content of arbitra the attacker in the request will be served in the HTTP response.

IPS Protection:
This protection will detect and block attempts to exploit this vulnerability

Attack Detection:
Attack Name: Application Servers Protection Violation
Attack Information: 3Com Network Supervisor directory traversal

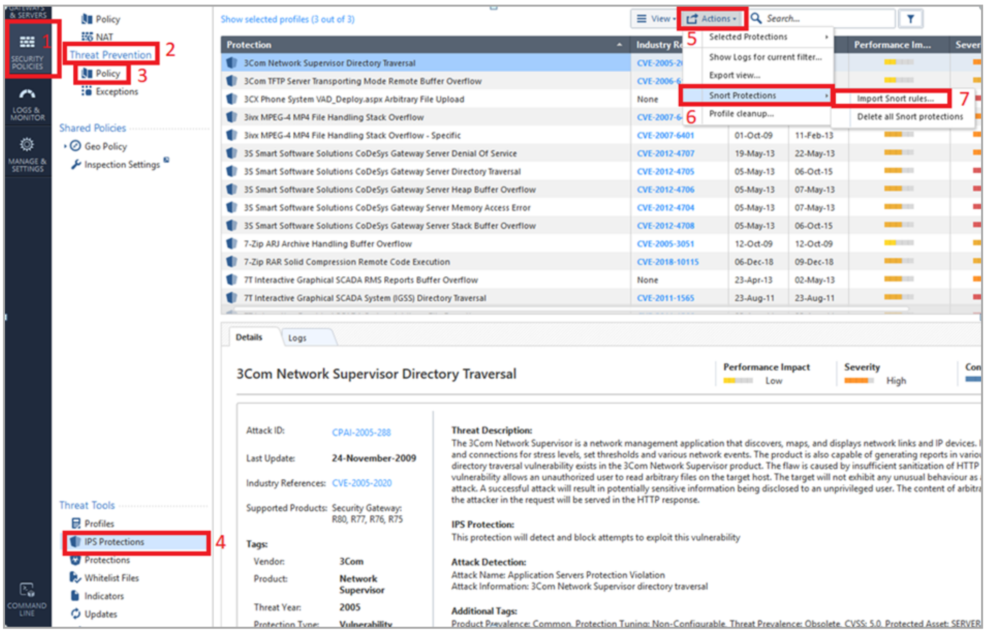
Additional Tags:
Product Prevalence: Common, Protection Tuning: Non-Configurable, Threat Prevalence: Obsolete, CVSS: 5.0, Protected Asset: SERVER

Importing SNORT Protection Rules to the Multi-Domain Server

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

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

To import SNORT rules to the Multi-Domain Server

Step	Instructions
1	Connect with SmartConsole to the Multi-Domain Server to the **MDS** context.
2	From the left navigation panel, click **Multi-Domain** > **Domains**.
3	Right-click on the **Global Domain** and select **Connect to domain**.
4	From the left navigation panel, click **Security Policies**.
5	Open the applicable global policy.
6	In the top section, go to **Threat Prevention** > **Custom Policy**.
7	In the bottom section **Custom Policy Tools**, click **IPS Protections**.  SECURITY POLICIES 1 Threat Prevention 2 Policy 3 Exceptions Shared Policies Geo Policy Inspection Settings Threat Tools Profiles IPS Protections 4 Protections Whitelist Files Indicators Updates View Actions 5 Search... Selected Protections Show Logs for current filter... Export view... Snort Protections 6 Profile cleanup... Import Snort rules... 7 Delete all Snort protections Details Logs
8	From the top toolbar, click **Actions** > **Snort Protections** > **Import Snort rules**.
9	Select the required file with the SNORT rules and click **Open**. The tool converts the rules to Check Point syntax and updates the protections database. **Important** - SmartConsole shows the converted SNORT rules as IPS protections whose names start with "**Snort imported**".
10	Publish the SmartConsole session.
11	Close the SmartConsole connected to the Global Domain.

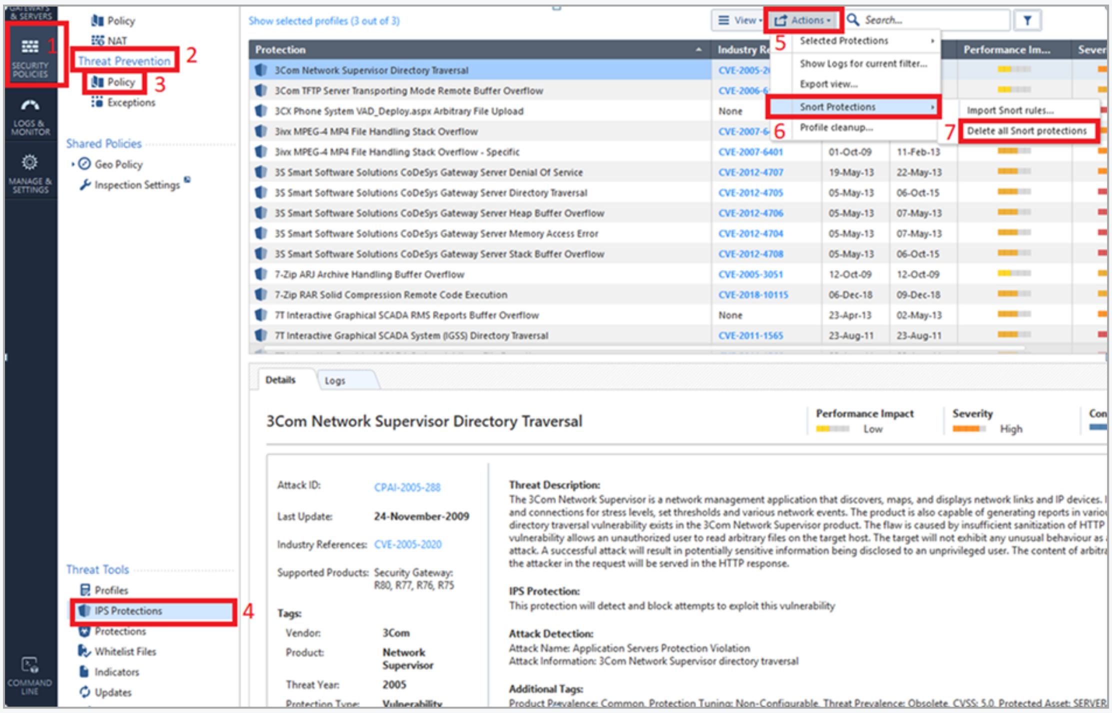
Step	Instructions
12	From the left navigation panel, click **Multi Domain** > **Global Assignments**.
13	Reassign the Global Policy to the Local Domains.
14	Connect with SmartConsole to the applicable Domain Management Server that manages the applicable Security Gateway or Security Cluster.
15	Install the Threat Prevention Policy on the applicable Security Gateway or Security Cluster.

To override the profile settings for a specific SNORT protection, see *"Action on SNORT Protection Rules" on the next page*).

Deleting SNORT Protection Rules from the Multi-Domain Server

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

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

Step	Instructions
8	From the top toolbar, click **Actions** > **Snort Protections** > **Delete all Snort protections**. 
9	Publish the session.
10	Close the SmartConsole connected to the Global Domain.
11	From the left navigation panel, click **Multi Domain** > **Global Assignments**.
12	Reassign the Global Policy to the Local Domains.
13	Connect with SmartConsole to the applicable Multi-Domain Server that manages the applicable Security Gateway or Security Cluster.
14	Install theThreat Prevention Policy on the applicable Security Gateway or Security Cluster.

Protection	Industry Re			Performance Im...	Sever
3Com Network Supervisor Directory Traversal	CVE-2005-2				
3Com TFTP Server Transporting Mode Remote Buffer Overflow	CVE-2006-6				
3CX Phone System VAD_Deploy.aspx Arbitrary File Upload	None				
3ivx MPEG-4 MP4 File Handling Stack Overflow	CVE-2007-6				
3ivx MPEG-4 MP4 File Handling Stack Overflow - Specific	CVE-2007-6401	01-Oct-09	11-Feb-13		
3S Smart Software Solutions CoDeSys Gateway Server Denial Of Service	CVE-2012-4707	19-May-13	22-May-13		
3S Smart Software Solutions CoDeSys Gateway Server Directory Traversal	CVE-2012-4705	05-May-13	06-Oct-15		
3S Smart Software Solutions CoDeSys Gateway Server Heap Buffer Overflow	CVE-2012-4706	05-May-13	07-May-13		
3S Smart Software Solutions CoDeSys Gateway Server Memory Access Error	CVE-2012-4704	05-May-13	07-May-13		
3S Smart Software Solutions CoDeSys Gateway Server Stack Buffer Overflow	CVE-2012-4708	05-May-13	06-Oct-15		
7-Zip ARJ Archive Handling Buffer Overflow	CVE-2005-3051	12-Oct-09	12-Oct-09		
7-Zip RAR Solid Compression Remote Code Execution	CVE-2018-10115	06-Dec-18	09-Dec-18		
7T Interactive Graphical SCADA RMS Reports Buffer Overflow	None	23-Apr-13	02-May-13		
7T Interactive Graphical SCADA System (IGSS) Directory Traversal	CVE-2011-1565	23-Aug-11	23-Aug-11		

3Com Network Supervisor Directory Traversal

Performance Impact Low

Severity High

Con

Attack ID: CPAI-2005-288

Last Update: 24-November-2009

Industry References: CVE-2005-2020

Supported Products: Security Gateway: R80, R77, R76, R75

Tags:

Vendor: 3Com

Product: Network Supervisor

Threat Year: 2005

Protection Type: Vulnerability

Threat Description:
The 3Com Network Supervisor is a network management application that discovers, maps, and displays network links and IP devices. I
and connections for stress levels, set thresholds and various network events. The product is also capable of generating reports in variou
directory traversal vulnerability exists in the 3Com Network Supervisor product. The flaw is caused by insufficient sanitization of HTTP
vulnerability allows an unauthorized user to read arbitrary files on the target host. The target will not exhibit any unusual behaviour as a
attack. A successful attack will result in potentially sensitive information being disclosed to an unprivileged user. The content of arbitra
the attacker in the request will be served in the HTTP response.

IPS Protection:
This protection will detect and block attempts to exploit this vulnerability

Attack Detection:
Attack Name: Application Servers Protection Violation
Attack Information: 3Com Network Supervisor directory traversal

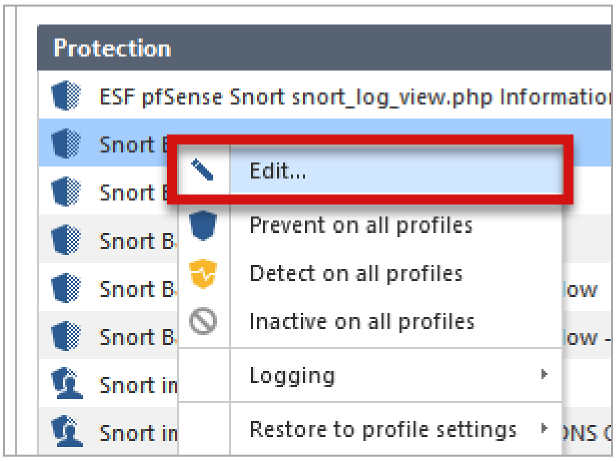
Additional Tags:
Product Prevalence: Common, Protection Tuning: Non-Configurable, Threat Prevalence: Obsolete, CVSS: 5.0, Protected Asset: SERVER

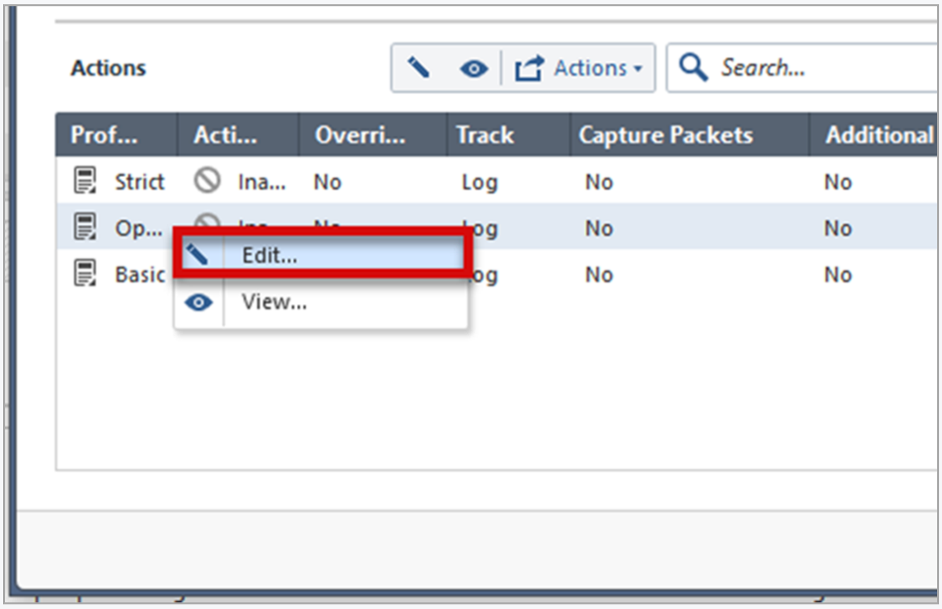
Action on SNORT Protection Rules

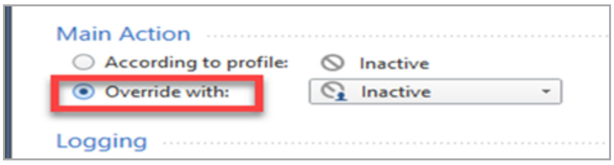
The Security Gateway enforces SNORT protection rules based on the profile which is installed on the Security Gateway. For example, if the profile installed on the Security Gateway is **Optimized**, by default the Security Gateway does not enforce SNORT protection rules, because their performance impact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

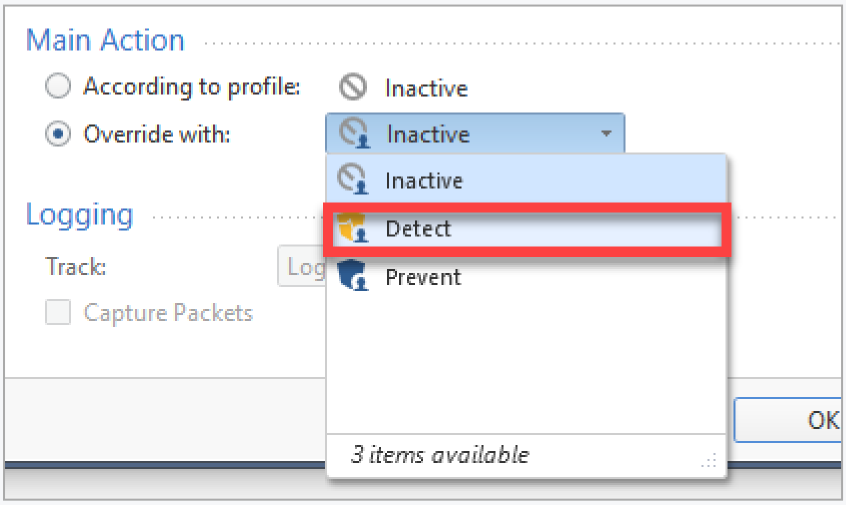
To override the profile settings for a specific SNORT protection

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

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>1</td><td>In <b>IPS Protections</b>, right-click a SNORT protection and select <b>Edit</b>.
<b>Note</b> - The SNORT protection names start with "<b>Snort imported</b>".

Protection
ESF pfSense Snort snort_log_view.php Informatio
Snort E
Snort E
Snort B
Snort B
Snort B
Snort in
Snort in
low
low -
DNS (
Edit...
Prevent on all profiles
Detect on all profiles
Inactive on all profiles
Logging
Restore to profile settings

</td></tr>
<tr><td>2</td><td>Right-click the profile and select <b>Edit</b>.


<table>
<tr><th>Prof...</th><th>Acti...</th><th>Overri...</th><th>Track</th><th>Capture Packets</th><th>Additional</th></tr>
<tr><td>Strict</td><td>Ina...</td><td>No</td><td>Log</td><td>No</td><td>No</td></tr>
<tr><td>Op...</td><td>Ina...</td><td>No</td><td>Log</td><td>No</td><td>No</td></tr>
<tr><td>Basic</td><td></td><td></td><td>Log</td><td>No</td><td>No</td></tr>
</table></td></tr>
<tr><td>3</td><td>In the <b>Main Action</b> area, select <b>Override with</b>.

Main Action
○ According to profile: Inactive
● Override with: Inactive
Logging</td></tr>
</table>

Step	Instructions
4	From the drop-down menu, select the required action. 
5	Click **OK**.
6	Click **Close**.
7	Publish the SmartConsole session.
8	Install the Threat Prevention Policy.

Main Action

○ According to profile: Inactive

● Override with: Inactive

Alternative Methods to add and delete SNORT Protection Rules

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

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

Adding SNORT Rules

The applicable command accepts two arguments:

- package-format" which always takes the string value "snort"
- "package-path" which is the path to the protections' package

The command returns:

Upon success:	0

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

Examples

- From the `mgmt_cli` tool, run this command

  ```
  mgmt_cli add threat-protections package-path
  "/path/to/community.rules" package-format "snort" --version
  1.2 --format json
  ```

- From the SmartConsole CLI, run this command

  ```
  add threat-protections package-path
  "/path/to/community.rules" package-format "snort" --version
  1.2 --format json
  ```

- From the Gaia Clish, run this command

  ```
  mgmt add threat-protections package-path
  "/path/to/community.rules" package-format "snort" --version
  1.2 --format json
  ```

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

- POST Request Method

  A post request must:

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

The server returns:

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

Example

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

Deleting SNORT Protections

The applicable command accepts one argument "package-format", which always takes the string value "snort".

The command returns:

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

Examples

- From the `mgmt_cli` tool, run this command

  ```
  mgmt_cli delete threat-protections package-format "snort" --
  version 1.2
  ```

- From the SmartConsole CLI, run this command

  ```
  delete threat-protections package-format "snort" --version
  1.2
  ```

- From the Gaia Clish, run this command

  ```
  mgmt delete threat-protections package-format "snort" --
  version 1.2
  ```

- POST Request method

  A POST Request must be send to this URL:

  ```
  https://<IP-address-of-mgmt-server>:<port>/web_
  api/v1.2/delete-threat-protections
  ```

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

The server returns:

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

Example

```
Content-Type: application/json
X-chkp-sid: {{session}}
{
  "package-format" : "snort"
}
```

Creating SNORT Rule Files

You can write your own SNORT rules and then import them to a Check Point Management Server to become IPS protections.

For more information about SNORT, see snort.org.

Check Point supports SNORT 2.9 version and lower.

SNORT rules use signatures to define attacks. A SNORT rule has a rule header and rule options.

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

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

SNORT Rule Syntax

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

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

- SNORT Rule Header:

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

- SNORT Rule Options:

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

Example:

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

Where:

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

Supported SNORT Syntax

These are the generally supported syntax components. There are some limitations (see *"Unsupported SNORT Syntax" on page 157*).

Syntax components

Keyword	Description
`length`	Specifies the original length of the content that is specified in a protected_content rule digest
`pcre`	Lets you write rules with Perl-compatible regular expressions. Example: `alert tcp any any -> any 80 (content:"/foo.php?id="; pcre:"/\/foo.php?id=[0-9]{1,10}/iU";)`

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

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

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

Debugging:

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

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

Unsupported SNORT Syntax

This syntax is not supported and will not convert

- PCRE modifiers: 'G', 'O', 'A'
- PCRE regular expression with lookahead assertion: ?!
- Using byte_test keyword with operator not in: <, >, =, &, ^
- http_method is not supported if it is the only http modifier type in the SNORT Rule
- Protocols: icmp, ip ("all" is interpreted as UDP and TCP protocols)
- SNORT Rule without content keyword
- All PORT macros, except HTTP_PORTS
- Specification of source port (only "any" is supported)
- Specification of destination port "any" (you must specify an exact destination port number, or a range of destination port numbers).

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

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

These combinations of keywords and modifiers are implemented differently in the IPS blade as SNORT protection rules than in SNORT Rules.

Best Practice - Test them before activating them in a production environment.

Keywords and modifiers

- `rawbytes` content
- "`B`" PCRE modifiers with `http_uri` content
- "`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 ^ (carret) 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.

SSL Services

In addition to the conventional metadata service options, Check Point supports additional keywords specifically for SSL traffic.

SNORT rules for SSL traffic can be defined using the metadata keyword.

In the **Snort rule** options add:

```
metadata: service <ssl service>;
```

Example

```
alert tcp any any -> any 443 (msg:"Fake SSL Certificate";
content:"|08 e4 98 72 49 bc 45 07 48 a4 a7 81 33 cb f0 41 a3 51 00
33|"; metadata: service sslHello;)
```

Options for <ssl service>

Service	Description
`sslHello`	The sslHello service will search the Client Hello or Sever Hello depending on the flow.
`sslCertificate`	The sslCertificate service will search the Client Certificate or Sever Certificate depending on the flow.
`sslKeyx`	The sslKeyx service will search the Client Key Exchange or Sever Key Exchange depending on the flow.
`sslHeartbeat`	The sslHeartbeat will search the SSL heartbeats.
`sslCiphersuite`	The sslCiphersuite will search the Cipher Suite sent by the client.

When you use the `sslHello`, `sslCertificate`, or `sslKeyx` services, it is necessary to define a flow direction as either "`flow: to_server`" or "`flow: from_server`".

Note - These services and content modifiers are unique to Check Point and will not be supported by other SNORT engines.

Optimizing IPS - Custom Threat Prevention

IPS is a robust solution which protects your network from threats. Implementation of the recommendations in this chapter helps maintaining 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.

Troubleshooting IPS on a Security Gateway

You can temporarily stop protections on a Security Gateway set to Prevent from blocking traffic. This is useful when troubleshooting an issue with network traffic.

In the **Activation Mode** section, click **Detect only**.

All protections set to Detect only allow traffic to pass, but continue to track threats according to the Track setting.

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

Step	Instructions
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 the Threat Prevention Policy.

Tuning Protections

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.

Using the Allow List

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

To add a file to the Allow List

Step	Instructions
1	Select **Threat Prevention** > **Custom Policy Tools** > **Allow List Files**. The **Allow List Files** page opens.
2	Click **New**. The **New File Exception** window opens.
3	Enter parameters for the new file exception: ■ **Name** ■ **Comment** (optional) ■ **MD5** signature ■ Select a color (optional) - the default is black
4	Click **OK**.

To edit attribute of a file from the Allow List

Step	Instructions
1	Select **Threat Prevention** > **Custom Policy Tools** > **Allow List Files**. The **Allow List Files** page opens.
2	Select a file.
3	Click **Edit**.
4	In the file properties window that opens, make necessary changes.
	Click **OK**.

To remove a file from the Allow List

Step	Instructions
1	Select **Threat Prevention** > **Custom Policy Tools** > **Allow List Files**. The **Allow List Files** page opens.

Step	Instructions
2	Select a file or multiple files.
3	Click **Delete**.

Configuring Threat Prevention Settings on VSX Gateways

This section contains the instructions to enable Threat Prevention Software Blades on VSX Virtual Systems.

For more information, see sk106496 and sk79700.

To enable Anti-Bot, Anti-Virus, or IPS on Virtual Systems

Important:

- Make sure the routing, DNS, and proxy settings for the VSX Gateway or VSX Cluster Members (VS0) are configured correctly.
- You must enable and configure the Software Blades in these objects:
  - VSX Gateway or VSX Cluster (because VS0 handles contract validation for all Virtual Systems).
  - Applicable Virtual Systems.
- Make sure the VSX Gateway or VSX Cluster and the applicable Virtual Systems can connect to the Internet.
  Virtual Systems get updates through the VSX Gateway or VSX Cluster (VS0).
  If the VSX Gateway or VSX Cluster fails to connect, each Virtual System uses its proxy settings to get the updates from the Internet.

Step	Instructions
1	If applicable, configure proxy settings for the VSX Gateway or VSX Cluster (VS0) or the Virtual Systems (or both) in SmartConsole: a. From the left navigation panel, click **Gateways & Servers**. b. Double-click the VSX Gateway or VSX Cluster object (or the applicable Virtual System object). c. From the navigation tree, click **Topology** > **Proxy**. d. Configure the proxy settings. e. Click **OK**

Step	Instructions
2	Enable the Software Blade on the VSX Gateway or VSX Cluster (VS0): 1. Double-click the applicable VSX Gateway or VSX Cluster object. 2. From the navigation tree, click **General Properties**. 3. On the **Threat Prevention** tab, select any or all of these Software Blades: ■ Anti-Bot ■ Anti-Virus ■ IPS When you enable these Software Blades, the **First Time Activation** window opens. You must select: ■ **According to the policy** ■ **Detect only** 4. From the navigation tree, click and configure the Software Blades you enabled. 5. Click **OK**.
3	Enable the Software Blade on the applicable Virtual Systems: 1. Expand the VSX Gateway or VSX Cluster object and double-click the applicable Virtual System object. 2. From the navigation tree, click **General Properties**. 3. On the **Threat Prevention** tab, select any or all of these Software Blades (the same you selected in the VSX Gateway or VSX Cluster object): ■ Anti-Bot ■ Anti-Virus ■ IPS When you enable these Software Blades, the **First Time Activation** window opens. You must select: ■ **According to the policy** ■ **Detect only** 4. From the navigation tree, click and configure the Software Blades you enabled. 5. Click **OK**.
4	Configure the Threat Prevention policies for: ■ The VSX Gateway or VSX Cluster (VS0). ■ The applicable Virtual Systems.
5	Install the default VSX policy on the VSX Gateway or VSX Cluster. This policy is called: `<Name of VSX Gateway or VSX Cluster Object>_VSX`

Step	Instructions
6	Install the Threat Prevention policy: - On the VSX Gateway or VSX Cluster (VS0). - On the applicable Virtual Systems (and Access Control Policy, if needed).

To enable Threat Emulation on Virtual Systems

Important:

- Make sure the routing, DNS, and proxy settings for the VSX Gateway or VSX Cluster Members (VS0) are configured correctly.
- Do **not** enable the Threat Emulation Software Blade in the VSX Gateway or VSX Cluster object, because it does not participate in the Threat Emulation process.

Step	Instructions
1	If applicable, configure proxy settings for the VSX Gateway or VSX Cluster (VS0), or the Virtual Systems (or both) in SmartConsole: a. From the left navigation panel, click **Gateways & Servers**. b. Double-click the VSX Gateway or VSX Cluster object (or the applicable Virtual System object). c. From the navigation tree, click **Topology** > **Proxy**. d. Configure the proxy settings. e. Click **OK**
2	Enable **Threat Emulation** on the applicable Virtual Systems: a. Expand the VSX Gateway or VSX Cluster object and double-click the applicable Virtual System object. b. From the navigation tree, click **General Properties**. c. On the **Custom Threat Prevention** tab, select **SandBlast Threat Emulation**. The **Threat Emulation First Time Activation Wizard** opens. d. Configure the **Emulation Location** and click **Next**. e. Configure the settings on the **Activate Threat Extraction** page and click **Next**. f. In the **Summary** window, click **Finish**. g. From the navigation tree, click and configure the Software Blades you enabled. h. Click **OK**.

Step	Instructions
3	Configure the Threat Prevention policies for the applicable Virtual Systems.
4	Install the Threat Prevention policy on the applicable Virtual Systems (and Access Control Policy, if needed).

To enable Threat Extraction on Virtual Systems

Important:

- Make sure the routing, DNS, and proxy settings for the VSX Gateway or VSX Cluster Members (VS0) are configured correctly.
- Enable the Threat Extraction Software Blade in the VSX Gateway or VSX Cluster object.

Step	Instructions
1	If applicable, configure proxy settings for the VSX Gateway or VSX Cluster (VS0) or the Virtual Systems (or both) in SmartConsole: 1. From the left navigation panel, click **Gateways & Servers**. 2. Double-click the VSX Gateway or VSX Cluster object (or the applicable Virtual System object). 3. From the navigation tree, click **Topology** > **Proxy**. 4. Configure the proxy settings. 5. Click **OK**
2	Enable **Threat Extraction** on the applicable Virtual Systems: 1. Expand the VSX Gateway or VSX Cluster object and double-click the applicable Virtual System object. 2. From the navigation tree, click **General Properties**. 3. On the **Threat Prevention** tab, select **SandBlast Threat Extraction**. 4. Click **OK**.
3	Optional: When you enable Threat Extraction, support for web traffic over the HTTP and HTTPS protocol is enabled automatically. For Threat Extraction to scan e-mail attachments as well, configure the Security Gateway as a Mail Transfer Agent (MTA) (see *"Configuring the Security Gateway as a Mail Transfer Agent" on page 170*.
4	Configure the Threat Prevention policies for: - The VSX Gateway or VSX Cluster (VS0). - The applicable Virtual Systems.

Step	Instructions
5	Install the default VSX policy on the VSX Gateway or VSX Cluster. This policy is called: `<Name of VSX Gateway or VSX Cluster Object>_VSX`
6	Install the Threat Prevention policy: ■ On the VSX Gateway or VSX Cluster (VS0). ■ On the applicable Virtual Systems (and Access Control Policy, if needed).

Configuring the Security Gateway as a Mail Transfer Agent

You can configure the Security Gateway / Cluster as a Mail Transfer Agent (MTA) to manage SMTP traffic.

When a Security Gateway scans SMTP traffic, sometimes the email client is not able to keep the connection open for the time that is necessary to handle the email. In such cases, there is a timeout for the email.

MTA prevents this problem. The MTA first accepts the email from the previous hop, does the necessary actions on the email, and then relays the email to the next hop.

The MTA scans SMTP/TLS encrypted traffic for the supported Software Blades.

Notes:

- MTA is not supported in Autonomous Threat Prevention. To use MTA, enable **Custom Threat Prevention** in the Security Gateway / Cluster object.
- MTA is supported on VSX Gateways / VSX Clusters. The MTA configuration is the same for non-VSX Gateways / non-VSX Clusters.
- You can configure MTA to only scan the emails and not forward them to the mail server (see *"Deploying MTA in Backward Compatibility Mode" on page 177*).

Enabling Mail Transfer Agent

Procedure

Step	Instructions
1	Connect with SmartConsole to the Management Server. From the left navigation panel, click **Gateways & Servers**.
2	Create one of these required objects, if such object does not exist yet (later, you select this object in the applicable MTA rule as the Next Hop): ■ A **Host** object that represents the mail server. ■ A **Domain** object that represents the recipient domain. This lets you use multiple mail servers based on a DNS name. This DNS configuration allows load balancing and high-availability capabilities based on DNS configuration. This configuration requires Security Gateways R80.20 and higher. You can select only one object in each MTA rule.
3	Open the Security Gateway object.
4	From the navigation tree, click the **General Properties** page.
5	Enable the required Software Blades. Mail Transfer Agent supports these Software Blades: ■ **Threat Extraction** (appears on the **Threat Prevention (Custom)** tab). ■ **Threat Emulation** (appears on the **Threat Prevention (Custom)** tab). ■ **Anti-Spam and Mail Security** (appears on the **Network Security** tab).
6	From the navigation tree, click the **Mail Transfer Agent** page.
7	Select **Enable as a Mail Transfer Agent (MTA)**.

Step	Instructions
8	In the **Mail Forwarding** section, add one or more rules. These rules configure the email traffic that the Security Gateway sends to the mail servers after it completed the scanning. The Management Server automatically adds these MTA rules at the top of the **Threat Prevention - Custom Policy**. In these rules: ■ The **Name** column contains "`MTA traffic to Gateway <`*`Name of Object`*`>`". ■ The **Comment** column contains "`Automatic rule for MTA traffic`". Steps: 1. From the toolbar, click the applicable button to add a rule (above or below). 2. Right-click the **Domain** cell and select **Edit**. 3. Enter the domain FQDN for the SMTP traffic for this rule. You can enter the wildcard ***** to accept all recipient domains. 4. Click **OK**. 5. Click the **Next Hop** cell and select the required **Host** / **Domain** object. 6. **Optional:** Right-click the **Comment** cell and select **Edit** > enter the description for this rule and click **OK**.
9	**Optional:** Select **Add signature to scanned emails** and enter the message to add to the end of the email body after the Security Gateway scans it successfully.
10	The **SMTP/TLS** section applies if the email server uses TLS inspection: a. In **Step 1**, click **Import**. The **Import Outbound Certificate** window opens. b. Click **Browse** and select the required certificate file. c. In the **Private key password** field, enter the password you configured for this certificate. d. Click **OK**. e. In **Step 2**, select **Enable SMTP/TLS**.

Step	Instructions
11	In the **Implied Rule** section, configure the implied rule. By default, when you configure a Security Gateway as MTA, the Management Server automatically adds an implied rule at the top of the Access Control Policy. This implied rule accepts traffic on the TCP port 25 that the network sends to the Security Gateway. The default source in this implied rule is any IP address. You can configure the source in this implied rule to allow traffic only from specific IP addresses. To disable this implied rule, clear **Create an implied rule at the top of the Access Control Policy**.

Step	Instructions
12	**Optional:** In the **Advanced Settings** section, click **Configure Settings**. a. In the **Interfaces** section, configure the interfaces on which the Security Gateway accepts the SMTP traffic: ■ **All interfaces** - SMTP traffic from all the interfaces is sent for scanning. ■ **All external** - SMTP traffic from the external interfaces is sent for scanning. ■ **Use specific** - SMTP traffic from the list of specified interfaces is sent for scanning. To add an interface to the list, click the plus sign (+). To remove a selected interface from the list, click the minus sign (-). b. In the **Mail Settings** section, configure the applicable email settings: ■ **Maximum delayed time** - The maximum number of minutes that the MTA keeps emails. ■ **Maximum disk usage** - Amount of free disk space that the MTA can use of storage (in percent or total number of megabytes). ■ **If limits are exceeded or in case of an error** - Configure: What to do when the specified Mail Settings are exceeded: • **Allow** - The Security Gateway allows the SMTP traffic • **Block** - The Security Gateway blocks the SMTP traffic • **None** - The Security Gateway does not generate logs How to track it: • **None** - The Security Gateway does not generate logs • **Log** -The Security Gateway generates logs • **Alert** - The Security Gateway generates logs and sends the configured alert (see **Menu** > **Global properties** >) c. In the **Troubleshooting** section, configure these settings: ■ **When mail is delayed for more than** - Configure the maximum number of minutes that email is delayed in the MTA before the Security Gateway applies the configured track action. ■ **Track** - configure on of these: • **None** - The Security Gateway does not generate logs • **Log** -The Security Gateway generates logs • **Alert** - The Security Gateway generates logs and sends the configured alert (see **Menu** > **Global properties** >) d. Click **OK** to close the **MTA Advanced Settings** window.
13	Click **OK** to close the Security Gateway properties window.
14	Install the Access Control policy on the Security Gateway.

Step	Instructions
15	Install the Threat Prevention policy on the Security Gateway.
16	Change the network 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, change the SMTP settings or MX records first. Failure to do so can result in lost emails (see *"Disabling Mail Transfer Agent" on the next page*). **To configure an MTA for emails that are sent to the internal mail server:** a. Change the applicable DNS settings on the network servers. b. Change the MX records, and configure the Security Gateway as the next hop. **To configure an MTA for emails that are sent to a different MTA:** a. Connect to the MTA that sends email to the internal mail server. b. Change the SMTP settings and configure the Security Gateway as the next hop.

Disabling Mail Transfer Agent

Note - If the MTA queue is not empty, or if you disable the MTA first, it is possible to lose emails that are sent to the network.

1. Change the network settings to **stop** sending SMTP traffic from external networks to the Security Gateway.

   Procedure

Step	Instructions
1	Change the MX records for the network, and configure the mail server as the next hop (instead of the Security Gateway).
2	Wait for 24 hours because your servers can save the MTA address in their cache.

2. Disable the MTA in the Security Gateway object.

   Procedure

Step	Instructions
1	Connect with SmartConsole to the Management Server. From the left navigation panel, click **Gateways & Servers**.
2	Open the Security Gateway object.
3	From the navigation tree, click the **Mail Transfer Agent** page.
4	Clear **Enable as a Mail Transfer Agent (MTA)**.
5	Click **OK**.
6	Install the Threat Prevention policy.

Deploying MTA in Backward Compatibility Mode

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

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

Procedure

Step	Instructions
1	Connect with SmartConsole to the Management Server. From the left navigation panel, click **Gateways & Servers**.
2	Create a new **Host** object with these settings: ■ **Name** - Enter some name. For example: `No_Forward_MTA` ■ **IPv4 Address** - Enter `0.0.0.0`
3	Open the Security Gateway object.
4	From the navigation tree, click the **Mail Transfer Agent** page.
5	Select **Enable as a Mail Transfer Agent (MTA)**.
6	In the **Mail Forwarding** section, delete all current rules.
7	From the toolbar, click the applicable button to add a rule (above or below).
8	Right-click the **Domain** cell and select **Edit**. Enter the wildcard * to accept all recipient domains. Click **OK**.
9	Click the **Next Hop** cell and select the **Host** object you created earlier.
10	**Optional:** Right-click the **Comment** cell and select **Edit** > enter the description for this rule and click **OK**.
11	Click **OK**.
12	Install the Threat Prevention policy.

MTA Engine Updates

The Mail Transfer Agent Engine Update is an accumulation of new features and bug fixes to the MTA engine.

MTA updates are available for Security Gateways R80.20 and higher, and R80.10 with the R80.10 Jumbo Hotfix Accumulator Take 142 (and higher).

It is delivered in the form of a CPUSE package and can be installed and upgraded manually through the CPUSE .The `cpstop/cpstart` or reboot are not required.

The updates do not conflict with the regular Jumbo Hotfix Accumulators and can be installed independently.

For more information about the MTA engine updates, see sk123174.

To check the current version of Mail Transfer Agent Update, run this command in the Expert mode on the Security Gateway:

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

Monitoring MTA

There are three views for MTA monitoring in SmartView available for Security Gateways R80.20 and higher, and R80.10 with R80.10 Jumbo Hotfix Accumulator Take 142 (and higher).

Procedure

Step	Instructions
1	Connect with SmartConsole to the Management Server.
2	Make sure the required Software Blades are enabled on the Management Server / Log Server object, to which the Security Gateways send their logs: a. From the left navigation panel, click **Gateways & Servers**. b. Open the Management Server / Log Server object. c. From the navigation tree, click the **General Properties** page. d. On the **Management** tab, select: ■ Logging & Status ■ SmartEvent Server ■ SmartEvent Correlation Unit e. Click **OK**. f. Click **Menu** > click **Install database** > select the servers > click **Install**.
3	Make sure the MTA Live Monitoring is enabled in the applicable Threat Prevention profiles: a. From the left navigation panel, click **Security Policies**. b. In the top middle panel, click **Threat Prevention**. c. In the bottom middle section **Custom Policy Tools**, click **Profiles**. d. Double-click the applicable profile. e. From the navigation tree, click the **Mail** section > **General** page. f. In the **General** section, select **Enable MTA Live Monitoring**. g. Click **OK**.
4	If the option **Enable MTA Live Monitoring** was cleared and you selected it in a profile, then install the Threat Prevention Policy.

Step	Instructions
5	From this point, you can monitor MTA in SmartConsole or SmartView: a. From the left navigation panel, click **Logs & Monitor** > **Logs**. b. At the top, click **[+]** to open a new tab. c. In the top section, click **Views**. d. In the top search field, enter: **MTA** e. Double-click the applicable MTA Monitoring view (see the details below): ▪ **MTA Live Monitoring** ▪ **MTA Overview** ▪ **MTA Troubleshooting** The views are based on logs that are updated with each email status change. You can customize the views, create new widgets, and export the views to Excel/PDF. For more information, see the *R81.20 Logging and Monitoring Administration Guide*.

View "MTA Live Monitoring"

This view shows the current status of the email traffic which passed through the MTA in these timelines:

- **Emails in Queue Timeline**
- **Current Emails in Queue**

These timelines shows the distribution of the emails in queue in a graph and a table.

If you right-click the **Action** column in the table, you can do these actions on the email:

- **Retry** - Try to handle the email again.
- **Drop** - Delete the email.
- **Bypass** - Do not perform the security inspection and send the email to the next hop.

Additional widgets:

- **Current Emails in Queue**
  - **Emails In Queue**
  - **For More Than 1 Minute**
  - **For More Than 3 Minutes**
  - **Earliest Email in Queue Arrived**
- **Emails Delivered**
  - **Emails Delivered**
- **Email Status**
  - **Bounced** - The MTA sent the Emails back to the sender.
  - **Deferred** - A temporary failure occurred. The MTA will retry to perform the applicable action again.
  - **Dropped** - The MTA did not transfer the emails to the next hop.
  - **Skipped** - The MTA bypassed the emails. No performance was performed.

When you click a column in the diagram, a window opens with a list of the logs that the column is based on.

View "MTA Overview"

This view shows statistical data on the email traffic which passed through the MTA in these timelines:

- **Emails by Status Timeline**
- **Email Content Timeline**
- **Emails in Queue Timeline**

You can use compare these timelines to identify trends in email traffic and analyze the root cause for all kinds of situations.

For example, if the emails in queue timeline shows many emails in the queue at a certain point in time, you can look at the other timelines to check the possible reasons for this.

If the content timeline shows many emails with links and attachments at the same point in time, this could explain it, because they take longer to scan.

Additional widgets:

- **Emails Additional Information**
  - **Emails Delivered**
  - **Unique Email Senders**
  - **Unique Email Recipients**
- **Emails Content**
  - **Emails With Links**
  - **Emails With Attachments**

View "MTA Troubleshooting"

This view shows the causes of failure and the number of failures for each cause:

- **Failures Timeline**
- **Most Common Failures**

  This timeline shows the X top failures. The default is 5.
- **Email Failures**

  This timeline shows all failures.

ICAP

Note - If you are in autonomous Threat Prevention - the option to enable ICAP does not appear. To be able to use ICAP, you must switch to Custom Threat Prevention

The **Internet Content Adaptation Protocol (ICAP)** is a lightweight HTTP-like protocol (request and response protocol), which is used to extend transparent proxy servers. This frees up resources and standardizes the way in which new features are implemented. ICAP is usually used to implement virus scanning and content filters in transparent HTTP proxy caches.

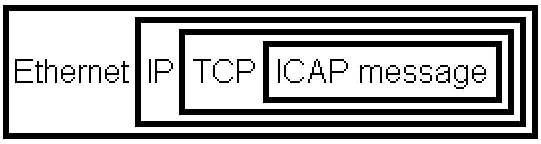
The ICAP allows ICAP Clients to pass HTTP / HTTPS messages to ICAP Servers for content adaptation. The ICAP Server executes its transformation service on these HTTP / HTTPS messages and sends responses to the ICAP Client, usually with modified HTTP / HTTPS messages. The adapted HTTP / HTTPS messages can be HTTP / HTTPS requests, or HTTP / HTTPS responses.

ICAP is a request and response protocol that is equivalent in semantics and usage to HTTP/1.1 protocol. Despite the similarity, ICAP is neither HTTP / HTTPS , nor an application protocol that runs over HTTP / HTTPS.

ICAP is an RFC protocol, which lets devices from different vendors communicate. ICAP is specified in RFC 3507 (for more information, see (*ICAP Specification*). In addition, see the Draft RFC - ICAP Extensions.

ICAP packet structure

The ICAP message is encapsulated into the TCP.



ICAP methods

Method	Description
REQMOD	Client Request Modification. The ICAP Client uses this method for an HTTP / HTTPS request modification.
RESPMOD	Server Response Modification. The ICAP Client uses this method for an HTTP / HTTPS response modification.
OPTIONS	The ICAP Client uses this method to retrieve configuration information from the ICAP Server.

ICAP response codes

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

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

You can configure Check Point Security Gateway as:

- ICAP Client - To send the HTTP / HTTPS messages to ICAP Servers for content adaptation.

  See *"Security Gateway as ICAP Client" on page 186*.

- ICAP Server - To perform content adaptation in the HTTP / HTTPS messages received from ICAP Clients.

  See *"The Security Gateway as an ICAP Server" on page 235*.

- Both ICAP Client and ICAP Server at the same time.

Check Point Security Gateway configured for ICAP can work with third party ICAP devices without changing the network topology.

Security Gateway as ICAP Client

In This Section:

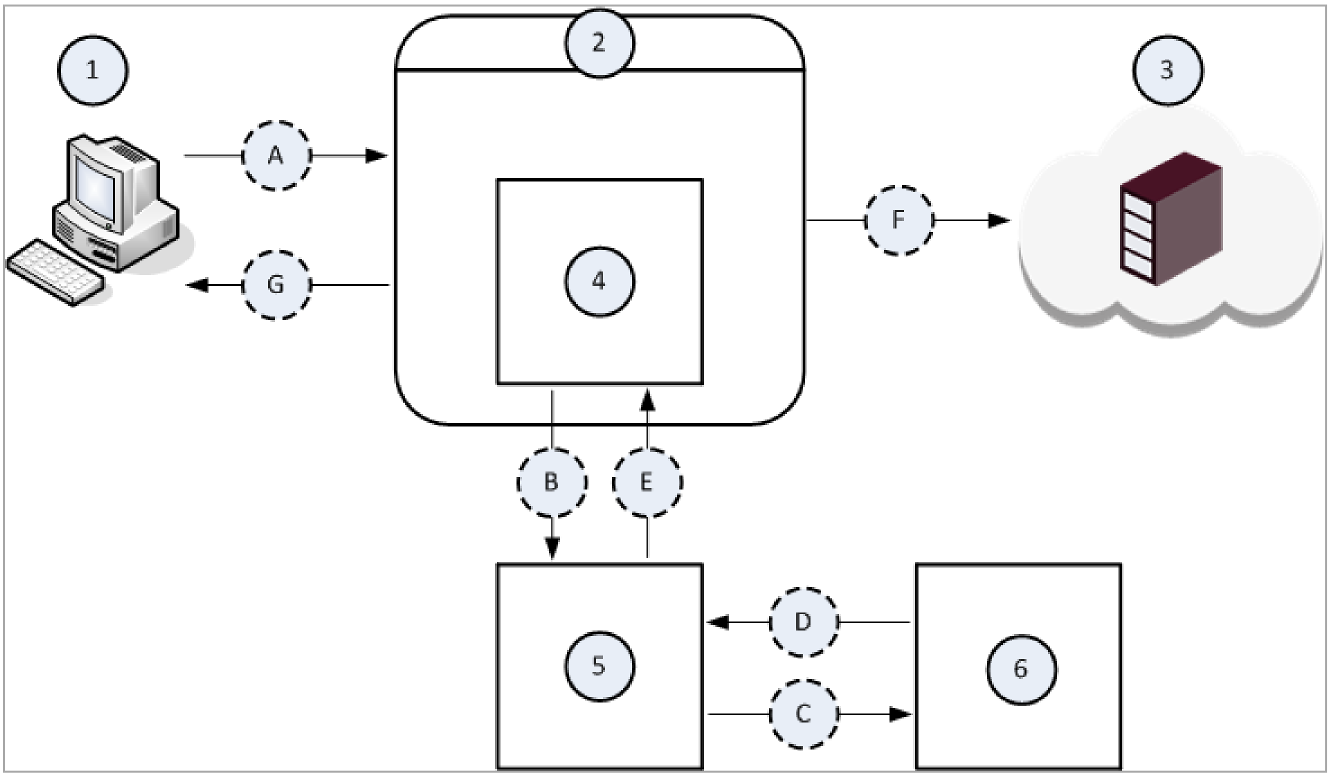
Use Cases

- A content provider provides a popular web page with a different advertisement each time the page is viewed.
- Translation of web pages to different formats that are applicable for special physical devices (PDA-based or cell-phone-based browsers).
- Firewalls send outgoing HTTP / HTTPS requests to a service that makes sure the URI in the HTTP / HTTPS request is allowed. In this case, it is an HTTP / HTTPS request that is being adapted, not an object returned by an HTTP / HTTPS response.
- Users download an executable program through a caching proxy. This proxy acts as an ICAP client and asks an external server to check the executable for viruses before accepting it into its cache.

ICAP Decisions

ICAP Decision	Description and Example
Block	■ ICAP Server sends an error to the ICAP Client. ■ ICAP Server sends a block page to the ICAP Client. For example, you can present a Check Point UserCheck page from the Threat Emulation, Anti-Virus, or URL Filtering Software Blades.
Data Modification	Modification of the HTTP content. For example, your Data Loss Prevention engine can replace the DOCX file attached to an email with a PDF file.
Continue / Not modified	Default Gateway or Proxy server can forward the HTTP Request / Response to its original destination.

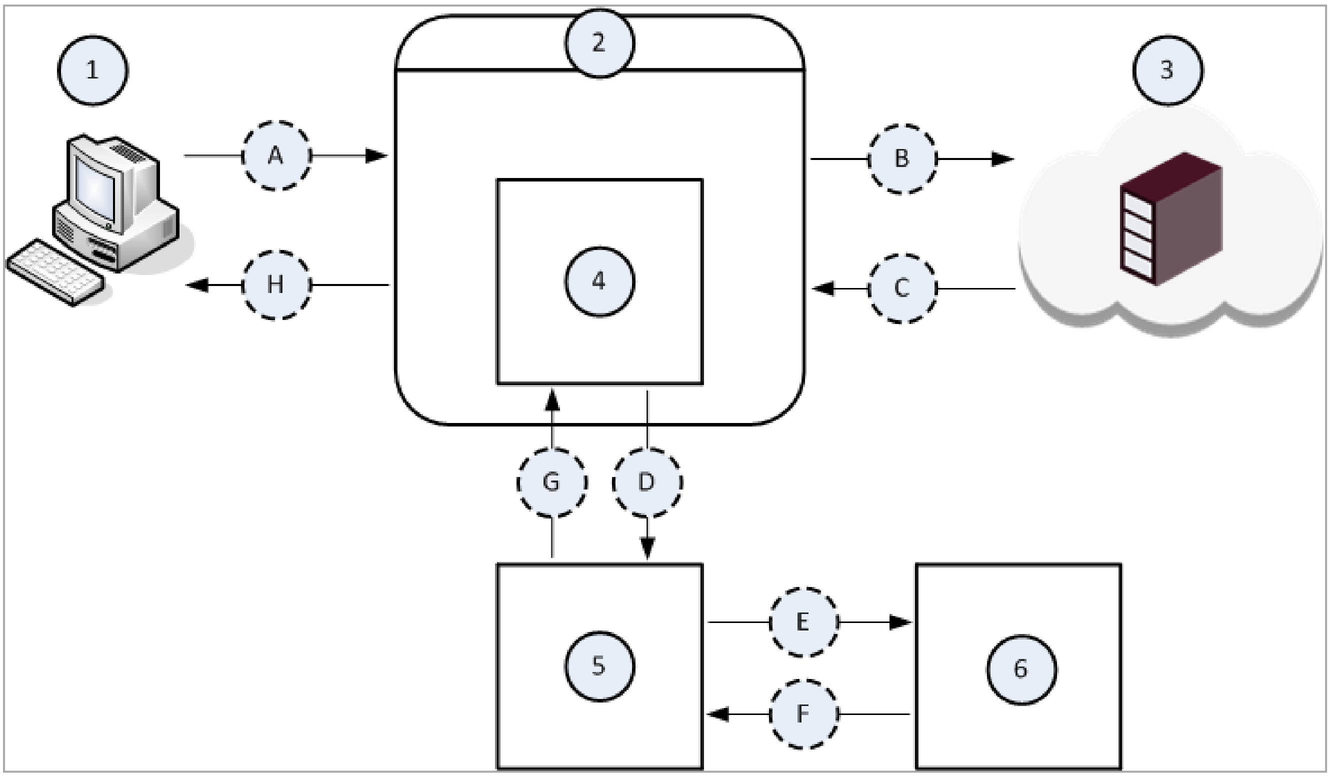
Example Data Flow in the Request Modification (REQMOD) Mode



Item	Description
1	The Client computer.
2	The Proxy server.
3	The Server computer on the Internet.
4	The ICAP Client component that runs on the Proxy server **(2)**.
5	The ICAP Server component that runs on some computer on the network.
6	The Data Loss Prevention component that runs on some computer on the network.
A	The Client computer **(1)** initiates a file upload to the Server computer **(3)**.
B	The ICAP Client component (4) intercepts the uploaded file and sends it to the ICAP Server component **(5)**.
C	The ICAP Server component **(5)** forwards the uploaded file to the Data Loss Prevention component **(6)** for examination, whether the DLP policy allows this file to leave your network.

Item	Description
D	The Data Loss Prevention component **(6)** returns its verdict about the uploaded file.
E	The ICAP Server component **(5)** returns one of these to the ICAP Client component **(4)**: ▪ A block message. ▪ The modified file.
F	The ICAP Client component **(4)** forwards the modified file from the ICAP Server component **(5)** to the Server computer **(3)**.
G	The ICAP Client component **(4)** forwards the block message from the ICAP Server component **(5)** to the Client computer **(1)**.

Example Data Flow in Server Response Modification (RESPMOD) Mode



Item	Description
1	The Client computer.
2	The Proxy server.
3	The Server computer on the Internet.
4	The ICAP Client component that runs on the Proxy server **(2)**.
5	The ICAP Server component that runs on some computer on the network.
6	The Threat Emulation component that runs on some computer on the network.
A	The Client computer **(1)** initiates a file download from the Server computer **(3)**.
B	The Proxy server **(2)** forwards the file download request to the Server computer **(3)**.
C	The Server **(3)** sends the requested file.
D	The ICAP Client component **(4)** intercepts the downloaded file and sends it to the ICAP Server component **(5)**.

Item	Description
E	The ICAP Server component **(5)** forwards the downloaded file to the Threat Emulation component **(6)** for examination, whether this file is malicious.
F	The Threat Emulation component **(6)** returns its verdict about the downloaded file.
G	The ICAP Server component **(5)** returns one of these to the ICAP Client component **(4)**: ■ A block message. ■ The modified file.
H	The ICAP Client component **(4)** forwards one of these responses from the ICAP Server component **(5)** to the Client computer **(1)**: ■ A block message. ■ The modified file.

Limitations

ICAP Client does not support ClusterXL Load Sharing mode.

ICAP Client Functionality

The ICAP Client functionality in your Check Point Security Gateway or Cluster enables it to interact with an ICAP Server responses, modify their content, and block the matched HTTP connections.

In addition, you can add an ICAP Server decision to the enforcing logic on your Security Gateway, or Cluster (see *"Configuring Additional ICAP Response Headers for Enforcement" on page 216*).

The ICAP Client functionality in your Check Point Security Gateway or Cluster lets you work with 3rd party devices without changing your network topology.

The ICAP Client feature in your Check Point Security Gateway or Cluster supports these:

- HTTP request modification (ICAP REQMOD).
- HTTP response modification (ICAP RESPMOD).
- HTTPS traffic, which you can send to an ICAP Server.

  Important:
  - You must enable and configure the HTTPS Inspection on your Security Gateway or Cluster.
  - The ICAP Client communication with the configured ICAP Servers is in clear (unencrypted) traffic.

- Multiple ICAP Servers:

  ICAP Client can send the HTTP messages to several ICAP Servers concurrently.

- User-defined ICAP *request* header extensions (X-Headers):
  - *X-Client-IP*, *X-Server-IP* (for the destination host), and *X-Authenticated-User* (if the ICAP Client knows it).
  - To work with user-defined ICAP *response* header extension, you must configure them explicitly (see *"Configuring Additional ICAP Response Headers for Enforcement" on page 216*).
  - See the Draft RFC - ICAP Extensions.
- Data Trickling mode.
- UserCheck.

This ICAP Client functionality was tested against an internal ICAP Server and against the Check Point ICAP Server.

Notes:

- There is no full Fail-Open support. In case of HTTP / HTTPS requests or responses with body and with only a single ICAP Server Service, the Fail Mode is always Fail-Close.
  ICAP Client in Check Point Security Gateway can support the Fail-Open with the *Trickling From The End* mode (see *"Configuring ICAP Client Data Trickling Parameters" on page 231*).
- To inspect IPv6 traffic:
  1. Enable IPv6 support on your Security Gateway or Cluster members
  2. Configure all ICAP Servers with IPv6 addresses.

ICAP Client User Disclaimer

You acknowledge you are authorized to receive and install the ICAP Client feature and functionality that can decrypt HTTPS traffic and forward it to 3rd party automated devices for storage and/or compliance.

By installing this feature, you understand that transferring such decrypted data may be in breach of privacy laws in certain countries, and that it is your responsibility to determine whether it is legal to use this functionality in your jurisdiction.

By enabling this functionality, you declare that you have the legal right to decrypt and forward HTTPS traffic, using the ICAP protocol, in all relevant jurisdictions and that you have obtained all necessary consents from your users to do so.

You agree to indemnify and hold harmless Check Point from any and all claims and/or demands related to the violation of any data protection laws and regulation, or to the inappropriate use or implementation of this feature.

Getting Started with ICAP Client

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Procedure:

1. **Configure ICAP Client in Gateway mode**

   a. Connect to the command line on the Security Gateway.

   b. Log in to the Expert mode.

   c. Follow the instructions in the ICAP user-disclaimer:

   ```
   [Expert@GW:0]# IcapDisclaimer.sh
   ```

   If you agreed to the ICAP user-disclaimer, continue to the next step.

   d. Backup the default ICAP Client configuration file:

   ```
   cp -v $FWDIR/conf/icap_client_blade_configuration.C{,_
   BKP}
   ```

   e. Configure the ICAP Client parameters:

   ```
   vi $FWDIR/conf/icap_client_blade_configuration.C
   ```

   For details, see these sections:

   - *"The ICAP Client Configuration File" on page 198*
   - *"Example of the ICAP Client Configuration File" on page 211*

   f. Save the changes in the file and exit the editor.

   g. To inspect the HTTPS traffic with the ICAP Client, you must:

      i. Enable the HTTPS Inspection in the Security Gateway object.

      ii. Configure the HTTPS Inspection Rule Base.

   For details, see *"HTTPS Inspection " on page 393*.

h. Install the Access Control Policy on the Security Gateway:

- If you enabled and configured the HTTPS Inspection, install the policy from the SmartConsole.
- If you did not enable and configure the HTTPS Inspection, you can do one of these:
  - Install the policy from the SmartConsole.
  - Fetch the local policy with the this command on the Security Gateway:

    ```
    fw fetch localhost
    ```

Note - If one of the ICAP configuration parameters is not configured correctly, SmartConsole shows an error with the name of the applicable parameter.

2. Make sure you have an ICAP Server on the network, and that it can receive requests from the ICAP Client. To configure a Check Point Security Gateway as an ICAP Server, see *"Getting Started with ICAP Server" on page 238*.

Configuring ICAP Client in VSX mode

You configure the ICAP Client functionality in the context of *each* applicable Virtual System.

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Procedure:

1. Connect to the command line on the VSX Gateway.
2. Log in to the Expert mode.
3. Go to the context of the applicable Virtual System:

   ```
   vsenv <VSID>
   ```

4. Follow the instructions in the ICAP user-disclaimer:

   ```
   IcapDisclaimer.sh
   ```

   If you agreed to the ICAP user-disclaimer, continue to the next step.

5. Backup the default ICAP Client configuration file:

   ```
   cp -v $FWDIR/conf/icap_client_blade_configuration.C{,_BKP}
   ```

6. Configure the ICAP Client parameters:

   ```
   vi $FWDIR/conf/icap_client_blade_configuration.C
   ```

   For details, see these sections:

   - *"The ICAP Client Configuration File" on page 198*
   - *"Example of the ICAP Client Configuration File" on page 211*

7. Save the changes in the file and exit the editor.
8. To inspect the HTTPS traffic with the ICAP Client, you must:

   a. Enable the HTTPS Inspection in the Virtual System object.

   b. Configure the HTTPS Inspection Rule Base.

   For details, see *"HTTPS Inspection " on page 393*.

9. Install the Access Control Policy on the Virtual System:

- If you enabled and configured the HTTPS Inspection, install the policy from the SmartConsole
- If you did not enable and configure the HTTPS Inspection, you can do one of these:
  - Install the policy from the SmartConsole.
  - Fetch the local policy with the this command in the context of this Virtual System:

    ```
    fw fetch localhost
    ```

Note - If one of the ICAP configuration parameters is not configured correctly, SmartConsole shows an error with the name of the applicable parameter.

The ICAP Client Configuration File

The ICAP Client configuration file on Check Point Security Gateway (`$FWDIR/conf/icap_client_blade_configuration.C`) contains a number of sections.

Each section contains the applicable parameters.

Some parameters accept only string values (notice the mandatory double quotes).

Some parameters accept only integer values.

Parameter	Accepted Values	Description
`:enabled ()`	▪ `"false"` ▪ `"true"`	Controls the ICAP Client feature: ▪ `"false"` - Disables the feature ▪ `"true"` - Enables the feature **Default:** `"false"`
`:filter_http_method ()`	▪ `:method ("GET")` ▪ `:method ("PUT")` ▪ `:method ("POST")` ▪ `:method ("CONNECT")` ▪ `:method ("HEAD")` ▪ `:method ("OPTIONS")`	Controls which HTTP methods to process. If this section is empty, there is no filter for HTTP requests. As a result, ICAP functionality is not activated on *all* HTTP requests. **Default:** `"GET"`, `"PUT"`, and `"POST"`

Parameter	Accepted Values	Description
`:http_services ()`	`:port (`*`NUMBER`*`)` Integer from 1 to 65535	Controls on which port to process the HTTP packets. This is in addition to the HTTP services that are defined by default in SmartConsole (such as: HTTP for TCP port 80 and HTTPS for TCP port 443). You must explicitly add every port, on which you transfer HTTP packets. Ranges of ports are not supported. ICAP filtering (HTTP methods) works on every port you define in this section. If traffic matches a filter, full ICAP functionality is activated on that port. **Default:** `8080` ★ **Best Practice** - Add only applicable ports.
`:inspect_html_response ()`	■ `"false"` ■ `"true"`	Controls whether ICAP Client sends HTTP responses with content-type "`text/html`": ■ `"false"` - ICAP Client does not send an HTTP response with content-type "`text/html`". ■ `"true"` - ICAP Client also sends an HTTP response with content-type "`text/html`". **Default:** `"false"`

Parameter	Accepted Values	Description
`:user_check_interaction_name ()`	Plain-text string (string length is up to 32 characters)	Controls the name of UserCheck block page. If you change the default value, you must configure your value in the SmartConsole: 1. **Objects** menu **> Object Explorer > More object types > UserCheck > New Drop**. 2. Select the **Access Control** related policy. 3. Click **OK**. 4. You must enter the same name as you configured in the ICAP Client configuration file. 5. Add the new message for the UserCheck Block page. 6. Click **OK**. 7. Install the Access Control Policy on the Security Gateway. **Default:** `"Blocked Message - Access Control"`

Parameter	Accepted Values	Description
`:trickling_mode ()`	- `0` - `1` - `2` - `3`	Controls the Data Trickling mode (see *"Configuring ICAP Client Data Trickling Parameters" on page 231*). To avoid HTTP connection timeout when you upload or download large files, you can use the Data Trickling to pass some of the original HTTP payload to its destination, while the ICAP Server scans this HTTP payload. - `0` - *No data trickling*. ICAP Client always holds the HTTP connections until it gets a verdict from an ICAP Server (same functionality as for processing small files). - `1` - Read-only mode. The ICAP Client sends the entire HTTP payload to its original destination without waiting for the ICAP Server's response. When the ICAP Server responds, a log is generated according to the log configuration. - `2` - *Trickling from the Start mode*. ICAP Client sends the entire HTTP payload to its original destination, but slower than the original HTTP connection speed. This behavior is so that the ICAP Server verdict arrives before ICAP Client sends the HTTP payload to its original destination. - `3` - *Trickling at the End* mode. ICAP Client sends the entire HTTP payload to its original destination, except for the last (constant size) HTTP payload. Based on the verdict from the ICAP Server, ICAP Client sends or does not send this last HTTP payload.

Parameter	Accepted Values	Description
		Default: `0`
`:log_level ()`	- `0` - `1` - `2` - `3`	Controls the ICAP Client log level: - `0` - No logs. - `1` - Error logs (arrive with Alert). - `2` - Information logs (include verdict for the original HTTP connection). - `3` - Verbose logs (include service action for each ICAP Server connection). **Default:** `0`
`:icap_servers ()`		Defines the ICAP Servers, with this the ICAP Client works.

`:icap_servers ()`
`- :name ()`
	Plain-text string (string length is up to 32 characters)	Defines the name of the ICAP Server. Used for logging.

`:icap_servers ()`
`- :ip ()`
	IPv4 Address in quad-decimal format (string length is up to 32 characters)	Defines the IPv4 address of the ICAP Server.
		This parameter is mandatory.
		Note - For the ICAP Server on a Check Point cluster, must enter the Cluster Virtual IPv4 address.

`:icap_servers ()`
`- :ip6 ()`
	IPv6 Address (string length is up to 40 characters)	Defines the IPv6 address of the ICAP Server.
		This parameter is optional.
		Notes:
		- The ICAP server must have an IPv6 set up.
		- For the ICAP server on a Check Point cluster, must enter the Cluster Virtual IPv6 address.

`:icap_servers ()`
`- :port ()`
	Integer from 1 to 65535	Defines the port on the ICAP Server.
		Default: `1344`

`:icap_servers ()`
`- :service ()`
	Plain-text string up to 32 characters	Defines the name of the ICAP service.
		Default: `"echo"`

Parameter	Accepted Values	Description
`:icap_servers () - :proto ()`	`"icap"`	Defines the ICAP protocol. **Note** - You must **not** change this value. **Default:** `"icap"`
`:icap_servers () - :modification_mode ()`	■ `"reqmod"` ■ `"respmod"` ■ `"both"`	Defines the ICAP modification mode: ■ `"reqmod"` - HTTP request modification (REQMOD) only. ■ `"respmod"` - HTTP response modification (RESPMOD) only. ■ `"both"` - Both HTTP request and HTTP response modification modes. **Default:** `"both"`
`:icap_servers () - :transp ()`	`"3rd_cpas"`	Defines the 3rd party connection type. **Note** - You must **not** change this value. **Default:** `"3rd_cpas"`
`:icap_servers () - :failmode ()`	■ `close` ■ `open`	Defines the ICAP Client fail mode: ■ `close` - In case of an ICAP error, the original HTTP connection is closed. ■ `open` - In case of an ICAP error, the original HTTP connection stays opened. ■ Logs will be according to `:log_level ()` value. For HTTP requests or responses with a body, the last service fail-mode action is always treated as `close`, regardless of the defined value. **Default:** `close`
`:icap_servers () - :timeout ()`	Integer from 1 to (2^32)-1	Defines the ICAP Client timeout (in seconds). After this time passes, the ICAP Client sends a reset to the ICAP Server. **Default:** `61`

Parameter	Accepted Values	Description
`:icap_servers () - :max_conns ()`	Integer from 1 to (2^32)-1	Defines the maximal number of ICAP opened connections to each configured ICAP Server. **Default:** `250`
`:icap_servers () - :user_check_ action ()`	- `0` - `1` - `2`	Defines the UserCheck action: - `0` - No "Block" page. - `1` - ICAP "Block" page. - `2` - Redirect to UserCheck Portal ("Block" page). On the Security Gateway, you must enable at least one of the supported Software Blades and the UserCheck. **Default:** `1`
`:icap_servers () - :x_headers ()`		Controls the X-Headers: *X-Client-IP*, *X-Server-IP*, and *X-Authenticated-User*.
`:icap_servers () - :x_headers () - :x_client_ip ()`	- `"false"` - `"true"`	Controls the X-Header *X-Client-IP*: - `"false"` - Does not process this X-Header. - `"true"` - Adds the XFF header value of the original HTTP request, if this X-Header exists, or the source IP address if it does not. **Default:** `"false"`
`:icap_servers () - :x_headers () - :x_server_ip ()`	- `"false"` - `"true"`	Controls the X-Header *X-Server-IP*: - `"false"` - Does not process this X-Header. - `"true"` - Adds the destination IP address (proxy's IP address or resolving HTTP Hostname). **Default:** `"false"`

Parameter	Accepted Values	Description
`:icap_servers () - :x_headers () - :x_authenticated_user ()`	■ `"false"` ■ `"true"`	Controls the X-Header *X-Authenticated-User*. ■ `"false"` - Does not process this X-Header. ■ `"true"` - Adds the username from Identity Awareness Software Blade. **Default:** `"false"`
`:icap_servers () - :x_headers () - :authentication_source ()`	■ `"WinNT"` ■ `"LDAP"` ■ `"Radius"` ■ `"Local"`	Defines the Auth-Scheme for user authentication URI. **Note** - URI is given as plain-text, and not in the Base64 encoding. **Default:** `"Local"`
`:icap_servers () - :x_headers () - :base64_username_encode ()`	■ `"false"` ■ `"true"`	Controls whether to encode the X-Header *X-authenticated-user* with Base64 encoding ■ `"false"` - Does not encode. ■ `"true"` - Encodes with the Base64 encoding. **Default:** `"true"`
`:rules_type ()`	■ `"none"` ■ `"include"` ■ `"exclude"`	Controls the network filter rules: ■ `"none"` - Disables the network filter rules. ICAP Client ignores all other parameters of network filter rules. Same as "`any`" in the Source and Destination. ■ `"include"` - ICAP Client sends all IP addresses in the IP ranges (see below) to the ICAP Server ■ `"exclude"` - ICAP Client does **not** send the IP addresses in the IP ranges (see below) to the ICAP Server **Default:** `"none"`
`:network_filter_rules_ip4 ()`		Controls the network filter rules for source and destination IPv4 addresses.

Parameter	Accepted Values	Description
`:network_filter_rules_ip4 () - :src_ip_ranges ()`		Defines the source IPv4 addresses. Each rule can contain only one "`:src_ip_ranges ()`" parameter. The "`:src_ip_ranges ()`" parameter can contain more than one "`:min_ip ()`" and "`:max_ip ()`" parameters.
`:network_filter_rules_ip4 () - :src_ip_ranges () - :min_ip ()`	■ `any` ■ IPv4 Address in quad-decimal format	Defines the minimal source IPv4 address in the range of IPv4 source addresses. ■ `any` - ICAP Client processes the HTTP traffic from all HTTP clients. If you defined "`:min_ip (any)`", you must also define "`:max_ip (any)`". ■ IPv4 Address - ICAP Client processes the HTTP traffic from HTTP clients, whose IPv4 addresses start from this configured IPv4 address.
`:network_filter_rules_ip4 () - :src_ip_ranges () - :max_ip ()`	■ `any` ■ IPv4 Address in quad-decimal format	Defines the maximal source IPv4 address in the range of IPv4 source addresses. ■ `any` - ICAP Client processes the HTTP traffic from all HTTP clients. If you defined "`:max_ip (any)`", you must also define "`:min_ip (any)`". ■ IPv4 Address - ICAP Client processes the HTTP traffic from HTTP clients, whose IPv4 addresses end with this configured IPv4 address.

Parameter	Accepted Values	Description
`:network_filter_rules_ip4 () - :dst_ip_ranges ()`		Defines the destination IPv4 addresses. Each rule can contain only one "`:dst_ip_ranges ()`" parameter. The "`:dst_ip_ranges ()`" parameter can contain more than one "`:min_ip ()`" and "`:max_ip ()`" parameters.
`:network_filter_rules_ip4 () - :dst_ip_ranges () - :min_ip ()`	■ `any` ■ IPv4 Address in quad-decimal format	Defines the minimal destination IPv4 address in the range of IPv4 destination addresses. ■ `any` - ICAP Client processes the HTTP traffic from all HTTP clients. If you defined "`:min_ip (any)`", you must also define "`:max_ip (any)`". ■ IPv4 Address - ICAP Client processes the HTTP traffic from HTTP clients, whose IPv4 addresses start from this configured IPv4 address.
`:network_filter_rules_ip4 () - :dst_ip_ranges () - :max_ip ()`	■ `any` ■ IPv4 Address in quad-decimal format	Defines the maximal destination IPv4 address in the range of IPv4 destination addresses. ■ `any` - ICAP Client processes the HTTP traffic sent to all HTTP servers. If you defined "`:max_ip (any)`", you must also define "`:min_ip (any)`". ■ IPv4 Address - ICAP Client processes the HTTP traffic sent to HTTP servers, whose IPv4 addresses end with this configured IPv4 address.
`:network_filter_rules_ip6 ()`		Controls the network filter rules for source and destination IPv6 addresses.

Parameter	Accepted Values	Description
`:network_filter_rules_ip6 () - :src_ip_ranges ()`		Defines the source IPv6 addresses. Each rule can contain only one "`:src_ip_ranges ()`" parameter. The "`:src_ip_ranges ()`" parameter can contain more than one "`:min_ip ()`" and "`:max_ip ()`" parameters.
`:network_filter_rules_ip6 () - :src_ip_ranges () - :min_ip ()`	- `any` - IPv6 Address	Defines the minimal source IPv6 address in the range of IPv6 source addresses. - `any` - ICAP Client processes the HTTP traffic from all HTTP clients. If you defined "`:min_ip (any)`", you must also define "`:max_ip (any)`". - IPv6 Address - ICAP Client processes the HTTP traffic from HTTP clients, whose IPv6 addresses start from this configured IPv6 address.
`:network_filter_rules_ip6 () - :src_ip_ranges () - :max_ip ()`	- `any` - IPv6 Address	Defines the maximal source IPv6 address in the range of IPv6 source addresses. - `any` - ICAP Client processes the HTTP traffic from all HTTP clients. If you defined "`:max_ip (any)`", you must also define "`:min_ip (any)`". - IPv6 Address - ICAP Client processes the HTTP traffic from HTTP clients, whose IPv6 addresses end with this configured IPv6 address.

Parameter	Accepted Values	Description
`:network_filter_rules_ip6 () - :dst_ip_ranges ()`		Defines the destination IPv6 addresses. Each rule can contain only one "`:dst_ip_ranges ()`" parameter. The "`:dst_ip_ranges ()`" parameter can contain more than one "`:min_ip ()`" and "`:max_ip ()`" parameters.
`:network_filter_rules_ip6 () - :dst_ip_ranges () - :min_ip ()`	■ `any` ■ IPv6 Address	Defines the minimal destination IPv6 address in the range of IPv6 destination addresses. ■ `any` - ICAP Client processes the HTTP traffic from all HTTP clients. If you defined "`:min_ip (any)`", you must also define "`:max_ip (any)`". ■ IPv6 Address - ICAP Client processes the HTTP traffic from HTTP clients, whose IPv6 addresses start from this configured IPv6 address.
`:network_filter_rules_ip6 () - :dst_ip_ranges () - :max_ip ()`	■ `any` ■ IPv6 Address	Defines the maximal destination IPv6 address in the range of IPv6 destination addresses. ■ `any` - ICAP Client processes the HTTP traffic from all HTTP clients. If you defined "`:max_ip (any)`", you must also define "`:min_ip (any)`". ■ IPv6 Address - ICAP Client processes the HTTP traffic from HTTP clients, whose IPv6 addresses end with this configured IPv6 address.

Notes about the "`:network_filter_rules_ip4 ()`" and "`:network_filter_rules_ip6 ()`" parameters:

- Each "`:network_filter_rules_ipX ()`" rule can contain only one "`:src_ip_ranges ()`" parameter.

  The "`:src_ip_ranges ()`" parameter in the rule can contain more than one "`:min_ip ()`" and "`:max_ip ()`" parameters.
- Each "`:network_filter_rules_ipX ()`" rule can contain only one "`:dst_ip_ranges ()`" parameter.

  The "`:dst_ip_ranges ()`" parameter in the rule can contain more than one "`:min_ip ()`" and "`:max_ip ()`" parameters.
- ICAP Client performs these logical operations in parallel:
  - [`:network_filter_rules_ip4 ()`] **OR** [`:network_filter_rules_ip6 ()`]
  - [`:src_ip_ranges ()`] **AND** [`:dst_ip_ranges ()`]
  - In the "`:src_ip_ranges ()`" parameter - [`:min_ip ()`] **OR** [`:max_ip ()`]
  - In the "`:dst_ip_ranges ()`" parameter - [`:min_ip ()`] **OR** [`:max_ip ()`]

  If the result of these logical operations is TRUE and `:rules_type ("include")`, then ICAP Client works.

  If the result of these logical operations is TRUE and `:rules_type ("exclude")`, then ICAP Client does **not** work.

Example of the ICAP Client Configuration File

This is an example configuration file `$FWDIR/conf/icap_client_blade_configuration.C`:

```
(
    :enabled ("true")
    :filter_http_method (
            : (
                :method ("GET")
            )
            : (
                :method ("PUT")
            )
            : (
                :method ("POST")
            )
    )
    :http_services (
            : (
                :port (8080)
            )
            : (
                :port (8443)
            )
    )
    :inspect_html_response ("false")
    :trickling_mode (0)
    :user_check_interaction_name ("Blocked Message - Access Control")
    :log_level (2)
    :icap_servers (
            : (
                :name ("icap_server_1")
                :ip ("10.1.0.20")
                :ip6 ("2001:db8:6:f101::15")
                :port (1344)
                :service ("echo")
                :proto ("icap")
                :modification_mode ("both")
                :transp ("3rd_cpas")
                :failmode (open)
                :timeout (60)
                :max_conns (50)
                :user_check_action (1)
                :x_headers (
                    :x_client_ip ("false")
                    :x_server_ip ("false")
                    :x_authenticated_user ("false")
                    :authentication_source ("Local")
                    :base64_username_encode ("true")
                )
            )
            : (
                :name ("icap_server_2")
                :ip ("10.1.0.30")
                :ip6 ("2001:db8:6:f101::16")
                :port (1344)
                :service ("echo")
                :proto ("icap")
                :modification_mode ("respmod")
                :transp ("3rd_cpas")
                :failmode (close)
                :timeout (120)
                :max_conns (250)
                :user_check_action (2)
                :x_headers (
                    :x_client_ip ("true")
                    :x_server_ip ("true")
                    :x_authenticated_user ("true")
                    :authentication_source ("WinNT")

                )
            )
    )
    :rules_type ("include")
    :network_filter_rules_ip4 (
            : (
                :src_ip_ranges (
                    : (
                        :min_ip ("10.0.0.6")
                        :max_ip ("10.0.0.10")
                    )
                    : (
                        :min_ip ("10.0.0.100")
                        :max_ip ("10.0.0.150")
                    )
                )
                :dst_ip_ranges (
                    : (
                        :min_ip ("10.1.0.1")
                        :max_ip ("10.1.255.255")
                    )
                )
            )
            : (
                :src_ip_ranges (
                    : (
                        :min_ip ("10.0.0.21")
                        :max_ip ("10.0.0.24")
                    )
                )
                :dst_ip_ranges (
                    : (
                        :min_ip ("any")
                        :max_ip ("any")
                    )
                )
            )
    )
    :network_filter_rules_ip6 (
            : (
                :src_ip_ranges (
                    : (
                        :min_ip ("2001:db8:5:f101::11")
                        :max_ip ("2001:db8:5:f101::15")
                    )
                )
                :dst_ip_ranges (
                    : (
                        :min_ip ("2001:db8:6:f101::1")
                        :max_ip ("2001:db8:6:f101::20")
                    )
                )
            )
    )
)
```

Clarification about the rules in the example above:

- [`:network_filter_rules_ip4 ()`] **OR** [`:network_filter_rules_ip6 ()`]
- In the "`:network_filter_rules_ip4 ()`":

  [`:src_ip_ranges ()`] **AND** [`:dst_ip_ranges ()`]

  - Rule

    All traffic that arrives from IPv4 (10.0.0.6 **OR** 10.0.0.7 ... **OR** 10.0.0.10)

    AND destined to IPv4 (10.1.0.1 **OR** 10.1.0.2 ... **OR** 10.1.255.255)

  - Rule

    All traffic that arrives from IPv4 (10.0.0.100 **OR** 10.0.0.101 ... **OR** 10.0.0.150)

    AND destined to IPv4 (10.1.0.1 **OR** 10.1.0.2 ... **OR** 10.1.255.255)

  - Rule

    All traffic that arrives from IPv4 (10.0.0.21 **OR** 10.0.0.22 ... **OR** 10.0.0.24)

    AND destined to any IPv4 address

- In the "`:network_filter_rules_ip6 ()`":

  [`:src_ip_ranges ()`] **AND** [`:dst_ip_ranges ()`]

  - Rule

    All traffic that arrives from IPv6 (2001:db8:5:f101::11 **OR** 2001:db8:5:f101::12 ... **OR** 2001:db8:5:f101::15)

    AND destined to IPv6 (2001:db8:6:f101::1 **OR** 2001:db8:6:f101::2 ... **OR** 2001:db8:6:f101::20)

Advanced ICAP Client Configuration

You can configure advanced settings in the ICAP Client using the applicable kernel parameters.

For general instructions, see the *R81.20 Quantum Security Gateway Guide* > *Working with Kernel Parameters on Security Gateway*.

You can configure these advanced settings in the ICAP Client:

- Additional ICAP response headers for enforcement
- Additional HTTPS Status Codes, which ICAP Client sends in RESPMOD
- Connection timeout for ICAP connections
- ICAP Client data trickling parameters

Configuring Additional ICAP Response Headers for Enforcement

In This Section:

Description

To adjust the enforcement according to ICAP response headers from an ICAP Server, you can configure specific HTTP headers. When ICAP Client on Check Point Security Gateway receives these HTTP headers, the Security Gateway blocks the matched HTTP connections. See the Draft RFC - ICAP Extensions.

Default HTTP Response X-Headers

By default, ICAP Client recognizes these three user-defined ICAP *response* header extensions.

Default X-Headers

HTTP Response X-Header	Description	Examples

`X-Virus-ID`	Contains a short description of the threat that was found in the content.
	On a single line it can contain any virus or threat description.
	If multiple threats were found, only the first one is returned.
	This header is a shorter alternative to the `X-Infection-Found` header.
	This header is available only if the content was scanned, and some violations were found.
		`X-Virus-ID: EICAR Test String`
		`X-Virus-ID: Encrypted Archive`

HTTP Response X-Header	Description	Examples

`X-Violations-Found`	Contains the detailed description of all the policy violations (for example, found viruses) that occurred while handling the request.
	If the scanned content was an archive, the scan results are listed for the contained files as well.
	If multiple threats were found for a single file, only the first one is returned.
	This header is present only if the content was scanned, and some violations were found.
	This header has a multi-line value starting with the number of reported violations on the first line and four additional lines per violation:
	1. The first line contains the number of the reported violations.
	2. The following lines contain the details:
	`Filename`
	May describe a single file within an archive that the ICAP Client sent to the ICAP Server.
	`ThreadDescription`
	Human readable description of the threat. For example, the virus name or the policy violation description. It may contain spaces and should not be quoted.
	`ProblemID:`
		`X-Violations-Found: 2`
		`test.zip/dir1/eicar.com`
		`EICAR Test String`
		`11101`
		`2`
		`test.zip/dir2/eicar.com`
		`EICAR Test String`
		`11101`
		`2`

HTTP Response X-Header	Description	Examples
	One-digit integer identifier of the policy violation. For example, a virus ID. Currently, 0 is returned for all threats. `ResolutionID:` 0: File was not repaired. 1: File was repaired. 2: Violating part was removed (usually used if a file was removed from a container).	

HTTP Response X-Header	Description	Examples

`X-Infection-Found`	Contains the description of the threat that was found in the ICAP message body of the request.
	If multiple threats were found, only the first one is returned.
	This header is present only if the content was scanned, and some violations were found.
	The value is a semicolon-separated parameter list with exactly three parameters in a given order:
	`TypeID:`
	0: Virus infection.
	1: Mail policy violation (for example, illegal file attachment name).
	2: Container violation (for example, a ZIP file that takes too long to decompress).
	`ResolutionID:`
	0: File was not repaired.
	1: The returned file in the RESPMOD response is the repaired version of the infected file that was encapsulated in the request.
	2: The original file should be blocked or rejected due to container or mail policy violations.
	`ThreadDescription:`
		`X-Infection-Found: Type=0; Resolution=1; Threat=EICAR Test String;`
		Explanation: The ICAP request contained data that is infected by the EICAR test string. The file was repaired (for example, the `eicar.com` file was removed from an archive and the remaining archive is sent back in the response).

HTTP Response X-Header	Description	Examples
	Human readable description of the threat. For example, the virus name or the policy violation description. It may contain spaces and should not be quoted. It must not contain semicolons, because it is terminated by the final semicolon of the header definition.	

Additional HTTP Response X-Headers

You can add additional HTTP response X-Headers for the ICAP Client to recognize.

Additional X-Headers

HTTP Response X-Header	Description	Examples

`X-Response-Info`	Contains a one word description of the action the ICAP Server applied on the HTTP request.
	This header is available in all responses sent by the ICAP Server.
		`X-Response-Info: Allowed`
		`X-Response-Info: Blocked`
		`X-Response-Info: Options`

`X-Response-Desc`	Contains a one line description about the action that the ICAP Server applied on the content.
	This header is available in all "blocked" responses.
	In case of the content was scanned, and some violations were found, the returned string is equivalent to `X-Blocked-Reason`'s value.
		`X-Response-Desc: Infected`
		`X-Response-Desc: Encrypted Archive`

`X-Include`	Contains the list of requested HTTP headers, which the ICAP Client should add to the HTTP requests, if the information is available. This header is present only in HTTP `Options` responses. This header is a comma-separated list of any ICAP header extension field names that the ICAP Server wants the ICAP Client to add to the requests, if the information is available and the header is supported.	`X-Include: X-Client-IP`
`X-Blocked-Reason`	Metadefender specific custom header. Contains the blocking reason of the content. This header is available only if the content was scanned, and some violations were found.	`X-Blocked-Reason: Infected`

HTTP Response X-Header	Description	Examples
`X-ICAP-Profile`	Contains the applied workflow's name (user profile). This header is available only if the file was scanned.	`X-ICAP-Profile: Proxy`

Configuring the Additional HTTP Response X-Headers

You add the additional HTTP response X-Headers as values of the specific kernel parameter:

Item	Description
Name	`icap_unwrap_append_header_str`
Type	String
Notes	■ Length of each added HTTP header is up to 80 characters ■ You can add up to 21 such HTTP headers ■ The ICAP Client also uses this HTTP response status: `HTTP/1.0 403 Forbidden` (according to RFC 3507).

For general instructions, see the *R81.20 Quantum Security Gateway Guide* > Chapter *Working with Kernel Parameters on Security Gateway*.

To see the list of the configured HTTP response X-headers

1. Set the value of this kernel parameter to the string `'__print__'`:

   ```
   fw ctl set str icap_unwrap_append_header_str '__print__'
   ```

2. Print the list of the configured HTTP headers:

   ```
   dmesg | grep append_icap_unwrap_headers
   ```

Example:

```
[Expert@GW:0]# fw ctl set str icap_unwrap_append_header_str '__print__'
[Expert@GW:0]# dmesg | grep append_icap_unwrap_headers
[fw6_0];append_icap_unwrap_headers: ==> new icap_unwrap_headers array is: [ X-Virus-ID ; X-
Violations-Found ; X-Infection-Found ;]
[fw4_0];append_icap_unwrap_headers: ==> new icap_unwrap_headers array is: [ X-Virus-ID ; X-
Violations-Found ; X-Infection-Found ;]
[Expert@GW:0]#
```

To add an HTTP response X-Header in detect only mode temporarily

Note - In this mode, the ICAP Client does not block the matched HTTP connections.

1. Set the value of this string kernel parameter to the name if the X-header:

   ```
   fw ctl set str icap_unwrap_append_header_str '<Name of X-header>'
   ```

2. Print the list of the configured HTTP headers:

   ```
   dmesg | grep append_icap_unwrap_headers
   ```

Example:

```
[Expert@GW:0]# fw ctl set str icap_unwrap_append_header_str 'X-Response-Info'
[Expert@GW:0]# fw ctl set str icap_unwrap_append_header_str 'X-Response-Desc'
[Expert@GW:0]# fw ctl set str icap_unwrap_append_header_str '__print__'
[Expert@GW:0]# dmesg | grep append_icap_unwrap_headers
[fw6_0];append_icap_unwrap_headers: ==> new icap_unwrap_headers array is: [ X-Virus-ID ; X-
Violations-Found ; X-Infection-Found ; X-Response-Info ; X-Response-Desc ;]
[fw4_0];append_icap_unwrap_headers: ==> new icap_unwrap_headers array is: [ X-Virus-ID ; X-
Violations-Found ; X-Infection-Found ; X-Response-Info ; X-Response-Desc ;]
[Expert@GW:0]#
```

To delete all configured HTTP response X-Headers temporarily

1. Set the value of this kernel parameter to an empty string `''`:

   ```
   fw ctl set str icap_unwrap_append_header_str ''
   ```

2. Print the list of the configured HTTP headers:

   ```
   fw ctl set str icap_unwrap_append_header_str '__print__'
   dmesg | grep append_icap_unwrap_headers
   ```

Example:

```
[Expert@GW:0]# fw ctl set str icap_unwrap_append_header_str ''
[Expert@GW:0]# fw ctl set str icap_unwrap_append_header_str '__print__'
[Expert@GW:0]# dmesg | grep append_icap_unwrap_headers
[Expert@GW:0]#
```

To restore the default configured HTTP response X-Headers temporarily

1. Set the value of this kernel parameter to the strings `'X-Virus-ID'`, `'X-Violations-Found'`, and `'X-Infection-Found'`:

   ```
   fw ctl set str icap_unwrap_append_header_str 'X-Virus-ID'
   fw ctl set str icap_unwrap_append_header_str 'X-Violations-
   Found'
   fw ctl set str icap_unwrap_append_header_str 'X-Infection-
   Found'
   ```

2. Print the list of the configured HTTP headers:

   ```
   fw ctl set str icap_unwrap_append_header_str 'X-Infection-
   Found'
   dmesg | grep append_icap_unwrap_headers
   ```

Configuring Additional HTTPS Status Code, which ICAP Client Sends in RESPMOD

In This Section:

Description

To send HTTP server response to an ICAP server in RESPMOD, you can configure HTTP server status codes that the ICAP Client sends to the ICAP server.

By default, the ICAP Client sends server status codes 1xx or 2xx.

Configuring the HTTP Server Status Codes

You add the HTTP server status codes as values of the specific kernel parameter:

Item	Description
Name	`icap_append_status_code_str`
Type	String
Notes	■ Length of each added server status code is from 1 to 3 characters ■ Accepted string values are: • `'<Single Digit N>'` - ICAP Client sends all status codes Nyz that start with the specified digit N (for example, if you set the value to `'3'`, the ICAP Client sends status codes 3yz) • `'<Two Digits NN>'` - ICAP Client sends all status codes NNz that start with the specified two digits N (for example, if you set the value to `'30'`, the ICAP Client sends status codes 30z) • `'<Three Digits NNN>'` - ICAP Client sends the specified status code NNN (for example, if you set the value to `'304'`, the ICAP Client sends the status code 304) ■ You can add up to 10 server status codes

For general instructions, see the *R81.20 Quantum Security Gateway Guide* > Chapter *Working with Kernel Parameters on Security Gateway*.

To see the list of the configured HTTP server status codes

1. Set the value of this kernel parameter to the string `'__print__'`:

   ```
   fw ctl set str icap_append_status_code_str '__print__'
   ```

2. Print the list of the configured server status codes:

   ```
   dmesg | grep icap_client_append_status_code
   ```

Example:

```
[Expert@GW:0]# fw ctl set str icap_append_status_code_str '__print__'
[Expert@GW:0]# dmesg | grep icap_client_append_status_code
[fw6_0];icap_client_append_status_code: ==> new 'status code' array is: [ 1 ; 2 ;]
[fw4_0];icap_client_append_status_code: ==> new 'status code' array is: [ 1 ; 2 ;]
[Expert@GW:0]#
```

To add an HTTP server status code temporarily

1. Set the value of this kernel parameter to the desired string (see the *Notes* above):

   ```
   fw ctl set str icap_append_status_code_str 'N'
   fw ctl set str icap_append_status_code_str 'N'
   fw ctl set str icap_append_status_code_str 'NNN'
   ```

2. Print the list of the configured server status codes:

   ```
   fw ctl set str icap_append_status_code_str '__print__'
   dmesg | grep icap_client_append_status_code
   ```

Example:

```
[Expert@GW:0]# fw ctl set str icap_append_status_code_str '3'
[Expert@GW:0]# fw ctl set str icap_append_status_code_str '__print__'
[Expert@GW:0]# dmesg | grep icap_client_append_status_code
[fw6_0];icap_client_append_status_code: ==> new 'status code' array is: [ 1 ; 2 ; 3 ;]
[fw4_0];icap_client_append_status_code: ==> new 'status code' array is: [ 1 ; 2 ; 3 ;]
[Expert@GW:0]#
```

To delete all configured HTTP server status codes temporarily

1. Set the value of this kernel parameter to an empty string `''`:

   ```
   fw ctl set str icap_append_status_code_str ''
   ```

2. Print the list of the configured HTTP headers:

   ```
   fw ctl set str icap_append_status_code_str '__print__'
   dmesg | grep icap_client_append_status_code
   ```

Example:

```
[Expert@GW:0]# fw ctl set str icap_append_status_code_str ''
[Expert@GW:0]# fw ctl set str icap_append_status_code_str '__print__'
[Expert@GW:0]# dmesg | grep icap_client_append_status_code
[Expert@GW:0]#
```

To restore the default configured HTTP server status codes temporarily

1. Set the value of this kernel parameter to the strings `'1'` and `'2'`:

   ```
   fw ctl set str icap_append_status_code_str '1'
   fw ctl set str icap_append_status_code_str '2'
   ```

2. Print the list of the configured server status codes:

   ```
   fw ctl set str icap_append_status_code_str '__print__'
   dmesg | grep icap_client_append_status_code
   ```

Configuring Connection Timeout for ICAP Connections

Description

To release idle connections and unresponsive sessions to ICAP Servers, you can adjust the connection timeout (in seconds) in the ICAP Client.

Configuring the Connection Timeout

You configured the connection timeout as a value of the specific kernel parameter:

Item	Description
Name	`icap_blade_conn_pool_timeout`
Type	Integer
Notes	■ Default value is 300 (seconds) ■ The ICAP Server should maintain its own Timeout/KeepAliveTimeout configurations to handle unexpected traffic lost from the ICAP Client side (for example, due to reboot or disconnect)

For general instructions, see the *R81.20 Quantum Security Gateway Guide* > Chapter *Working with Kernel Parameters on Security Gateway*.

To print the current connection timeout value

```
fw ctl get int icap_blade_conn_pool_timeout
```

Example:

```
[Expert@GW:0]# fw ctl get int icap_blade_conn_pool_timeout
icap_blade_conn_pool_timeout = 300
[Expert@GW:0]#
```

To set the connection timeout value temporarily

```
fw ctl set int icap_blade_conn_pool_timeout <Number>
```

Additional Information

You can cancel the reuse of ICAP Client-to-Server connections on your Security Gateway for ICAP requests/responses.

Use this kernel parameter:

Item	Description
Name	`icap_blade_enable_reuse_opt`

Item	Description
Type	Integer
Notes	■ Accepted values: • `0` - Security Gateway does not reuse the ICAP Client-to-Server connections • `1` - Security Gateway reuses the ICAP Client-to-Server connections - each connection is reused and not closed after handling the successful ICAP requests ■ Default value: `1`

Configuring ICAP Client Data Trickling Parameters

Description

Patience pages provide a solution to appease users during relatively short delays in object scans. However, scanning relatively large objects, scanning objects over a smaller bandwidth pipe, or high loads on servers might disrupt the user experience, because connection timeouts occur. To prevent such time-outs, you can allow data trickling to occur. During the Data Trickling, the data transmits at a very slow rate to the client at the beginning of the scan, or near the very end.

Trickle from the Start mode

In Trickle from Start mode, the ICAP Client buffers a small amount of the beginning of the HTTP response body. As the ICAP Server continues to scan the HTTP response, the ICAP Client allows one byte per second to the HTTP Client. After the ICAP Server completes its scan, if the object is deemed to be clean (no HTTP response modification is required), the ICAP Client sends the rest of the object bytes to the HTTP Client at the best speed allowed by the connection. If the object is deemed to be malicious, the ICAP Client terminates the connection and the remainder of the HTTP response object. Trickling from the Start is the more secure Data Trickling option, because the HTTP Client receives only a small amount of data pending the outcome of the virus scan.

Trickle at the End mode

In Trickle at End mode, the ICAP Client sends the HTTP response to the HTTP Client at the best speed allowed by the connection, except for the last 16KB of data. As the ICAP Server performs the content scan, the ICAP Client allows one byte per second to the HTTP Client. After the ICAP Server completes its scan, if the object is deemed to be clean (no HTTP response modification is required), the ICAP Client sends the rest of the object bytes to the HTTP Client at the best speed allowed by the connection. This method is more user-friendly than Trickle at Start. This is because users tend to be more patient when they notice that 99% of the object is downloaded versus 1%, and are less likely to perform a connection restart. However, network administrators might perceive this method as the less secure method, as a majority of the object is delivered before the results of the ICAP scan.

Notes about Data Trickling on Check Point Security Gateway

- There is no true data-modification (meaning, no true content adaptation) during the data trickling.

  In the *Trickling at the End* mode, there is no data modification at all.

- Data Trickling (both *Trickling from the Start* and *Trickling at the End* modes) cannot work when there is no *Content-length* header in the HTTP message.

- In the *Trickling at the End* mode, Check Point Security Gateway supports the 204 status code (with the HTTP header "`Allow: 204`", for HTTP reply "`No change / Unmodified`").

- There is still an applicative timeout (`:icap_servers ()`-`:timeout`) of the ICAP session that user needs to define according to the `icap-service` demand, after which the `fail-action` follows.

  The applicative timeout is also a factor in determining the maximal buffer size for *Trickling from the Start* mode..

Configuring ICAP Client Data Trickling

You configure the ICAP Client Data Trickling with the specific kernel parameters on Security Gateway.

For general instructions, see the R81.20 Quantum Security Gateway Guide > Chapter *Working with Kernel Parameters on Security Gateway*.

Kernel Parameter 1

Item	Description
Name	`icap_blade_trickling_bytes_ps`
Description	Specifies how many bytes per second to send to the original HTTP destination, while *Trickling from the Start* works. The HTTP Client sees very slow upload and download progress.
Type	Integer
Default value	10
Notes	The configured value must be much less than the byte-rate of the ICAP connection.
Example	If the ICAP Server scans a file with the size of ~600 kilobytes for a 1 minute, the ICAP connection byte-rate is ~10 kilobytes per second. Therefore, the configured value must be much less than 10,000 bytes per second.

Kernel Parameter 2

Item	Description
Name	`icap_blade_trickling_interval`
Description	Specifies the interval in seconds for sending bytes to the original HTTP destination, while *Trickling from the Start* works.
Type	Integer
Default value	1
Notes	The configured value must be more than or equal to 1.
Example	Value 2 means that the ICAP Client sends bytes to the original HTTP destination only every 2 seconds.

Kernel Parameter 3

Item	Description
Name	`icap_blade_trickling_threshold_mb`
Description	Specifies the *Content-Length* threshold in megabytes. Only if the HTTP *Content-Length* of the original HTTP connection is greater than this threshold, the *Trickling from the Start* is activated.
Type	Integer
Default value	0
Example	Value 1 means: ■ The ICAP Client sends only files that are larger than 1 megabyte to the original HTTP destination. ■ The ICAP Client does not send all other files before it gets the verdict from the ICAP Server.

Kernel Parameter 4

Item	Description
Name	`icap_blade_trickling_kbytes_from_end`
Description	During the *Trickling at the End* mode, specifies how many kilobytes ICAP Client does not send to the original HTTP destination before the ICAP Client gets the verdict from the ICAP Server.
Type	Integer
Default value	16
Example	Value 16 means: ■ The ICAP Client does not send only the last 16 kilobytes of the file before it gets the verdict from the ICAP Server. ■ The ICAP Client sends all other files to the original HTTP destination in the HTTP connection byte-rate.

The Security Gateway as an ICAP Server

In This Section:

Check Point ICAP Server can work with multiple ICAP Clients.

Check Point ICAP Server is supported on R80.20 Security Gateways and higher for the Threat Emulation and Anti-Virus blades. From R81, ICAP Server also supports the Threat Extraction blade.

To activate the ICAP Server on a Security Gateway object in SmartConsole, you must first enable Threat Emulation and/or Anti-Virus and/or Threat Extraction on that Security Gateway object.

If you enable ICAP Server on the Security Gateway and not enable the Threat Emulation Anti-Virus, or Threat Extraction blades, the ICAP Server runs but without inspection.

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

ICAP Server functionality is not supported in ClusterXL Load Sharing mode.

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

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

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

For more information, see sk111306.

ICAP Server Actions

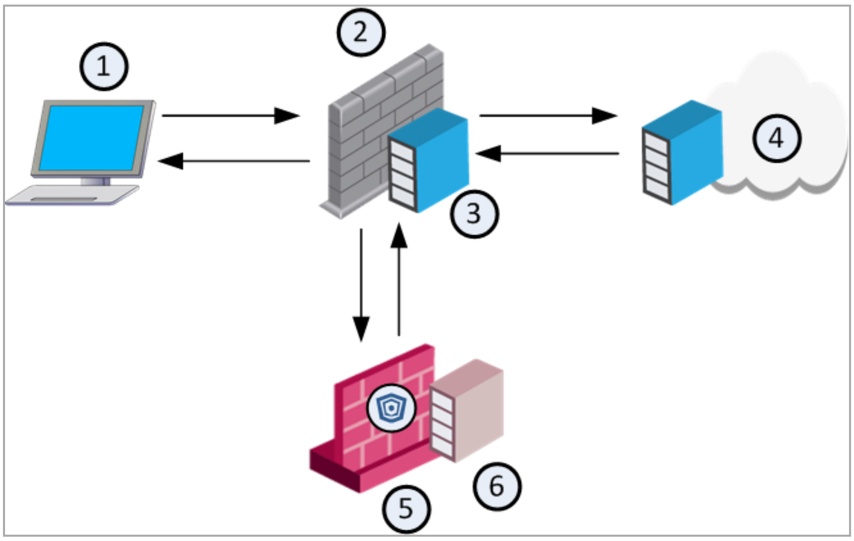
Check Point ICAP Server has 3 possible actions:

ICAP Action	Description and Example
Block	▪ ICAP Server sends an error to the ICAP Client. ▪ ICAP Server sends a block page to the ICAP Client. For example: A Check Point UserCheck page presented by the Threat Emulation, Anti-Virus, or Threat Extraction Software Blades.
Continue / Not modified	A default gateway or a proxy server can forward the HTTP Request / Response to its original destination.

ICAP Action	Description and Example
Flie modification	Applicable when Threat Extraction is activated. The ICAP Server modifies the HTTP/HTTPS content and sends the modified content to the ICAP Client.

ICAP Server Workflow

Sample Workflow



Item No.	Description
1	Client
2	Third party gateway or proxy
3	ICAP Client
4	Web server
5	Check Point gateway
6	ICAP Server

Workflow example for working with Check Point ICAP Server in RESPMOD

Step	Instructions
1	The client sends a request to the third party gateway/proxy server to download a file.
2	The third party gateway/proxy sends the download request to the Web server.

Step	Instructions
3	The Web server sends the requested file to the third party gateway/proxy.
4	The ICAP Client forwards the file to the ICAP Server which is in the Check Point Threat Emulation gateway.
5	The ICAP Server sends the file to the Threat Emulation engine.
6	The Threat Emulation checks the file a. The Threat Emulation engine returns a verdict (block, modified or continue) to the ICAP Server. b. The ICAP Server sends the verdict to the ICAP Client. c. The ICAP Client sends the verdict to the client.

Getting Started with ICAP Server

To enable ICAP Server support on the Security Gateway / Cluster:

Step	Instructions
1	**Enable ICAP Server support on the Check Point Security Gateway or Cluster** 1. From the left navigation panel, click **Gateways & Servers**. 2. Double-click the Security Gateway / Cluster object. 3. From the left tree, go to **ICAP Server**. 4. Select **Enable ICAP Server**. 5. In **Service**, the default service is TCP ICAP, which runs on port 1344. **Optional: You can create a new ICAP service and use it instead of the default service** a. Go to the Object Explorer and select **New** > **More** > **Service** > **TCP**. b. Enter the object name and add a comment if necessary. c. In **General**, do not select a protocol. d. In **Match By**, select the **Port** you want the service to run on. e. **Optional:** Configure the **Advanced** features. For a detailed explanation on the advanced service features, check the online help. f. Click **OK** The new service now appears in the drop-down **Service** list. **Optional: You can create a new ICAP service to work over TLS** From R81.20, Check Point Security Gateway supports encrypted connection between the ICAP Server and ICAP Client. a. Go to the Object Explorer and select **New** > **More** > **Service** > **TCP**. b. Enter the object name and add a comment if necessary. c. In **General**, do not select a protocol. d. In **Match By**, select the **Port** you want the service to run on. e. **Optional:** Configure the **Advanced** features. For a detailed explanation on the advanced service features, check the online help. f. Click **OK**. g. Create the CA certificate and ICAP Server certificate through your application of choice. h. Export the certificates in PEM file formats: i. Copy the server certificate "`icapcert.pem`" to the Security Gateway / each Cluster Member to some directory (for example, `/home/admin`). j. Connect to the command line on the Security Gateway / each Cluster Member. k. Log in to the Expert mode. l. Edit the ICAP Server configuration file: `vi $FWDIR/c-icap/etc/c-icap.conf`

Step	Instructions

m. Add this line with the path of the server certificate:

```
TlsPort [port_number]
cert=/home/admin/icapcert.pem
```

n. Save the changes in the file and exit the editor.

o. Load the updated ICAP Server configuration with this command on the Security Gateway / each Cluster Member.:

```
icap_server reconf
```

p. Copy the CA certificate PEM file of the ICAP Server to the ICAP Client.

q. Configure the ICAP Client so it is able to connect to the ICAP Server over TLS. Note these parameters:

- ICAP protocol (icaps - for TLS).
- ICAP Server IP address and port number.
- Direct the ICAP modification requests to the ICAP Server SandBlast service.
- TLS specifications

For example:

Third party ICAP Client (Squid) configuration:

```
adaptation_send_client_ip on
adaptation_send_username on
icap_client_username_encode on
icap_client_username_header X-Authenticated-User
icap_service service_req_pre reqmod_precache
icaps://<IP_ADDRESS>:<PORT_NUMBER>/sandblast tls-
cafile=<CERTIFICATE_FILE> tls-domain=<DOMAIN_NAME>
icap_service service_req_post reqmod_postcache
icaps://<IP_ADDRESS>:<PORT_NUMBER>/sandblast tls-
cafile=<CERTIFICATE_FILE> tls-domain=<DOMAIN_NAME>
icap_service service_resp_pre respmod_precache
icaps://<IP_ADDRESS>:<PORT_NUMBER>/sandblast tls-
cafile=<CERTIFICATE_FILE> tls-domain=<DOMAIN_NAME>
icap_service service_resp_post respmod_postcache
icaps://<IP_ADDRESS>:<PORT_NUMBER>/sandblast tls-
cafile=<CERTIFICATE_FILE> tls-domain=<DOMAIN_NAME>
adaptation_access service_req_post allow all
adaptation_access service_resp_pre allow all
adaptation_access service_resp_post allow all
```

6. Configure **Fail Mode** - In case of an error, configure if requests to the ICAP server are blocked or allowed.
7. You can configure an implied rule for ICAP in the Access Control policy.

Step	Instructions
	8. Click **OK**.
2	Configure the ICAP client to connect to the Gateway. See *"Getting Started with ICAP Client" on page 194*.
3	**Configure the ICAP rule** When you enable ICAP Server in the Security Gateway or Cluster object, SmartConsole automatically creates a rule in the Threat Prevention Rule Base. One rule is created for each Security Gateway / Cluster that has ICAP Server enabled. Configure the applicable action in the **Action** column of this rule. You can select a different profile for each ICAP rule. **Notes:** ■ In **Threat Extraction > UserCheck** settings, if you want to allow the user access to the original file, you must configure access from the internal network to the ICAP server. This way, the client is able to download the original files (the internal network is connected to the ICAP client and not directly to the gateway or ICAP Server). ■ Unlike other Threat Prevention rules, you cannot create exceptions for an ICAP rule.
4	For Threat Extraction support, in the Threat Prevention profile editor, go to **Threat Extraction** > **General** page > **Protocol** > select **Web (HTTP/HTTPS)**.
5	To scan files with Anti-Virus, in the Threat Prevention profile, go to the **Anti-Virus** page, and select **Enable deep inspection scanning (impacts performance)**.

Step	Instructions

6	**Configure advanced ICAP Server settings on the Security Gateway**
	The ICAP Server uses processes to handle the requests it receives from the ICAP Client. Each process generates multiple threads, and each thread handles one request from the ICAP Client to the ICAP Server.
	The ICAP Server supports dynamic scaling of the number of processes for optimal performance.
	1. From the left navigation panel, click **Gateways & Servers**.
	2. Double-click the Security Gateway / Cluster object.
	3. From the left tree, go to **ICAP Server** > **Advanced**.
	4. Configure the applicable settings:
	■ **The maximum allowed number of server processes**
	The number of processes increases or decreases as needed.
	You can configure the maximum value.
	Range: 1-100
	The maximum number of concurrent connections that the ICAP Server can handle:
	`(The maximum allowed number of server processes) x`
	`(The number of threads per a child process)`
	■ **The number of threads per a child process**
	The number of available threads increases or decreases as needed.
	You can configure the maximum value.
	Range: 1-100
	■ **Start a new child process if the number of available threads is less than [x]**
	This option allows dynamic growth and lets you configure the number of new threads as needed.
	The ICAP Server counts the total number of available (idle) threads.
	If this number is lower than the number configured in this field, it creates a new child process.
	■ **End a child process if the number of available threads is more than [x]**
	This option allows dynamic reduction of the number of threads as needed.
	The ICAP Server counts the total number of available (idle) threads.
	If this number is higher than the number configured in this field, it ends a child process.
	5. Click **OK**.
	6. Install the Threat Prevention Policy.

7	Install the Threat Prevention policy.

For information on how to test ICAP Server functionality, see sk174487.

Related Configuration on the ICAP Client

When you work with Check Point ICAP Server, make sure to set this configuration on your ICAP Client.

Configuration for ICAP Client

- Direct the ICAP modification requests to the ICAP Server **sandblast** service.

  For example: `icap://<IP_Address>:1344/sandblast.`
- Set the ICAP Client to send these headers, if possible:
  - `X-Client-IP`
  - `X-Server-IP`
  - `X-Authentication-User`

  These headers are used in the ICAP Server logs.
- Make sure the operation timeout for the ICAP Client is equal or higher than the operation timeout for the ICAP Server.

  Note - The **sandblast** service on the Check Point ICAP Server can take some time to respond.
- For HTTPS traffic, configure the ICAP Client to send clear HTTP (decrypted HTTPS) traffic to the Check Point ICAP Server. If this option is not available on your ICAP Client, the ICAP Server is not able to process the traffic.

Notes:

- For a detailed explanation on how to configure a Check Point ICAP Client, see *"Security Gateway as ICAP Client" on page 186*
- For a detailed explanation on how to configure a third party ICAP Client, see vendor's documentation.

Use Case

You can use the ICAP technology to communicate HTTPS content.

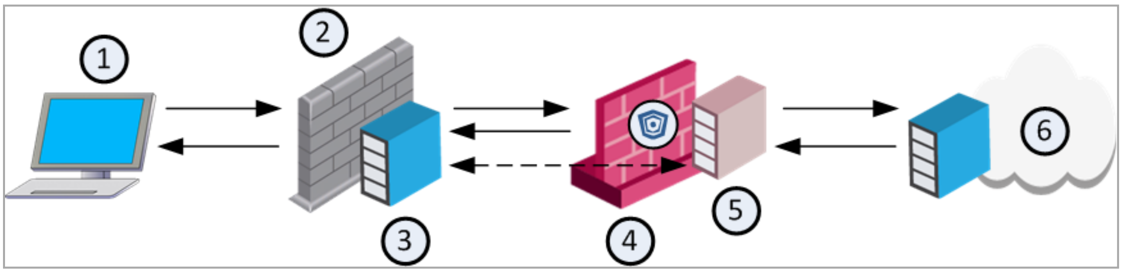
You are a system administrator, who manages a network that includes a third party gateway/proxy and a Check Point Security Gateway.

The Check Point Security Gateway enforces the Threat Emulation and Anti-Virus blades.

The third party gateway/proxy has HTTPS Inspection enabled, but the Check Point Security Gateway does not.

With the ICAP Client and Check Point ICAP Server enabled and configured to work together, the ICAP Client can send the decrypted traffic to the ICAP Server for inspection. This way, the Check Point Security Gateway can read the HTTPS content for the Threat Emulation and Anti-Virus blades, even if no HTTPS Inspection is enabled on the Check Point Security Gateway.

Workflow for ICAP technology in HTTPS Inspection



Item No.	Description
1	HTTPS client
2	Third party gateway or proxy
3	ICAP Client
4	Check Point Security Gateway
5	Check Point ICAP Server
6	Web server

Workflow:

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

Threat Prevention and UserCheck - Custom Threat Prevention

When you enable the UserCheck feature, the Security Gateway sends messages to users about possible non-compliant behavior or dangerous Internet browsing, based on the rules an administrator configured in the Security Policy. This helps users prevent security incidents and learn about the organizational security policy. You can develop an effective policy based on logged user responses. Create UserCheck objects and use them in the Rule Base, to communicate with the users.

These Software Blades support the UserCheck feature:

- Data Loss Prevention
- Access Control:

  - Application Control
  - URL Filtering
  - Content Awareness
- Threat Prevention:
  - Anti-Bot
  - Anti-Virus
  - Threat Emulation
  - Threat Extraction
  - Zero Phishing

Configuring UserCheck on the Security Gateway

Enable or disable UserCheck directly on the Security Gateway. When UserCheck is enabled, the user's Internet browser shows the UserCheck messages in a new window. If users connect to the Security Gateway remotely, set the internal interface of the Security Gateway (on the **Topology** page) to be the same as the **Main URL** for the UserCheck Portal.

To configure UserCheck on a Security Gateway

Step	Instructions
1	Go to the gateway editor, > **UserCheck**, and select **Enable UserCheck for active blades**.
2	In the **UserCheck Web Portal** section: The **Main URL** field shows the primary URL for the web portal that shows the UserCheck notifications. You can use the suggested **Main URL** or manually enter a different **Main URL**.
3	Optional: Click **Aliases** to add URL aliases that redirect different hostnames to the **Main URL**. For example: `Usercheck.mycompany.com` The aliases must be resolved to the portal IP address on the corporate DNS server.

Step	Instructions
4	In the **Certificate** section, click **Import** to import a certificate that the portal uses to authenticate to the Security Management Server. By default, the portal uses a certificate from the Check Point Internal Certificate Authority (ICA). This might generate warnings if the user browser does not recognize Check Point as a trusted Certificate Authority. To prevent these warnings, import your own certificate from a recognized external authority. ⓘ **Note** - After you download your certificate, you can click **Replace** to replace it with a different certificate, and click **View** to see the certificate information.
5	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) - Interfaces used for establishing route-based VPN tunnels (VTIs). ■ **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**
6	**UserCheck Client** - The UserCheck Client is installed on Endpoint devices to communicate with the Security Gateway and show UserCheck Interaction notifications to users. ■ **Activate UserCheck Client support** - This enables UserCheck through the client. ■ Click **Download Client** to download the installation file for the UserCheck Client. ⓘ **Note** - The link is not active until the UserCheck Portal is up. For more information about installation and configuration of the UserCheck Client, see .

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>7</td><td>In the <b>Mail Server</b> section, configure a mail server for UserCheck. This server sends notifications to users that the Security 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 Security Gateway cannot redirect the user to the UserCheck Portal because the traffic is not HTTP.
<b>If the user does not have a UserCheck Client, UserCheck sends an email notification to the user.</b><ul><li><b>Use the default settings</b> - Click the link to see which mail server is configured.</li><li><b>Use specific settings for this gateway</b> - Select this option to override the default mail server settings.</li><li><b>Send emails using this mail server</b> - Select a mail server from the list, or click <b>New</b> and define a new mail server.</li></ul></td></tr>
<tr><td>8</td><td>Click <b>OK</b>.</td></tr>
<tr><td>9</td><td>If there is encrypted traffic through an internal interface, add a new rule to the Firewall Layer of the Access Control Policy.
<b>This is a sample rule</b>
<table>
<tr><th>Source</th><th>Destination</th><th>VPN</th><th>Services & Applications</th><th>Action</th></tr>
<tr><td>Any</td><td>Security Gateway on which UserCheck Client is enabled</td><td>Any</td><td>UserCheck</td><td>Accept</td></tr>
</table></td></tr>
<tr><td>10</td><td>Install the Access Control Policy.</td></tr>
</table>

The Threat Prevention UserCheck Interaction Objects

UserCheck Interaction objects add flexibility and give the Security Gateway a mechanism to communicate with users.

UserCheck Interaction objects:

- Help users with decisions that can be dangerous to the organization security.
- Share the organization's changing internet policy for web applications and sites with users, in real-time.

When UserCheck is enabled, the user's Internet browser shows the UserCheck Interaction messages in a new window.

The UserCheck page contains default UserCheck Interaction messages. You can edit, and preview UserCheck Interaction objects and their messages.

To see the existing UserCheck Interaction objects:

In SmartConsole, go to **Security Policies** > **Threat Prevention** > **Custom Policy Tools** > **UserCheck**.

These are the default UserCheck Interaction objects:

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 the company policy for the specific 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:

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

Creating Threat Prevention UserCheck Objects

To create a UserCheck Interaction object:

Step	Instructions
1	In the **UserCheck** page, click **New**, and then select the object type: - **Ask** Shows a message to users that asks them if they want to continue with the request or not. To continue with the request, the user is expected to supply a reason. - **Inform** Shows an informative message to users. Users can continue to the application or cancel the request. - **Block** Shows a message to users and blocks the application request. The window opens for the new UserCheck object.
2	**Enter Object Name**.
3	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
4	**Optional:** Click **Language** and select one or more languages for the message. The default language for messages is English.
5	Enter the text for the title, subtitle, and body of the message. In **Source** mode, 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. When the Ask User, Inform User, or Block action occurs, the UserCheck Portal and UserCheck Client replaces these variables with applicable values in the message. **Notes -** To resolve the **Username** variable, you must enable the **Identity Awareness**Software Blade and configure the required settings. See the *R81.20 Identity Awareness Administration Guide*. - **Insert User Input** - To insert special fields for user input, such as: Confirm check box, Report Wrong Category and so on, from the top toolbar, click **Insert User Input** and click the applicable option.

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

Step	Instructions
7	You can also click **Settings** from the navigation tree to configure one or more of these options. **Options** ■ **Languages** - Select a language in case the user browser language is not defined. ■ For the Ask and Inform UserCheck Interaction objects, you can select a **Fallback Action** if the user cannot see the message. Select one of these messages: • **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. ■ For an Ask UserCheck Interaction object, you can configure **Conditions**: The UserCheck message can contain these items that require user interaction (shown with sample messages). The traffic is allowed only after the user does the necessary actions. Select one or both options: • **User accepted and selected the confirm checkbox** - User is ignoring the warning and wishes to continue. This applies if on the **Message** page from the **Insert User Input** menu you inserted the element **Confirm Checkbox**. • **User entered the required textual input in the user input field** - The user must enter the reason for ignoring the Threat Prevention warning. This applies if on the **Message** page from the **Insert User Input** menu you inserted the element **Textual Input** **Important** - The traffic or connection is blocked until the user does the necessary actions. ■ **Redirect the user 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. In **External Portal**, enter the URL for the external portal. The 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. Optional: Select **Add UserCheck Incident ID to the URL query** to add an incident ID to the end of the URL query. **Confirmation sent to the gateway**:

Step	Instructions
	• The URL template field points to an XML file. This file should be placed on the external portal so that it can be sent back to the Security Gateway. • The pre-shared secret authenticates the external portal to the Security Gateway.
8	Click **OK**.
9	Install the Threat Prevention policy.

Selecting Approved and Cancel UserCheck Messages

The 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 the Approved Page and Cancel Page:

Step	Instructions
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.

Send Email Notifications in Plain Text

Not all emails clients can handle emails in rich text or HTML format.

To accommodate such clients, you can configure the Security Gateway to send email notification in plain text without images, in addition to the HTML format. The user's email client decides which format to show.

1. Connect to the command line to the Security Gateway / each Cluster Member.
2. Log in to the Expert mode.

3. Back up the configuration file:

   ```
   cp -v $FWDIR/conf/usrchkd.conf{,_BKP}
   ```

4. Edit the configuration file:

   ```
   vi $FWDIR/conf/usrchkd.conf
   ```

5. Change the value of the applicable parameter:

   from

   ```
   :send_emails_with_no_images (false)
   ```

   to

   ```
   :send_emails_with_no_images (true)
   ```

6. Save the changes in the file and exit the editor.
7. Kill the `userchkd` process to load the new configuration:

   ```
   killall userchkd
   ```

   The Security Gateway automatically restarts this process.

UserCheck Client

The UserCheck Client is installed on endpoint computers to communicate with the Security Gateway and show notifications to users.

UserCheck Client sends notifications for applications that are not in a web browser, such as Skype, iTunes, or browser add-ons (such as radio toolbars). The UserCheck Client can also work together with the UserCheck Portal to show notifications on the computer itself in these cases:

- It is not possible to show the notification in a web browser.
- The UserCheck engine determines that the notification does not appear correctly in the web browser.

Notifications of incidents are shown in a pop up from the UserCheck Client in the system tray.

Users select an option in the notification message to respond in real-time.

UserCheck Client Requirements

See the R81.20 Release Notes > *UserCheck Client Requirements*.

Workflow for installing and configuring UserCheck Clients:

1. Open the Security Gateway object.
2. Enable UserCheck and the UserCheck Client in the Security Gateway object. See *UserCheck in the Access Control Policy*.
3. Configure how the UserCheck Clients communicate with the Security Gateway and create trust with it.

   See *"Client and Gateway Communication" on page 334*.
4. Install the UserCheck Client on the endpoint computers.

   See *"Installing UserCheck Client" on page 340*.
5. Connect the UserCheck Client to the Security Gateway.

   See *"Connecting UserCheck Client to the Security Gateway" on page 344*.
6. Make sure the UserCheck Clients can receive notifications.

   Perform a simplest action on the endpoint computers that violates the configured Security Policy.

Client and Gateway Communication

In an environment with UserCheck Clients, the Security Gateway acts as a server for the clients. Each client must be able to *discover* the server and create *trust* with it.

To create trust, the client makes sure that the server is the correct one. It compares the server fingerprint calculated during the SSL handshake with the expected fingerprint. If the server does not have the expected fingerprint, the client asks the user to manually confirm that the server is correct.

Here is a list of the methods that you can use for clients to discover and trust the server.

Option Comparison

Configuration	Must Have AD	Manual User Trust (one time) Necessary?	Multi-Site	Client Stays Signed?	Still works after Gateway Changes	Level	Recommended for...
File name based	No	Yes	No	Yes	No	Very Simple	Single Security Gateway configurations
AD based	Yes	No	Yes	Yes	Yes	Simple	Configurations with AD that you can modify
DNS based	No	Yes	Partially (per DNS server)	Yes	Yes	Simple	Configurations without AD With an AD you cannot change, and a DNS that you can change
Remote registry	No	No	Yes	Yes	Yes	Moderate	Where remote registry is used for other purposes

1. **File name based server configuration**

   If no other method is configured (default, out-of-the-box situation), all UserCheck Clients downloaded from the portal are renamed to have the portal machine IP address in the filename. During installation, the client uses this IP address to connect to the Security Gateway. Note that the user has to click **Trust** to manually trust the server.

Explanation

This option is the easiest to configure, and works out-of-the-box. It tells users to manually click **Trust** to trust the server the first time they connect. You can use this option if your configuration has only one Security Gateway with the relevant Software Blades.

How does it work?

When a user downloads the UserCheck Client, the address of the Security Gateway is inserted in the filename. During installation, the client finds if there is a different discovery method configured (AD based, DNS based, or local registry). If no method is configured, and the Security Gateway can be reached, it is used as the server. In the UserCheck Settings window, you can see that the server you connect to is the same as the Security Gateway in the UserCheck Client filename.

Users must manually make sure that the trust data is valid, because the filename can be easily changed.

Renaming the MSI

You can manually change the name of the MSI file before it is installed on a computer.

This connects the UserCheck Client to a different Security Gateway.

a. Make sure the Security Gateway has a DNS name.

b. Rename the MSI using this format:

   UserCheck_~*GWname*.msi

   Where *GWname* - is the DNS name of the Security Gateway.

   Optional format:

   UserCheck_~*GWname-port*.msi

   Where *port* is the port number of notifications.

   For example:

   ```
   UserCheck_~mygw-18300.msi
   ```

Notes:

- The prefix does not have to be "UserCheck". The important part of the format is underscore tilde (_~), which indicates that the next string is the DNS of the Security Gateway.
- If you want to add the port number for the notifications to the client from the Security Gateway, the hyphen (-) indicates that the next string is the port number.

2. **Active Directory Based Configuration**

If client computers are members of an Active Directory domain, you can configure the server addresses and trust data using a dedicated tool.

Explanation

If your client computers are members of an Active Directory domain and you have administrative access to this domain, you can use the Distributed Configuration tool to configure connectivity and trust rules.

The Distributed Configuration tool has three windows:

- **Welcome** - Describes the tool and lets you enter different credentials that are used to access the AD.
- **Server configuration** - Configure which Security Gateway the client connects to, based on its location.
- **Trusted Security Gateways** - View and change the list of fingerprints that the Security Gateways consider secure.

To enable Active Directory based configuration for clients:

a. Download and install the UserCheck Client MSI on a computer.

From the command line on that computer, run the client configuration tool with the AD utility.

For example, on a Windows 7 computer:

```
"C:\Users\%USERNAME%\Local Settings\Application
Data\Checkpoint\UserCheck\UserCheck.exe" -adtool
```

The **Check Point UserCheck - Distributed Configuration** tool opens.

b. In the **Welcome** page, enter the credentials of an AD administrator.

By default, your AD username is shown. If you do not have administrator permissions, click **Change user** and enter administrator credentials.

c. In the **Server Configuration** page, click **Add**.

The **Identity Server Configuration** window opens.

d. Select **Default** and then click **Add**.

e. Enter the IP address or Fully Qualified Domain Name (FQDN) and the port of the Security Gateway.

f. Click **OK**.

The identity of the AD Server for the UserCheck Client is written in the Active Directory and given to all clients.

Note - The entire configuration is written under a hive named **Check Point** under the **Program Data** branch in the AD database that is added in the first run of the tool. Adding this hive does not affect other AD based applications or features.

Server Configuration Rules

If you use the Distributed Configuration tool and you configure the client to **Automatically discover** the server, the client fetches the rule lists. Each time it must connect to a server, it tries to match itself against a rule, from top to bottom.

When the tool matches a rule, it uses the servers shown in the rule, according to the priority specified.

The configuration in this example means:

a. If the user is coming from `'192.168.0.1 - 192.168.0.255'`, then try to connect to `US-GW1`.

   If it is not available, try `BAK-GS2` (it is only used if `US-GW1` is not available, as its priority is higher).

b. If the user is connected from the Active Directory site `'UK-SITE'`, connect either to `UK-GW1` or `UK-GW2` (select between them randomly, as they both have the same priority). If both of them are not available, connect to `BAK-GS2`.

c. If rules 1 and 2 do not apply, connect to `BAK-GS2` (the default rule is always matched when it is encountered).

Use the **Add**, **Edit** and **Remove** buttons to change the server connectivity rules.

Trusted Gateways

The **Trusted Gateways** window shows the list of servers that are trusted - no messages open when users connect to them.

You can add, edit or delete a server. If you have connectivity to the server, you can get the name and fingerprint. Enter its IP address and click **Fetch Fingerprint** in the **Server Trust Configuration** window. If you do not have connectivity to the server, enter the same name and fingerprint that is shown when you connect to that server.

3. **DNS SRV Record Based Server Discovery**

   Configure the server addresses in the DNS server. Note that the user has to click **Trust** to manually trust the server.

Explanation

If you configure the client to **Automatic Discovery** (the default), it looks for a server by issuing a DNS SRV query for the address of the Security Gateway (the DNS suffix is added automatically). You can configure the address in your DNS server.

To configure DNS based configuration on the DNS server:

a. Go to **Start** > **All Programs** > **Administrative Tools** > **DNS**.

b. Go to **Forward lookup zones** and select the applicable domain.

c. Go to the **_tcp** subdomain.

d. Right-click and select **Other new record**.

e. Select **Service Location**, **Create Record**.

f. In the **Service** field, enter **CHECKPOINT_DLP**.

g. Set the **Port number** to 443.

h. In **Host offering this server**, enter the IP address of the Security Gateway.

i. Click **OK**.

To configure Load Sharing for the Security Gateway, create multiple SRV records with the same priority.

To configure High Availability, create multiple SRV records with different priorities.

Note - If you configure AD based and DNS based configuration, the results are combined according to the specified priority (from the lowest to highest).

Troubleshooting DNS Based Configuration

To troubleshoot issues in DNS based configuration, you can see the SRV records that are stored on the DNS server.

To see SRV records on the DNS server:

Run:

```
C:\> nslookup
 > set type=srv
 > checkpoint_dlp._tcp
```

Example result:

```
C:\> nslookup
 > set type=srv
 > checkpoint_dlp._tcp
Server: dns.company.com
Address: 192.168.0.17
checkpoint_dlp._tcp.ad.company.com SRV service location:
          priority = 0
          weight = 0
          port = 443
          svr hostname = dlpserver.company.com
dlpserver.company.com internet address = 192.168.1.212
>
```

Remote Registry

All of the client configuration, including the server addresses and trust data reside in the registry. You can configure the values before installing the client (by GPO, or any other system that lets you control the registry remotely). This lets you use the configuration when the client is first installed.

Explanation

If you have a way to configure registry entries to your client computers, for example, Active Directory or GPO updates, you can configure the Security Gateway addresses and trust parameters before you install the clients. Clients can then use the configured settings immediately after installation.

To configure the remote registry option:

1. Install the client on one of your computers. The agent installs itself in the user directory, and saves its configuration to `HKEY_CURRENT_USER`.
2. Connect manually to all of the servers that are configured, verify their fingerprints, and click **Trust** on the fingerprint verification dialog box.
3. Configure the client to manually connect to the requested servers (use the **Settings** window).
4. Export these registry keys:
   a. The entire tree:

      `HKEY_CURRENT_USER\SOFTWARE\CheckPoint\UserCheck\Trusted Gateways`

b. The branch:

`HKEY_CURRENT_USER\SOFTWARE\CheckPoint\UserCheck\`

i. The key:

`Default Gateway`

ii. The key:

`DefaultGatewayEnabled`

5. Import the exported keys to the endpoint computers before you install the UserCheck Client.

Installing UserCheck Client

After configuring the clients to connect to the Security Gateway, install the clients on the user machines.

1. Get the UserCheck Client MSI file from the Security Gateway in **one** of these ways:

Download the UserCheck Client from the Security Gateway using an SCP client

Important - The SCP user must have the default shell `/bin/bash` in Gaia OS on the Security Gateway.

a. Go to this directory:

```
/opt/CPUserCheckPortal/htdocs/UserCheck/client/
```

b. Download this file:

```
Check_Point_UserCheck.msi
```

Download the UserCheck Client from the Security Gateway object in SmartConsole

Important - Before you can use this link, you must install an Access Control policy at least one time so that the UserCheck Portal starts.

a. From the left navigation panel, click **Gateways & Servers**.

b. Double-click the Security Gateway object.

c. From the left tree, click **General Properties**.

d. Enable at least one of these Software Blades:

  - Data Loss Prevention
  - Access Control:
    - Application Control
    - URL Filtering
    - Content Awareness
  - Threat Prevention:
    - Anti-Bot
    - Anti-Virus
    - Threat Emulation
    - Threat Extraction
    - Zero Phishing

e. From the left tree, click **UserCheck**.

f. In the section **UserCheck Client**, click the link **Download Client**.

g. The download opens in your default web browser.

2. Install the UserCheck Client on the user endpoint computers.

   You can use any method of MSI mass configuration and installation that you select.

   For example, you can send users an email with a link to install the client. When a user clicks the link, the MSI file automatically installs the client on the computer.

   Notes:
   - The installation is silent.
     Reboot is not necessary.
   - To install the UserCheck Client for all user accounts on a Windows computer, see sk96107.
   - To uninstall the UserCheck Client from a Windows computer, see *"Uninstalling UserCheck Client" on page 342*.

Uninstalling UserCheck Client

Default Uninstall Procedure

1. Go to the **Start** menu > **Check Point** > **UserCheck**.
2. Click the "**Uninstall**" shortcut.

3. Follow the instructions on the screen.
4. Restart the endpoint computer.

Manual Uninstall Procedure

If there is no "**Uninstall**" shortcut in the **Start** menu, follow **one** of these procedures:

Uninstall the UserCheck Client manually using Windows Installer

1. Make sure the **UserCheck.exe** application is not running.

   Use Windows Task Manager, or any similar 3rd-party tool.

   If it is currently running, end / kill it.

2. Get the UserCheck Client GUID from the Windows Registry Editor:

   a. Open the Windows Registry Editor (**regedit**):

      i. Click the **Start** menu.

      ii. Enter **regedit**.

      iii. Click **Registry Editor**.

      Alternatively, press the **Windows + R** keys > type **regedit** > click OK / press the Enter key.

   b. Navigate to:

      ```
      Computer\HKEY_CURRENT_
      USER\Software\CheckPoint\UserCheck\1.0
      ```

   c. Right-click the key **PRODUCT_GUID** > click **Modify**.

   d. Copy the entire string **{<GUID>}** and paste it in a plain-text editor.

   e. Click **Cancel** in the Windows Registry Editor.

   f. Close the Windows Registry Editor.

3. In the plain-text editor, prepare the required syntax:

   ```
   %SystemRoot%\SysWOW64\msiexec.exe /x {<GUID you copied from
   Windows Registry Editor>}
   ```

   Dummy example:

   ```
   C:\Windows\SysWOW64\msiexec.exe /x {AAD3D77A-7476-469F-ADF4-
   04424124E91D}
   ```

Reference:

https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/msiexec

4. Open Windows Command Prompt:
   a. Click the **Start** menu.
   b. Enter **cmd**.
   c. Click **Command Prompt**.

   Alternatively, press the **Windows + R** keys > type **cmd** > click OK / press the Enter key.
5. Paste the required syntax from the plain-text editor and press the Enter key.
6. Restart the endpoint computer.

Delete the UserCheck client manually from the endpoint computer

1. Make sure the **UserCheck.exe** application is not running.

   Use Windows Task Manager, or any similar 3rd-party tool.

   If it is currently running, end / kill it.
2. Delete the **UserCheck** folder:

   Important - You must delete this folder for each user on the computer.

   a. In Windows File Manager (or any file manager), go to:

      ```
      C:\Users\%USERNAME%\AppData\Local\CheckPoint\
      ```
   b. Delete this folder:

      ```
      UserCheck
      ```
3. Delete the **UserCheck** branch in the Windows Registry:
   a. Open the Windows Registry Editor (**regedit**):
      i. Click the **Start** menu.
      ii. Enter **regedit**.
      iii. Click **Registry Editor**.

      Alternatively, press the **Windows + R** keys > type **regedit** > click OK / press the Enter key.

b. Navigate to:

```
Computer\HKEY_CURRENT_
USER\Software\CheckPoint\UserCheck
```

c. Back up the Windows Registry.

Refer to the Microsoft article "Windows registry information for advanced users".

d. Right-click the **UserCheck** branch > click **Delete** > confirm.

e. Close the Windows Registry Editor.

4. Restart the endpoint computer.

Connecting UserCheck Client to the Security Gateway

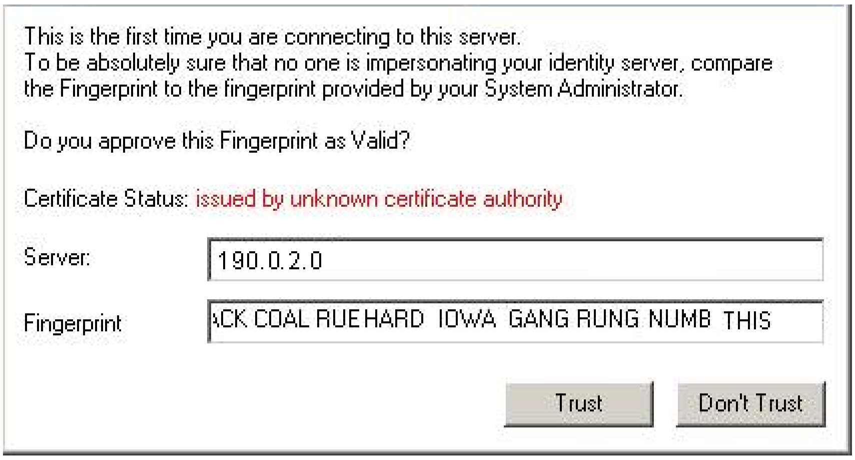
If UserCheck for DLP is enabled on the Security Gateway, users must enter their username and password after the client installs.

When the UserCheck Client is first installed, the UserCheck Client tray icon indicates that it is not connected.

When the UserCheck Client connects to the Security Gateway, the UserCheck Client tray icon shows that the client is active.

The first time that the UserCheck Client connects to the Security Gateway, it asks user to approve of the Security Gateway fingerprint.

Example:



This is the first time you are connecting to this server.
To be absolutely sure that no one is impersonating your identity server, compare the Fingerprint to the fingerprint provided by your System Administrator.

Do you approve this Fingerprint as Valid?

Certificate Status: issued by unknown certificate authority

Server: 190.0.2.0

Fingerprint ACK COAL RUE HARD IOWA GANG RUNG NUMB THIS

Best Practices:

- Let the users know this happens.
- Use a certificate that is trusted by the certificate authority installed on users' computers.
  Then users do **not** see a message "`Issued by unknown certificate authority`".

Example of message to users about the UserCheck Client installation (for DLP):

```
Dear Users,
Our company has implemented a Data Loss Prevention automation to
protect our confidential data from unintentional leakage. Soon you
will be asked to verify the connection between a small client that
we will install on your computer and the computer that will send
you notifications.
This client will pop up notifications if you try to send a message
that contains protected data. It might let you to send the data
anyway, if you are sure that it does not violate our data-security
guidelines.
When the client is installed, you will see a window that asks if
you trust the DLP server. Check that the server is SERVER NAME and
then click Trust.
In the next window, enter your username and password, and then
click OK.
```

Note - If the UserCheck Client is not connected to the Security Gateway, the behavior is as if the client was never installed. Email notifications are sent for SMTP incidents and the Gaia Portal is used for HTTP incidents.

UserCheck and Check Point Password Authentication

To enable Check Point password authentication:

1. SmartConsole Configuration:
    a. From the top, click **Objects** > **Object Explorer**.
    b. In the left pane, select only **Users/Identities**.
    c. Configure the required settings:

        If the required User object already exists

        i. Double-click the applicable **User** object.
        ii. From the left, click **General**.
        iii. In the **General properties** section, make sure to configure a valid email address.
        iv. Click **OK**.

        If the required User object does not exist yet

        i. Make sure the applicable **User Template** object exists.

            If it does not, from the top toolbar, click **New** > **Users/Identity** > **User Template** > configure the required settings > click **OK**.

        ii. From the top toolbar, click **New** > **Users/Identity** > **User**.
        iii. Select the required **User Template** and click **OK**.
        iv. Configure the required settings:
            - At the top, configure the object name
            - On **General** page, in the **General properties** section, make sure to configure a valid email address.
            - On **Authentication** page, in the **Authentication Method** section, select **Check Point Password** > click **Set new password** > enter the password > click **OK**.
        v. Click **OK**.
    d. Close the **Object Explorer** window.
2. UserCheck Client Configuration:

a. On the endpoint computer, right-click the UserCheck Client icon in the Notification Area (next to the system clock).

b. Click **Settings**.

c. Click **Advanced**.

d. Select **Authentication with Check Point user accounts defined internally in SmartConsole**.

Helping Users

If users require assistance to troubleshoot issues with the UserCheck Client, you can ask them to send you the logs.

To configure the UserCheck Client to generate logs:

1. Right-click the UserCheck Client tray icon and select **Settings**.
2. Click **Log to** and browse to a pathname where the logs are saved.
3. Click **OK**.
4. Make sure that the UserCheck Clients can connect to the Security Gateway and receive notifications.

   See *"Connecting UserCheck Client to the Security Gateway" on page 344*.

To send UserCheck Client logs from the endpoint computer:

1. Right-click the UserCheck Client tray icon and select **Status**.
2. Click **Advanced**.
3. Click the link **Collect information for technical support**.

   The default email client opens, with an archive of the collected logs attached.

Localizing and Customizing the UserCheck Portal

For more information, see sk83700.

Monitoring Threat Prevention - Custom Threat Prevention

Networks today are more exposed to cyber-threats than ever. This creates a challenge for organizations in understanding the security threats and assessing damage. SmartConsole helps the security administrator find the cause of cyber-threats, and remediate the network.

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

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

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

Log Sessions

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

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

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

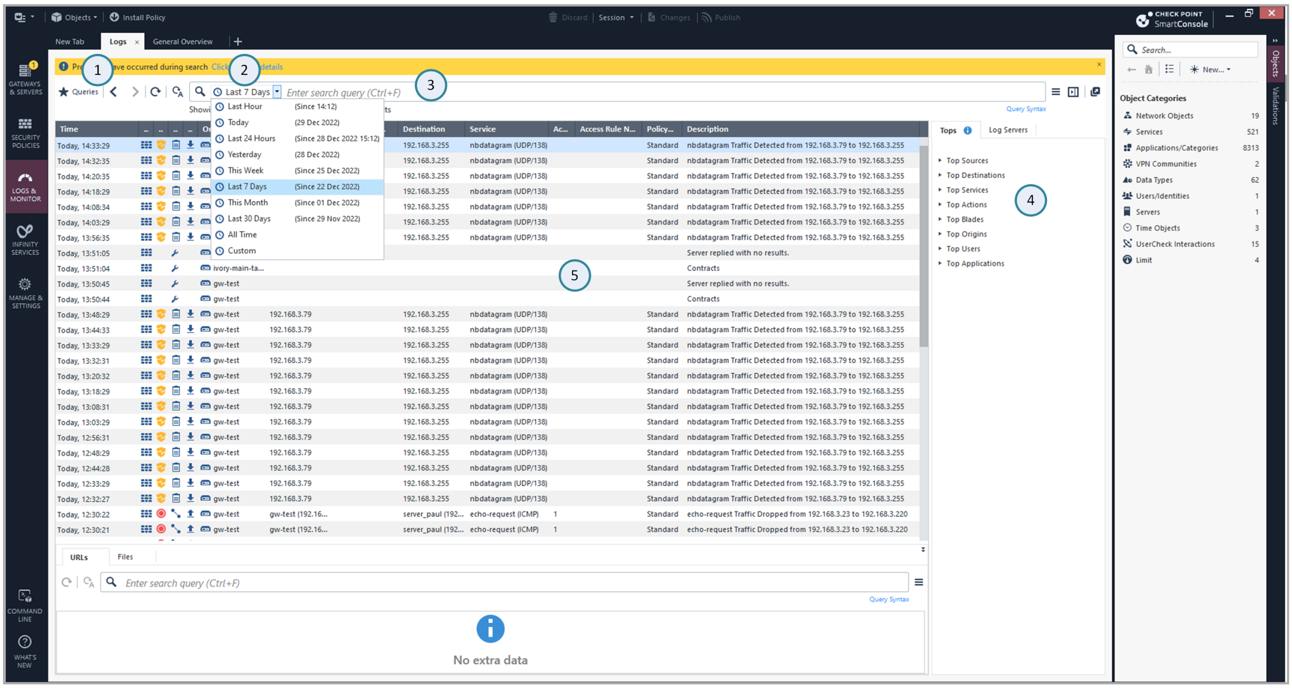
Using the Log View

In SmartConsole

Step	Instructions
1	Go to **Logs and Monitoring** > **View**.
2	Click **New**, and then select **New View**.

Step	Instructions
3	In the **New View** window, enter: ■ **Name** ■ **Category** - For example, select **Access Control** ■ **Description** - (optional)
4	In the new window that opens, create a query. Click **Options** > **View Filter** and select **Blade and App control**.
5	To customize how you see the data that comes back from the query, click **Add Widget**. Start with a Timeline of all events. In **Table**, you can create a table that contains multiple field such as user, application name, and the amount of traffic. Additional widgets for use: map, infographic, rich text, chart, and container (for multiple widgets). After you save the changes in SmartConsole, you can schedule and get an automatic email at multiple intervals.

This is an example of the Log view:



Time	Or		Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 14:33:29			192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 14:32:35			192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 14:20:35			192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 14:18:29			192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 14:08:34			192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 14:03:29			192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:56:35			192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:51:05								Server replied with no results.
Today, 13:51:04	ivory-main-ta...							Contracts
Today, 13:50:45	gw-test							Server replied with no results.
Today, 13:50:44	gw-test							Contracts
Today, 13:48:29	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:44:33	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:33:29	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:32:31	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:20:32	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:18:29	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:08:31	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:03:29	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 12:56:31	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 12:48:29	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 12:44:28	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 12:33:29	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 12:32:27	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 12:30:22	gw-test	gw-test (192.16...	server_paul (192...	echo-request (ICMP)	1		Standard	echo-request Traffic Dropped from 192.168.3.23 to 192.168.3.220
Today, 12:30:21	gw-test	gw-test (192.16...	server_paul (192...	echo-request (ICMP)	1		Standard	echo-request Traffic Dropped from 192.168.3.23 to 192.168.3.220

Item	Description
1	**Queries** - Predefined and favorite search queries.
2	**Time Period** - Search with predefined custom time periods.

Item	Description
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

Step	Instructions
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.

Example

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

Creating Custom Queries

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

To modify a predefined query:

Click inside the query box to add search filters.

To save the new query in the Favorites list

Step	Instructions
1	Click **Queries** > **Add to Favorites**. The **Add to Favorites** window opens.
2	Enter a name for the query.
3	Select or create a new folder to store the query.
4	Click **Add**.

Selecting Criteria from Grid Columns

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

To select query criteria from grid columns

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

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

Manually Entering Query Criteria

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

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

Selecting Query Fields

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

To select field criteria

Step	Instructions
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.

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 at a later time.

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

To deactivate packet capture (in the Threat Prevention only)

Step	Instructions
1	In SmartConsole > **Security Policies** view > **Threat Prevention** > **Custom Policy**.
2	Go to the required rule and right-click the **Track** column.
	Clear the **Packet Capture** option.

To see a packet capture

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

Advanced Forensics Details

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

To disable the Advanced Forensics Details feature

Step	Instructions
1	In SmartConsole > go to **Security Policies** > **Threat Prevention** > **Custom Policy**.
2	Go to the required rule and select right-click the **Track** column.
3	Clear the **Forensics** option.

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

Example

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

Threat Analysis in the Logs & Monitor View

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

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

Available options

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

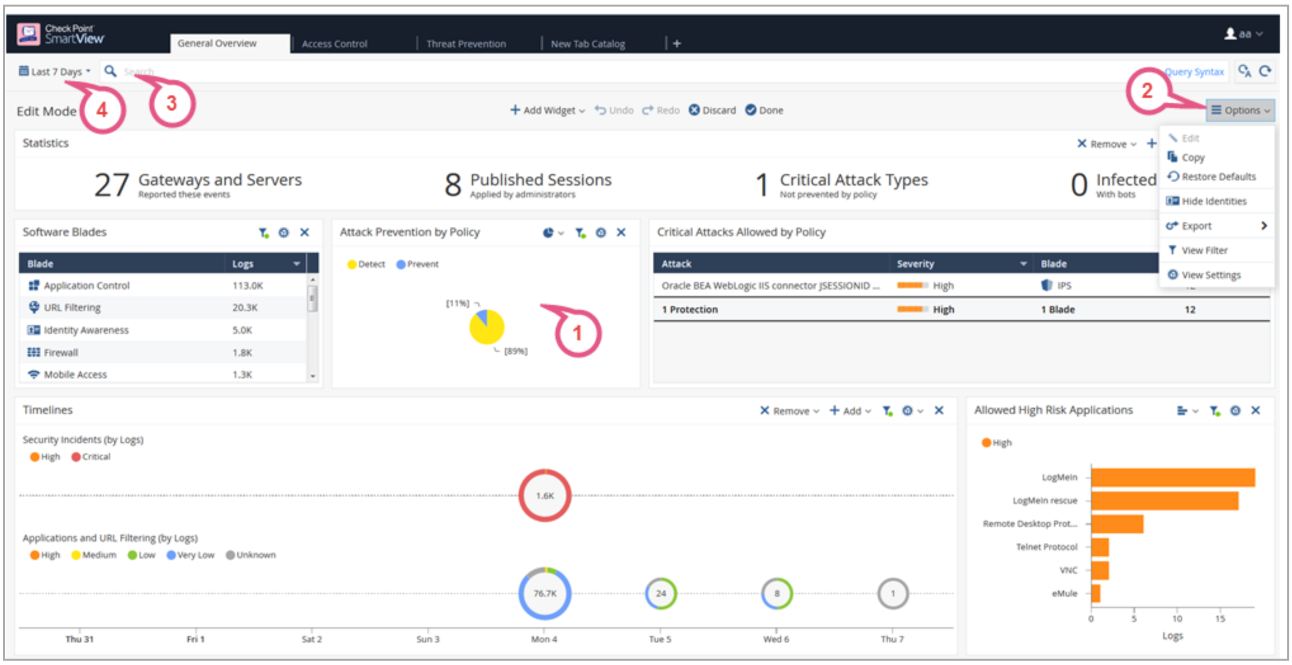
Views

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

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

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

Example View window



Blade	Logs
Application Control	113.0K
URL Filtering	20.3K
Identity Awareness	5.0K
Firewall	1.8K
Mobile Access	1.3K

Attack	Severity	Blade	
Oracle BEA WebLogic IIS connector JSESSIONID ...	High	IPS	
1 Protection	High	1 Blade	12

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

For more information on using and customizing reports, see the *R81.20 Logging and Monitoring Administration Guide*.

Reports

A report consists of multiple views and a cover page. There are several predefined reports, and you can create new reports. A report gives more details than a view. Reports can be customized, filtered, generated and scheduled. You cannot drill down into a report.

Click the (+) tab to open a catalog of all views and reports, predefined and customized. To open a report, double-click the report or select the applicable report and click **Open**.

For more information on using and customizing reports, see the *R81.20 Logging and Monitoring Administration Guide*

Log Fields

See *"Log Fields" on page 496*.

How to Investigate Threat Prevention Events

- *"Cyber Attack View - Gateway" on page 433*
- *"MITRE ATT&CK" on page 490*

Threat Prevention Scheduled Updates - Custom Threat Prevention

Introduction to Scheduled Updates

Check Point wants the customer to be protected. When a protection update is available, Check Point wants the configuration to be automatically enforced on the gateway. You can configure automatic gateway updates for Anti-Virus, Anti-Bot, Threat Emulation and IPS.

For Anti-Virus, Anti-Bot and Threat Emulation, the gateways download the updates directly from the Check Point cloud.

For IPS, prior to R80.20, the updates were downloaded to the Security Management Server, and only after you installed policy, the gateways could enforce the updates. Starting from R80.20, the gateways can directly download the updates. For R80.20 gateways and higher with no internet connectivity, you must still install policy to enforce the updates.

When you configure automatic IPS updates on the gateway, the action for the newly downloaded protections is by default according to the profile settings.

IPS, Anti-Virus and Anti-Bot updates are performed every two hours by default. Threat Emulation engine updates are performed daily at 05:00 by default, and Threat Emulation image updates are performed daily at 04:00 by default.

You can see the list of Anti-Bot and Anti-Virus protections in **Custom Policy Tools** > **Protections**, and the list of IPS protections in **Custom Policy Tools > IPS Protections**. The update date appears next to each protection.

Configuring Threat Prevention Scheduled Updates

To configure Threat Prevention scheduled updates

In SmartConsole, go to **Security Policies** > **Threat Prevention** > **Custom Policy** > **Custom Policy Tools**

Step	Instructions
1	Go to **Updates**.
2	Go to the section about the required Software Blade, click **Schedule Update**. The **Scheduled Updates** window opens.
3	Make sure **Enable <blade> scheduled updates** is selected.

Step	Instructions
4	**For IPS, there are 2 more configuration options for scheduling Security Management Server updates** ■ **On successful IPS update on the Security Management Server, install policy on the Security Gateway** - automatically installs the policy on the devices you select after the IPS update is completed. Click **Configure** to select these devices. **Note** - In pre-R80gateways, IPS was part of the Access Control policy. Therefore, when you select this option, a message shows which indicates that for pre-R80 gateways, the Access Control policy is installed and for R80 and above gateways, the Threat Prevention policy is installed. ■ **Perform retries on the Security Management Server when the update fails** - lets you configure the number of tries the scheduled update makes if it does not complete successfully the first time.
5	Click **Configure**.
6	**In the window that opens, set the Time of event** ■ **Update every**: set the update frequency by hours OR - ■ **Update at**: set the update frequency by days: • **Daily** - Every day • **Days in week** - Select days of the week • **Days in month** - Select dates of the month
7	Click **OK**.
8	Click **Close**.
9	Install the Threat Prevention policy.

Checking Update Status

In **Custom Policy Tools** > **Update**, a message shows which indicates the number of gateways which are up-to-date.

To check if the protections are update on a specific gateway

Step	Instructions
1	In the **Gateways & Servers** view, select a gateway.

Step	Instructions
2	Right-click the gateway, and select the **Monitor** button. The **Device & License Information** window opens.
3	The **Device Status** page shows the gateway status.

Turning Off IPS Automatic Updates on a Gateway

You can turn off automatic IPS updates on a specific gateway.

To turn off automatic IPS updates on a specific gateway

Step	Instructions
1	In SmartConsole, to the **Gateways & Servers** view, and double-click a gateway. The gateway properties window opens.
2	In the navigation tree, go to **IPS**.
3	In **IPS Update Policy**, select **Use IPS management updates**.
4	Click **OK**.
5	Install the Threat Prevention Policy.

IPS Updates Use Cases

These scenarios explain how an upgrade of the Security Gateways or the Security Management Server or both, affects the Scheduled Updates configuration.

Scenario 1:

Upgrading the Security Management Server to R80.20, and not upgrading the gateways to R80.20

If you do not upgrade the Security Gateways, then after the upgrade, the Security Gateways are still not able to receive the updates independently, only through the Security Management Server. In this case, the configuration stays the same compared to before the upgrade: Scheduled Updates will be enabled or disabled on the Security Management Server, depending on the configuration before the upgrade.

Scenario 2:

Upgrading the Security Gateways to R80.20 (with or without Security Management Server upgrade)

- If, before the upgrade, Scheduled Updates were configured on the Security Management Server with automatic policy installation, then after the upgrade, automatic IPS updates are still enabled on the Security Management Server, and are also applied to the upgraded gateways.
- If Scheduled Updates were disabled on the Security Management Server before the upgrade, then they remain disabled after the upgrade, both on the Security Management Server and the gateways.
- If, before the upgrade, Scheduled Updates were configured on the Security Management Server without automatic policy installation - then during the first policy installation after upgrade, a message shows which indicates that Security Gateways R80.20 and higher automatically update the IPS Protections. For Security Gateways R80.10 and lower, you must install policy to apply the updates.

SSH Deep Packet Inspection - Custom Threat Prevention

You can use the SSH Deep Packet Inspection ("SSH DPI") feature to decrypt and encrypt SSH traffic and let the Threat Prevention solution protect against advanced threats, bots, and other malware.

Key Motivation and Goals for SSH DPI

- Block SSH attacks
- Block the transmission of viruses through SCP and SFTP protocols
- Prevent brute force password cracking of SSH/SFTP servers
- Prevent the dangerous use of SSH Port forwarding
- Prevent using simple passwords like "password" when connecting to SSH/SFTP
- Prevent using vulnerable cryptography
- Prevent using vulnerable SSH clients and servers
- Prevent using port 22 for other protocols except for SSH

Note - Currently, these blades are supported: Anti-Virus, IPS and Threat Emulation.

SSH DPI Architecture

Similar to HTTPS Inspection, SSH DPI works as the man-in-the-middle.

```
SSH_CLIENT <=> Security Gateway <=> SSH_SERVER
```

Note - All TCP traffic should pass through the Security Gateway.

Enabling SSH Deep Packet Inspection on the Security Gateway

To enable SSH DPI

1. On the Security Gateway, Run:

```
cpssh_config ion
```

2. Run this command:

```
fw fetch local
```

Or install the Access Control policy in SmartConsole

Disabling SSH Deep Packet Inspection on the Security Gateway

To disable SSH DPI

On the Security Gateway, run:

```
cpssh_config ioff
```

Viewing SSH DPI Status

To view the status of SSH DPI

On the Security Gateway, run:

```
cpssh_config istatus
```

Note - All SSH inspection settings will be saved after Security Gateway reboot.

Configuring SSH Deep packet Inspection

Add an inspected SSH server

To add a non-transparent inspected SSH sever

Note - The Security Gateway introduces the Server to the Client with a new public key.

Step	Instructions
1	Copy the SSH server's public key to the Security Gateway **Note** - In Linux, the key on the Security Gateway is `/etc/ssh/ssh_host_rsa_key.pub`

2	On the Gateway, run this command:
	`cpssh_config -s -g SERVER_NAME -e /PATH/TO/RSA/KEY/THAT/YOU/COPIED.pub`
	For example:
	If your ssh sever host is `my_ssh_server_host.com`, and you copy the key to `/home/admin/mykey.pub`, then you must run this command:
	`cpssh_config -s -g my_ssh_server_host.com -e /home/admin/mykey.pub`

Step	Instructions
3	Repeat steps 1 and 2 for every SSH server to be added.

To add a transparent inspected SSH sever

Note - The Security Gateway introduces the Server to the Client with the original public key.

Step	Instructions
1	Copy the SSH server's public and private key to the Security Gateway. **Note** - The keys on the Security Gateway are: - `/etc/ssh/ssh_host_rsa_key.pub` - `/etc/ssh/ssh_host_rsa_key`

2	Run this command:
	`cpssh_config -s -a <SERVER_NAME> -e </PATH/TO/RSA/KEY/THAT/YOU/COPIED>.pub -i </PATH/TO/RSA/PRIVATE_KEY/THAT/YOU/COPIED>.pub`
	For example:
	If your ssh sever host is `my_ssh_server_host.com` and you copy the keys to `/home/admin/mykey.pub`, then you must run this command:
	`cpssh_config -s -a my_ssh_server_host.com -e /home/admin/mykey.pub -i /home/admin/mykey`

3	Repeat steps 1 and 2 for every SSH server to be added.

To disable SSH port forwarding

On the Security Gateway, run:

```
cpssh_config -w Global -y Port_fowarding_Enabled -u 0
```

To run SSH DPI on a non-standard port (not TCP port 22)

Step	Instructions
1	In SmartConsole, from the right panel, select **Objects** > **Services**.
2	Right-click on the **TCP**, and then choose **NEW TCP**.

Step	Instructions
3	Enter a name for the new TCP service: 1. Select **General** > **Protocol** as **SSH2**. 2. Choose **Match By** > **Customize to new port**, and then set the port. For example, `22222`
4	Install the Access Control Policy.

To configure IPS package installation

Step	Instructions
1	In SmartConsole, enable the IPS Software Blade in the Security Gateway object.
2	Enable the IPS Software Blade in the corresponding Threat Prevention policy.
3	Install Threat Prevention Policy.

To configure the Anti-Virus inspection for SSH

Step	Instructions
1	In SmartConsole, enable the Anti-Virus Software Blade in the Security Gateway object.
2	Enable Anti-Virus Software Blade in the corresponding Threat Prevention policy.
3	Install Threat Prevention Policy.

SSH Deep Packet Inspection Settings

To view all settings

```
cpssh_config -q
```

To view available options for key exchange

On the Security Gateway, run:

```
cpssh_config -w KeyExchange
```

To view available options for cipher

On the Security Gateway, run:

```
cpssh_config -w Cipher
```

To view available options for MAC

On the Security Gateway, run:

```
cpssh_config -w Mac
```

To view available options for Hostkey

On the Security Gateway, run:

```
cpssh_config -w Hostkey
```

To set option

On the Gateway, run:

```
cpssh_config -w Cipher -y <OPTION> -u <VALUE>
```

For example, to disable `aes128-cbc`:

```
cpssh_config -w Cipher -y aes128-cbc -u 0
```

Client Authorization (authorization by keys - without passwords)

To enable client authorization

Step	Instructions
1	Configure the SSH server to do the authorization through keys. This is done by copying the public key from the client to the server in `~/.ssh/authorized_keys/`. For more details, see askubuntu.com.
2	Copy SSH client public and private keys (`mykey.pub` and `mykey`) to the Security Gateway.
3	Copy the SSH server public key (`serverkey.pub`) to the Security Gateway.

Step	Instructions
4	Run this command: `cpssh_config -c -a <admin_username>@<my_ssh_server> -e /home/admin/mykey.pub -l /home/admin/serverkey.pub -i /home/admin/mykey` Where: ■ `admin_username` is the username on the SSH server ■ `my_ssh_server` is the resolvable hostname of IP address of the SSH server ■ `mykey.pub` and `mykey` are pairs of client keys

Cluster

Currently, we do not support keys syncing between cluster nodes automatically.

To manually sync the Cluster Members (after adding/modify/deleting keys)

On the Cluster Member, on which the keys were added, run these commands in the Expert mode:

```
cd /etc/
tar -cvvf ssh.tar ssh
scp ssh.tar admin@<IP_OF_OTHER_CLUSTER_MEMBER>:/tmp
```

On the other cluster members, run these commands in the Expert mode:

```
mv -v /tmp/ssh.tar /etc/
cd /etc/
mv -v ssh ssh_backup
tar -xvvf ssh.tar
killall -s HUP cpsshd
```

Troubleshooting

To make sure that SSH DPI is enabled

Connect to an SSH server with the `telnet` command.

The output should show "**SSH-2.0-cpssh**"

Example:

```
$ telnet 172.23.43.29 22
Trying 172.23.43.29...
Connected to 172.23.43.29.
Escape character is '^]'.
SSH-2.0-cpssh
```

Debugging

To collect Kernel Debug

1. Enable the debug flag "`cpsshi`" in the kernel debug module "`fw`".
2. Enable all the debug flags in the kernel debug module "`CPSSH`".

For instructions on the debugging procedures, see the *R81.20 Quantum Security Gateway Guide* > Chapter *Kernel Debug on Security Gateway*.

To collect User Space Debug

1. Create and then run this shell script:

   ```
   #!/bin/sh
   echo > $FWDIR/log/cpsshd.elg
   for PROC in $(pidof cpsshd)
   do
       fw debug $PROC on ALL=6
   done
   tail -f $FWDIR/log/cpsshd.elg
   ```

   To stop the output, press the **CTRL+C** keys.
2. Replicate the issue, or wait for it to occur.
3. Disable the User Space logs with this command:

   ```
   for PROC in $(pidof cpsshd) ; do fw debug $PROC off ALL=6 ;
   done
   ```
4. Examine the log files:

   ```
   $FWDIR/log/cpsshd.elg*
   ```

The Check Point ThreatCloud - Custom Threat Prevention

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-VirusSoftware 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.

You can access the ThreatCloud repository from ThreatWiki: In a web browser, go to *Check Point ThreatWiki*.

- In SmartConsole, go to **Security Policies** > **Threat Prevention** > **Custom Policy** > in the **Custom Policy Tools** section, click **ThreatWiki**.

SmartConsole - You can add specific malwares to rule exceptions when necessary.

1. In SmartConsole, go to **Security Policies** > **Threat Prevention** > **Custom Policy**.
2. Add an exception.
3. In the **Protection** column in the rule exception, click the plus sign.
4. Near the applicable protections, click the plus sign.

Data which Check Point Collects

When you enable information collection, the Check Point Security Gateway collects and securely submits event IDs, URLs, and external IP addresses 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 PointSecurity Gateway. It includes the event ID, URL, and external IP addresses. Note that the data does not contain confidential data or internal resource information. The source IP address is obscured. Information sent to the Check Point Lab is stored in an aggregated form.

Configuring Check Point ThreatCloud on a Gateway

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

Step	Instructions
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: 1. From the navigation tree click **Anti-Bot and Anti-Virus**. The **Anti-Bot and Anti-Virus** page opens. 2. To configure a Security Gateway to share Anti-Bot and Anti-Virus information with the ThreatCloud, select **Support the global community by sharing attack data with Check Point ThreatCloud**. - If you do not select this check box, no information is shared with Check Point about the attack. If you select this checkbox, you can select which information is exposed about the attack: ▪ **Receive alerts about threats (requires sharing additional end-user data)** - all attack information is exposed. ▪ **Anonymize collected data** (selected by default). Select one of these options: • **End-user data** (selected by default) - End-user information is anonymized, gateway is exposed. • **End-user data and customer identity** - both end-user and gateway data are hidden.

Step	Instructions
3	Configure the settings for IPS: 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**. **Note** - To disable sharing IPS information with the Check Point cloud, clear this option.
4	Click **OK**.

Check Point ThreatCloud Network

Check Point ThreatCloud is a dynamically updated service that is based on an innovative global network of threat sensors and organizations that share threat data and collaborate to fight against modern malware. Customers can send their own threat data to the ThreatCloud and receive protection updates with enriched threat intelligence.

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

When you send files to the ThreatCloud service for emulation, your network gets up-to-date threat information and operating system environments. The connection to the ThreatCloud is enabled by default. This connection gives many management features. We recommend to enable it. If you want to block this connection, you can change the default setting.

To block ThreatCloud

Step	Instructions
1	From the menu bar, click **Global Properties**.
2	In the navigation tree, go to **Data Access Control**
3	Clear: **Help Check Point Improve the product by sending anonymous information**.
4	Publish the SmartConsole session.
5	Restart SmartConsole.
6	Install the Policy.

Troubleshooting - Custom Threat Prevention

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

Step	Instructions
1	Make sure the Security 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. 1. Connect to the command line on the Security Gateway. 2. Log in to the Expert mode. 3. Connect with Telnet to port 25 of the designated Mail Transfer Agent.

Threat Extraction fails to extract threats from emails

Step	Instructions
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 stopped receiving emails

Step	Instructions

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 Security 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 the scrub daemon, 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`
	Important - When empty the queue, you lose 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 Security 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.

Step	Instructions
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 Security 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 Security Gateway:

Step	Instructions

1	Make sure that the disk or directories on the Security Gateway are not full.
	1. Run:
	`df -h /`
	2. Run:
	`df -h /var/log`

2	Make sure directories used by Threat Extraction can be written to. Run: 1. `touch /tmp/scrub/test` 2. `touch /var/log/jail/tmp/scrub/test` 3. `touch $FWDIR/tmp/email_tmp/test`

CPView shows Threat Extraction errors

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

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**.

Step	Instructions
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:

Step	Instructions
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

Step	Instructions
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 VSX Virtual System

Step	Instructions
1	Connect to the command line on the VSX Gateway.

Step	Instructions
2	Log in to Gaia Clish.
3	Go to the context of the applicable Virtual System: `vsenv <VSID>`
4	Create the file `scrub_connectivity_results.txt`: `touch $FWDIR/conf/scrub_connectivity_results.txt`
5	Test the connectivity with the Mail Server: `/etc/fw/scripts/scrub_cvsenvheck_connectivity.sh <`*`IP Address of Mail Server`*`> $FWDIR/conf/scrub_connectivity_results.txt`
6	Analyze this file: `$FWDIR/conf/scrub_connectivity_results.txt`

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.

To add Postfix options

Step	Instructions
1	Connect to the command line on the Security Gateway.
2	Create the file `mta_postfix_options.cf`: `touch $FWDIR/conf/mta_postfix_options.cf`
3	Edit the file and add the definitions.
4	Save the changes in the file and exit the editor.
5	In SmartConsole, 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 (see *"Configuring the Security Gateway as a Mail Transfer Agent" on page 170*). If you do not enable the MTA, it is possible that emails are dropped and do not reach the mail server.

Troubleshooting IPS for a Security Gateway

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

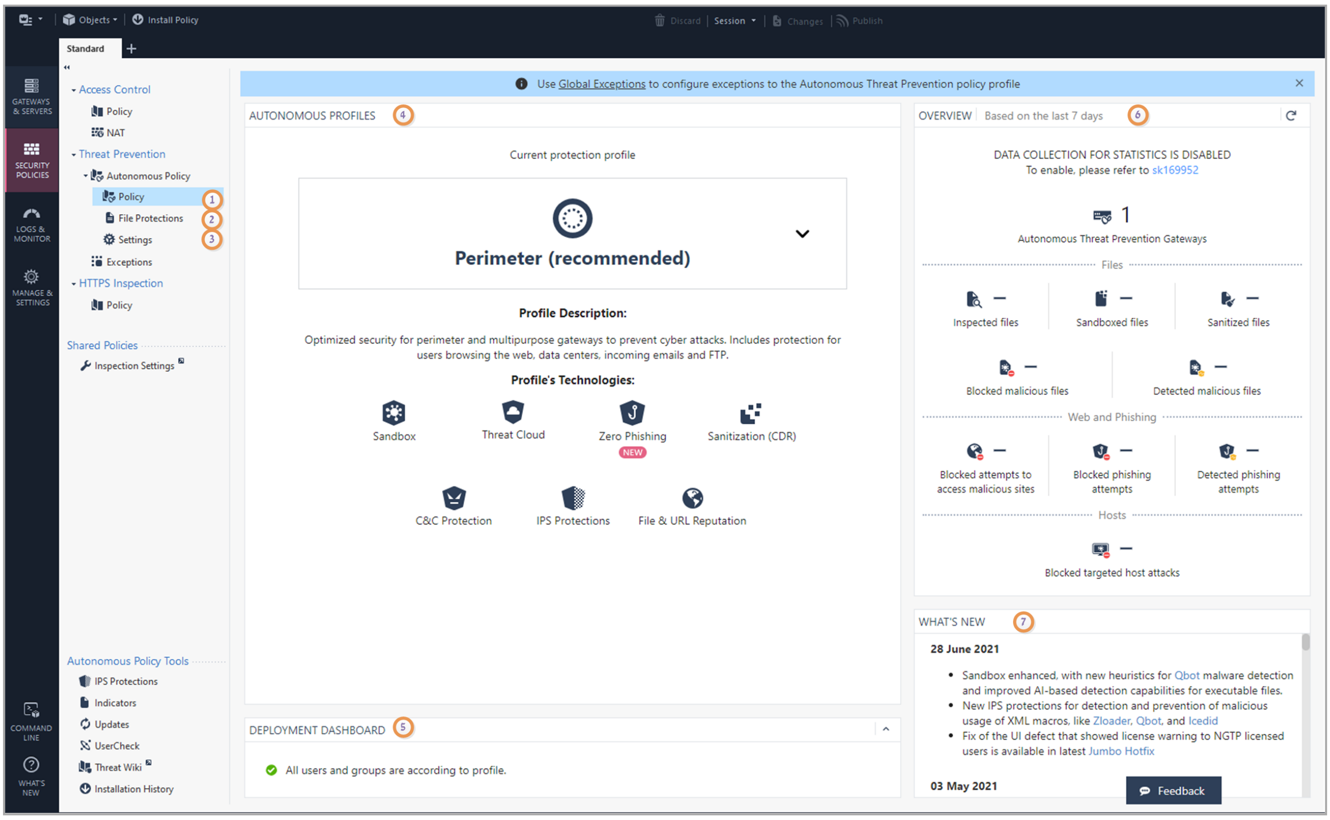
To enable Detect-Only for Troubleshooting

Step	Instructions
1	In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway
2	From the left tree, click **IPS**.
3	In the **Activation Mode** section, click **Detect Only**.
4	Click **OK**.
5	Install the Access Control policy. All protections set to Prevent allow traffic to pass, but continue to track threats according to the Track setting.

Autonomous Threat Prevention

Autonomous Threat Prevention is an innovative Threat Prevention management model that includes pre-defined security profiles. When you select a security profile, the Security Policy is created automatically. Autonomous Threat Prevention:

- Provides zero-maintenance protection from zero-day threats, and continuously and autonomously ensures that your protection is up-to-date with the latest cyber threats and prevention technologies.
- Empowers administrators with a one-click classification of the gateway role using out-of-the-box policy profiles based on your business and IT security needs.
- Streamlines configuration and deployment of policy profiles across your gateways.
- Provides simple and powerful customizations to best serve your organization’s needs.



Use Global Exceptions to configure exceptions to the Autonomous Threat Prevention policy profile

Optimized security for perimeter and multipurpose gateways to prevent cyber attacks. Includes protection for users browsing the web, data centers, incoming emails and FTP.

All users and groups are according to profile.

DATA COLLECTION FOR STATISTICS IS DISABLED
To enable, please refer to sk169952

28 June 2021

- Sandbox enhanced, with new heuristics for Qbot malware detection and improved AI-based detection capabilities for executable files.
- New IPS protections for detection and prevention of malicious usage of XML macros, like Zloader, Qbot, and Icedid
- Fix of the UI defect that showed license warning to NGTP licensed users is available in latest Jumbo Hotfix

03 May 2021

No.	Item	Description
1	**Autonomous Threat Prevention Policy**	This is where you manage the Autonomous Threat Prevention Policy.

No.	Item	Description
2	**File Protections**	See the protected files for each profile and customize as necessary. See *"File Protections" on page 308*.
3	**Settings**	Advanced settings. See *"Settings" on page 308*.
4	**Autonomous Threat Prevention Profiles**	Select your profile. See *"Autonomous Threat Prevention Profiles" on the next page*.
5	**Deployment Dashboard**	Advanced configuration. See *"Deployment" on page 307*.
6	**Overview**	See information about how Autonomous Threat Prevention handles malware attacks. See *"Autonomous Threat Prevention Overview Section" on page 368*
7	**What's New**	See the updates introduced to Autonomous Threat Prevention.

Note - For **offline** Threat Extraction Engine Release Updates, refer to sk167109.

If you prefer to create your Threat Prevention Security Policy manually, see *"Custom Threat Prevention" on page 34*.

Getting Started with Autonomous Threat Prevention

1. Enable Autonomous Threat Prevention in the Security Gateway / Cluster object (see *."Configuring Autonomous Threat Prevention" on page 305*
2. Select the required Autonomous Threat Prevention profile which creates the policy (see *"Autonomous Threat Prevention Profiles" below* and *"Configuring Autonomous Threat Prevention" on page 305*).
3. Optional: Configure advanced Threat Prevention settings:
   - **Security Gateway** / **Cluster** object - Settings for Threat Prevention Software Blades and features.
   - **Security Policies** view > **Threat Prevention** >**Autonomous Policy**:
     - **File Protections**
     - **Settings**
   - **Security Policies** view > **Threat Prevention** > **Exceptions**
   - **Security Policies** view > **Threat Prevention** > click **Autonomous Policy** > refer to the **Autonomous Policy Tools** section
   - **Security Policies** view > **HTTPS Inspection**
   - **Manage & Settings** view > **Blades** > **Threat Prevention** > **Advanced Settings**
   - **Security Gateway** / each **Cluster Member** command line - Configuration commands and files (for example, for SSH Deep Inspection)
4. Install the Autonomous Threat Prevention policy (see *"Configuring Autonomous Threat Prevention" on page 305*).

Monitoring

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.

Autonomous Threat Prevention Profiles

These are the 5 profiles supported by Autonomous Threat Prevention:

- **Recommended for Perimeter Profile**

  Optimized security for perimeter gateway to prevent cyberattacks. Includes protection for users browsing the web, data centers, incoming emails, and FTP. This is the default profile and the recommended profile for multiple protections on the same gateway (for example, when both Perimeter protection and Internal network protection are needed).

  Recommended for Perimeter is the most similar profile to the Optimized profile in the Custom Threat Prevention policy.

- **Strict Security for Perimeter Profile**

  Maximum security for perimeter gateways to prevent cyberattacks. Includes protection for users browsing the web, data centers, incoming emails and FTP.

- **Cloud/Data Center Profile**

  Optimized security to prevent cyberattacks on data centers. Includes extensive protection over servers and east-west traffic.

- **Internal Network Profile**

  Maximum security to prevent cyberattacks over internal traffic between internal users and internal servers.

- **Recommended for Guest Network Profile**

  ”Detect mode” security profile to monitor cyberattacks attempts through a guest network (Wi-Fi) non-intrusively.

Each profile consists of a wide range of industry-leading protections. This table summarizes the technologies used by each profile:

Profile	IPS Protections	File & URL Reputation	ThreatCloud	Sandbox	Sanitization (CDR)	C&C protection	Zero Phishing	
							URL-based Zero Phishing	In-browser Zero Phishing
Recommended for Perimeter Profile	✓	✓	✓	✓	✓	✓	✓	–
Cloud/Data Center Profile	✓	✓	✓	✓	–	✓	–	–

Profile	IPS Protections	File & URL Reputation	ThreatCloud	Sandbox	Sanitization (CDR)	C&C protection	Zero Phishing	
							URL-based Zero Phishing	In-browser Zero Phishing
Internal Network Profile	✓	✓	✓	✓	–	✓	–	–
Strict Security for Perimeter Profile	✓	✓	✓	✓	✓	✓	✓	–
Recommended for Guest Network Profile	✓	✓	✓	✓	–	✓	–	–

Here is a short explanation about each technology:

- **IPS Protections** - Integrated Intrusion Prevention System with leading performance and unlimited scaling. IPS implements advanced protections from network-based attacks and protects all IT systems, including servers, endpoints, industrial systems and IoT.
- **File & URL Reputation** - Files and URLs are checked through the ThreatCloud repository for reputation.
- **ThreatCloud** - A cloud-based real-time global threat intelligence using Check Point worldwide network of threat sensors.
- **Sandbox** - Prevents unknown, zero-day and advanced polymorphic attacks by executing suspicious files in evasion-resistant sandbox and applying advanced AI techniques.
- **Sanitization (CDR)** - Provides pro-active prevention of unknown attacks from day zero, by sanitizing incoming files before delivering them to users.
- **C&C protection** - Detects infected and compromised devices on the network. It blocks attacks and prevents damages by blocking malware Command & Control (C&C) communications.

- **Zero Phishing** - Zero Phishing prevents unknown zero-day and known phishing attacks on websites in real-time, by utilizing industry leading Machine-Learning algorithms and patented inspection technologies.

Configuring Autonomous Threat Prevention

To configure Autonomous Threat Prevention in your environment, follow these steps:

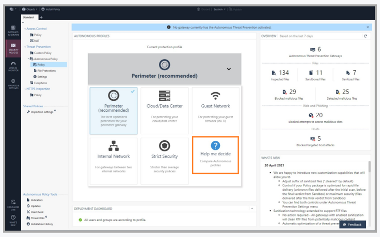
1. **Enable Autonomous Threat Prevention on the Security Gateway)**

Step	Instructions
1	In SmartConsole, go to the **Gateways & Servers** view, and right-click the required Security Gateway.
2	In the **General Properties** page, go to the **Threat Prevention** tab, and select **Autonomous Threat Prevention**

2. **Create an Autonomous Threat Prevention Policy**

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>1</td><td>In SmartConsole, go to <b>Security Policies</b> &gt; <b>Autonomous Threat Prevention</b> &gt; <b>Policy</b>.</td></tr>
<tr><td>2</td><td>

Click the default profile name to see the list of profiles, and select the required profile.
If you are not sure which profile to select, click the drop-down arrow next to the profile's name, and from the drop-down list, select **Help me decide**:



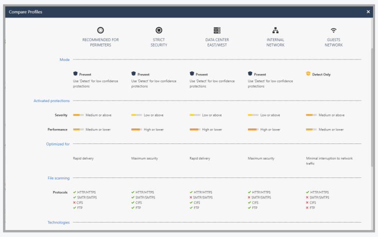
No gateway currently has the Autonomous Threat Prevention activated.

All users and groups are according to profile.

20 April 2021

- We are happy to introduce new customization capabilities that will allow you to
  - Adjust suffix of sanitized files (".cleaned" by default)
  - Control if your Policy package is optimized for rapid file delivery (unknown files delivered after the initial scan, before the final verdict from Sandbox) or maximum security (files delivered after the final verdict from Sandbox)
  - You can find both controls under Autonomous Threat Prevention Settings menu
- Sanitization technology extended to support RTF files
  - No action required - All gateways with enabled sanitization will clean RTF files from potentially malicious content
  - Automatic optimization of a threat preve

A table which specifies the differences between the profiles opens:



Compare Profiles

<table>
<tr><th></th><th>RECOMMENDED FOR PERIMETERS</th><th>STRICT SECURITY</th><th>DATA CENTER EAST/WEST</th><th>INTERNAL NETWORK</th><th>GUESTS NETWORK</th></tr>
<tr><td>Mode</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>Prevent
Use 'Detect' for low confidence protections</td><td>Prevent
Use 'Detect' for low confidence protections</td><td>Prevent
Use 'Detect' for low confidence protections</td><td>Prevent
Use 'Detect' for low confidence protections</td><td>Detect Only</td></tr>
<tr><td>Activated protections</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Severity</td><td>Medium or above</td><td>Low or above</td><td>Low or above</td><td>Low or above</td><td>Medium or above</td></tr>
<tr><td>Performance</td><td>Medium or lower</td><td>High or lower</td><td>High or lower</td><td>High or lower</td><td>Medium or lower</td></tr>
<tr><td>Optimized for</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>Rapid delivery</td><td>Maximum security</td><td>Rapid delivery</td><td>Maximum security</td><td>Minimal interruption to network traffic</td></tr>
<tr><td>File scanning</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Protocols</td><td>✓ HTTP/HTTPS
✓ SMTP/SMTPS
✗ CIFS
✓ FTP</td><td>✓ HTTP/HTTPS
✓ SMTP/SMTPS
✓ CIFS
✓ FTP</td><td>✓ HTTP/HTTPS
✗ SMTP/SMTPS
✓ CIFS
✓ FTP</td><td>✓ HTTP/HTTPS
✗ SMTP/SMTPS
✓ CIFS
✓ FTP</td><td>✓ HTTP/HTTPS
✗ SMTP/SMTPS
✗ CIFS
✗ FTP</td></tr>
<tr><td>Technologies</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Based on the table, select the profile which best suits your needs.

</td></tr>
<tr><td>3</td><td>Click <b>OK</b>.</td></tr>
</table>

Note - Each profile shows a list of the technologies that it uses.

3. **Install the Autonomous Threat Prevention Policy**

Step	Instructions
1	In SmartConsole, from the toolbar, select **Install Policy**. The **Install Policy** window opens.
2	Select **Threat Prevention**.
3	Select the gateway targets for Policy installation. **Note** - The Autonomous Threat Prevention Policy is installed on Security Gateways with Autonomous Threat Prevention enabled. Security Gateways with no Autonomous Threat Prevention enabled receive the Custom Threat Prevention Policy.
4	Click **Install**.

4. **Using different Autonomous Threat Prevention profiles on different Security Gateways**

You can use different Autonomous Threat Prevention profiles for different Security Gateways.

To do so, you must create a new policy package for each Security Gateway and follow the configuration steps, as follows:

Step	Instructions
1	In SmartConsole, create a new policy package. From the main menu, click the drop-down arrow and select **Manage policies and layers**. The **Manage policies and layers** window opens. Click **New** and configure the new policy package. For more information on policy packages, see the *R81.20 Security Management Administration Guide*.
2	Select the required Autonomous Threat Prevention profile. See *"Create an Autonomous Threat Prevention Policy" on the previous page*.
3	Install the Threat Prevention policy on the applicable Security Gateway. See *"Install the Autonomous Threat Prevention Policy" above*.

Note - MTA (Mail Transfer Agent) is not supported by Autonomous Threat Prevention. You can manage a Security Gateway configured as MTA by Custom Threat Prevention.

Exceptions

Global exceptions are available for use by gateways configured with Autonomous Threat Prevention or a Custom Threat Prevention policy. Global exceptions that existed prior to the migration to Autonomous Threat Prevention are enforced in Autonomous Threat Prevention without any action needed.

To add global exceptions to the Autonomous Threat Prevention policy:

1. Go to the **Security Policies** view > **Threat Prevention** > **Exceptions** > **Global Exceptions**.
2. Add the applicable exceptions.
3. In the **Install On** column, select the gateways to which each exception applies.

Deployment

The **Deployment Dashboard** view:

- Shows this information:
  - Security Gateways with HTTPS Inspection disabled.
  - Security Gateways that do not support Zero Phishing (versions R81.10 and lower).
  - Security Gateways with no FQDN configured (FQDN configuration is required only for Zero Phishing).
- Lets you gradually deploy Threat Prevention policy in your networks. The **Deployment Dashboard** includes these protection modes:
  - **According to profile** - The settings of the Threat Prevention profile apply to the object. By default any traffic is protected according to profile, and this is the recommendation. If gradual deployment is needed, you can put specific network objects in "**Detect only**". We recommend to move these object to the **According to profile** mode after a short trial period.
  - **No Protection** - The object is not protected by the selected Threat Prevention profile. Traffic is allowed and is not logged.
  - **Detect only** - Traffic is allowed, but it is logged according to the Threat Prevention profile settings.

  Note - You can easily drag and drop objects from any of the protection modes to any other protection mode.

  By default, the **No Protection** and **Detect Only** columns are empty, and the **According to Profile** column has one object: **Any**. When you add an object to the **No Protection** column or the **Detect Only** column, the object in the **According to Profile** column changes from **Any** to **All Other**.

File Protections

In the **File Protections** page, you can:

- View the protected file types and protection types for the selected Autonomous Threat Prevention profile.
- Override the recommended file protections according to profile and select different protections.

To configure file protections

1. Go to **Threat Prevention** > **Autonomous Threat Prevention** > **File Protections**
2. Click on the **+** sign and configure the required protection.

   These are the available protections:

   - **Inspect** - These technologies are operated: File Reputation, ThreatCloud and Sandbox. You can see Sandbox is enabled in the **Sandbox** column.
   - **Inspect & Clean** - These technologies are operated: File Reputation, ThreatCloud, Sandbox and Sanitization (CDR). You can see Sandbox is enabled in the **Sandbox** column.
   - **Block** - Block the file.
   - **Bypass** - Do not inspect the file.

   You cannot override the protections for file types which are not on the list. File types which are not on the list will be inspected in all profiles.

Settings

Sanitized File Settings - By default, this option is selected:

- **Allow end-users to access the original files that are not malicious according to Sandbox** - After a file is cleaned/sanitized, a banner with a link to original file is added to the document. An access to original file will be allowed only if the original file is found to be benign by all Threat Prevention engines, including Sandbox. If you clear this option, you will not be able to access the original file even if it is determined as non-malicious.
- **Modify the name of the cleaned file** - Select this option to modify the name of the cleaned file.

Advanced Settings - If needed, you can turn off certain features. We recommend to keep Sandbox, Sanitization and Archives deep scan On.

Configuring Threat Emulation on the Security Gateway - Autonomous Threat Prevention

Preparing for Local or Remote Emulation

For deployments that use a Threat Emulation appliance, prepare the network and Threat Emulation appliance for Local or Remote deployment in the internal network.

Step	Instructions
1	Open SmartConsole.
2	Create the Security Gateway object for the Threat Emulation appliance.
3	If you are running emulation on HTTPS traffic, configure the settings for HTTPS Inspection (see *"HTTPS Inspection " on page 393*).
4	Make sure that the traffic is sent to the appliance according to the deployment: ■ Local Emulation - The Threat 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 Threat Emulation appliance.

Changing the Analysis Location

You can select or change the location of the emulation analysis in the **Threat Emulation** page in **Gateway Properties.**

To select the location of the emulation analysis

Step	Instructions
1	Double-click the Security Gateway object of the **Threat Emulation appliance**. The **Gateway Properties** window opens.
2	From the navigation tree, select **Threat Emulation**. The **Threat Emulation** page opens.

Step	Instructions
3	From the **Analysis Location** section, select the emulation location: ■ **According to the gateway** - According to the gateway configuration. ■ Specify: • **Check Point ThreatCloud** - Files are sent to the Check Point ThreatCloud for emulation. • **Local Gateway** - This Security Gateway does the emulation. • **Remote Emulation Appliances** - Remote appliances do the emulation. You can select one or more appliances on which the emulation is performed.
4	**Optional:** Select **Emulate files on ThreatCloud if not supported locally**. If files are not supported on the Threat 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 Threat Emulation appliance.

Setting the Activation Mode

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

To configure the activation mode

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

Optimizing System Resources

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

You can configure the settings for these system resources:

- Minimum available hard disk space (If no emulation is done on a file, the Threat Prevention **Fail Mode** settings determine if the file is allowed or blocked.
- Maximum available RAM that can be used for Virtual Machines.

If you plan to change the available RAM, these are the recommended settings:

- If the appliance is only used for Threat Emulation, increase the available RAM.
- If the appliance is also used for other Software Blades, decrease the available RAM.

To optimize the system resources for the Threat Emulation appliance

Step	Instructions
1	Double-click the Security Gateway object of the **Threat Emulation appliance**. The **Gateway Properties** window opens.
2	From the navigation tree, select **Threat Emulation** > **Advanced**. The **Advanced** page opens.
3	Stopping the emulation is determined when the Log storage mechanism automatically deletes log files. Therefore, in order to change the relevant configured value (**Note** - It also affects the Log's files deletion). Navigate to **Logs** > **Local Storage** >. And from When disk space is below `<value>`**Start deleting old files**, you can change the `<value>`.
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.

Step	Instructions
5	**Optional.** To change the amount of available RAM: 1. Click **Configure**. The **Memory Allocation Configuration** window opens. 2. 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 512 MB - 1000 GB. 3. 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**.
8	Install the Threat Prevention Policy.

Managing Images for Emulation

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

To manage the images that the appliance uses for emulation

Step	Instructions
1	Double-click the Security Gateway object of the **Threat Emulation appliance**. The **Gateway Properties** window opens.
2	From the navigation tree, select **Threat Emulation** > **Advanced**. The **Advanced** page opens.

Step	Instructions
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**.
5	Install the Threat Prevention Policy.

Configuring Threat Extraction on the Security Gateway - Autonomous Threat Prevention

To configure the Threat Extraction blade on the Security Gateway

Step	Instructions
1	In the **Gateways & Servers** view, double-click the Security Gateway object and click the **Threat Extraction** page.
2	Make sure the **Activation Mode** is set to **Active**.
3	In the **Resource Allocation** section, configure the resource settings.
4	Click **OK**.
5	Install Policy.

For Threat Extraction API support, open the Security Gateway object, go to **Threat Extraction** > **Web API** > **Enable API**.

Threat Extraction and Endpoint Security

When both the Threat Extraction blade and the SandBlast Agent for Browsers are activated on the network Security Gateway, a special configuration is required. Without this configuration, when you download a file, it can be cleaned twice, both by the Threat Extraction blade and by the SandBlast Agent.

To prevent this, the Security Gateway adds a digital signature to all the files cleaned by the Threat Extraction blade. When the SandBlast Agent intercepts a downloaded file. If the digital signature is verified successfully, SandBlast Agent does not clean the file, so the file is not cleaned twice.

For details on how to configure the digital signature on the Security Gateway and how to configure the Endpoint management, see sk142732.

Configuring Threat Extraction in a Cluster

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

To configure Threat Extraction in a cluster

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

Notes:

- Only the High Availability mode is supported.
- The original files are synchronized between the Cluster Members. In case of a failure, there is still access to the original files.

Threat Extraction Statistics

To see Threat Extraction statistics

Step	Instructions
1	Connect to the command line on the Security Gateway with the Threat Extraction enabled.
2	Run these commands: ■ `cpview` ■ `cpstat scrub -f threat_extraction_statistics`

Using the Security Gateway CLI

The Security Gateway has a Threat Extraction menu

In this menu, you can:

- 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

Step	Instructions
1	Connect to the command line on the Security Gateway / each Cluster Member.
2	Log in to the Expert mode.
3	Run: `scrub`

The menu shows these options:

Option	Description
`debug`	Controls debug messages.
`queues`	Shows information on Threat Extraction queues. 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.

Option	Description
`bypass`	Bypasses all files. Use this command to debug issues with the `scrubd` (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.
`cache`	Shows and resets cache.
`backup_expired_mail`	Backs up expired mails to external storage.

Storage of Original Files

The Threat Extraction blade reconstructs files (cleans or converts files to PDF) to eliminate potentially malicious content. After the Threat Extraction blade reconstructs the files, the original files are saved on the gateway for a default period.

Mail attachments

Mail attachments are saved for a default period of 14 days.

To configure a different number of days for storage of mail attachments:

Step	Instructions
1	From the left navigation panel, click **Gateways & Servers**.
2	Open the Security Gateway / Cluster object.
3	From the left tree, click **Threat Extraction**.
4	Click **Resource Allocation** > **Delete stored original files older than x Days**.
5	Change the number of days as required. The maximum is 45 days.

Step	Instructions
6	Click **OK**.
7	Install the Threat Prevention Policy.

To save the files for a longer period, you must back them up to external storage (see *"Backup to External Storage" below*).

Web downloads

Web downloads are saved for a default period of 2 days.

To configure a different number of days for storage of web downloads:

Step	Instructions
1	Connect to the command line on the Security Gateway / each Cluster Member.
2	Log in to the Expert mode.
3	Edit the `$FWDIR/conf/scrub_debug.conf` file.
4	Search for `http_keep_original_duration` and change the value as required. Value can be between 2 and 45 days.
5	Save the changes in the file and exit the editor.

To save the files for a longer period, you must back them up to external storage (see *"Backup to External Storage" below*).

Backup to External Storage

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

Notes:

- In a cluster, you must configure all Cluster Members in the same way.
- End-users cannot access files on external storage. Only the administrator can access these files.

To back up original files to external storage

Step	Instructions
1	Connect to the command line on the Security Gateway / each Cluster Member.

Step	Instructions
2	Log in to the Expert mode.

3	Create the backup folder:
	`mkdir /mnt/<local_backup_folder>`
	Example:
	`mkdir /mnt/MyLocalBackupFolder`

4	Mount the backup folder to the remote folder:
	`mount -t cifs <remote_folder> /mnt/<local_backup_folder>`
	Example:
	`mount -t cifs //MyServer/MyBackupFolder /mnt/MyLocalBackupFolder`
	Best Practice - To preserve the mount configuration after reboot, configure a Scheduled Job to run the applicable "`mount`" command at startup (in Gaia Portal, go to **System Management** > **Job Scheduler**).

5	Edit the `$FWDIR/conf/scrub_debug.conf` file: `vi $FWDIR/conf/scrub_debug.conf`

6	Search for this section:
	`:external_storage.`
	1. Change the `enabled` value from "`0`" to "`1`".
	2. In the `external_path` parameter, write the full path to the local backup folder.
	3. The `expired_in_days` parameter sets the backup date.
	The value you enter for this parameter specifies how many days before expiration the backup is performed.
	Example:
	`:external_storage (`
	`    :enabled (1)`
	`    :external_path ("/mnt/MyLocalBackupFolder")`
	`    :expired_in_days (5)`

Step	Instructions

7	Configure the applicable values:
	1. Change the `enabled` value from "`0`" to "`1`".
	2. In the `external_path` parameter, write the full path to the local backup folder.
	3. The `expired_in_days` parameter sets the backup date. The value you enter for this parameter specifies how many days before expiration the backup is performed.
	Example:
	`:external_storage (`
	`    :enabled (1)`
	`    :external_path ("/mnt/MyLocalBackupFolder")`
	`    :expired_in_days (5)`

8	Save the changes in the file and exit the editor.

To test the backup manually

Run this command:

```
scrub backup_expired_mail <days for expired entries> <external_path>
```

In "`<days for expired entries>`" enter "0".

Configuring Zero Phishing Settings - Autonomous Threat Prevention

Zero Phishing is active by default on the Perimeter and Strict profiles.

In-Browser Zero Phishing is off by default in all profiles.

To enable In-browser Zero Phishing:

1. In SmartConsole, go to **Threat Prevention** > **Autonomous Policy** > **Settings** > **Advanced Settings**.
2. From the drop-down menu, select **In-browser Zero Phishing**.
3. Change the value to **On**.

4. Click **Apply**.
5. Install the Threat Prevention Policy.

If HTTPS Inspection is active, in-browser Zero Phishing requires:

- A certificate - HTTPS Inspection automatically generates this certificate.
- Configured FQDN on the Security Gateway / each Cluster Member - In-Browser Zero Phishing runs on the client side (the endpoint). The endpoint must have the possibility to communicate with the Security Gateway / each Cluster Member over HTTPS that relies on FQDN.

  To configure the FQDN in the Security Gateway / Cluster object:

  1. Go to the **Zero Phishing** tab.
  2. Configure the FQDN.
  3. Click **OK**.
  4. Install the Access Control and Threat Prevention policies.

  Notes:
  - The FQDN must be in the DNS records of your DNS server.
  - Make sure that the Zero Phishing portal is configured to work on a public IP address. For more information, see sk178769.

Limitations:

- In-browser Zero Phishing does not support Internet Explorer.
- In-browser Zero Phishing does not support mirrored traffic (Mirror Port, Span Port, Tap mode).

Zero Phishing and Unclassified Sites

You can block or allow sites that the Cloud Service is unable to classify as Phishing or Benign.

To block unclassified sites, run this command on the Security Gateway CLI:

```
zph att set inbrowser_block_unclassified_sites 1
```

To allow unclassified sites (default), run this command on the Security Gateway CLI:

```
zph att set inbrowser_block_unclassified_sites 0
```

Zero Phishing Exceptions

To skip unnecessary scans of popular sites, we recommend to configure the Zero Phishing blade to bypass specific popular sites.

To configure the Zero Phishing blade to bypass popular sites:

1. In SmartConsole, go to the **Security Policies** view > **Threat Prevention** > **Exceptions**.
2. Click **Add Exception** > **Below**.
3. Give a name to the rule.
4. In the **Protected Scope** column:
   a. Click the "Plus" (**+**) button.
   b. In the window that opens, go to **Import** > **Updatable Objects**.
   c. Search for **Zero Phishing Bypass** and select it.
   d. Click **OK**.
5. In the **Protection/Site/File/Blade** column:
   a. Click the "Plus" (**+**) button.
   b. From the drop-down menu in the window that opens, select **Blades**.
   c. From the list of blades, select **Zero Phishing**.
6. In the **Action** column, select **Inactive**.
7. Install Policy.

Notes -

- For proper enforcement, make sure that this rule is the last rule under Global Exceptions.
- For any exception rule that contains **Zero Phishing** in the **Protection/Site/File/Blade** column, in the **Install On** column, you must select Security Gateways with Zero Phishing enabled.

The list of bypassed sites dynamically changes. To see the list, go to sk179726.

IPS Protections

Protection Browser

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

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

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 Security Gateway. 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 Security Gateways on which they are activated.

Important - The **Performance Impact** of protections is rated based on how they affect Security Gateways that run R80.30 version and above. The Performance Impact on other Security 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 Security 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 Security 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 (see *"Updating IPS Protections" on the next page*). 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

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

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

To filter the protections

Step	Instructions
1	From the **IPS Protections** window, click the **Filter** icon. The **Filters** pane opens and shows IPS protections categories.

Step	Instructions
2	To add more categories 1. Click the **Add filter** button. A window opens and shows the IPS protections categories. 2. 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.

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.

Notes:

- To enforce the IPS updates, you must install the Threat Prevention Policy.
- When you assign or reassign a global configuration while an IPS update runs on a Domain, you may get an "Internal error occurred" error. To resolve this issue:
  1. Connect with SmartConsole to the Domain Management Server.
  2. Run the IPS update.
  3. Close the SmartConsole which is connected to the Domain Management Server.
  4. In the global SmartConsole, assign or reassign the global configuration.

To update IPS Protections

In SmartConsole, click the **Security Policies** view > **Threat Prevention** > in the **Autonomous Policy Tools** section, click **Updates**.

Step	Instructions
1	In the IPS section > **Update Now**. From the drop-down menu, select: ▪ **Download with SmartConsole** - If your Security Management Server has no internet access. ▪ **Download with Security Management Server**. ▪ **Offline Update** - If you want to manually upload the file. Select the required file for the update, and then click **Open**.
2	Install the Threat Prevention Policy.

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

Scheduling IPS Updates

You can configure a schedule for downloading the latest IPS protections and protection descriptions (see *"Threat Prevention Scheduled Updates - Custom Threat Prevention" on page 279*).

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

Step	Instructions
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**. Click **OK**.
3	Install the Threat Prevention Policy.

Reviewing New Protections

To see newly downloaded protections

In SmartConsole > go to **Security Policies > Threat Prevention** > **Autonomous Policy Tools**

Step	Instructions
1	Go to **IPS Protections**.
2	The **Update Date** column sorts the protections by date. By default, the latest protections are shown first. If not, click the column so that the latest protections are presented first.

IPS Protections Follow Up

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

To view protections marked for follow up

In SmartConsole, go to **Security Policies** > **Threat Prevention** > **Autonomous Policy Tools**

Step	Instructions
1	Go to **IPS Protections** > **Filters**.
2	Select **Follow Up**.

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

Manually Marking Protections for Follow Up

You can mark individual protections for Follow Up, which lets you quickly review the identified protections in the **IPS Protections** page. To make the Follow Up feature efficient, make sure to keep the list of marked protections as short as possible.

Mark newly downloaded protections and any protection that you want to monitor, but remember to remove protections from this list when you are more confident that you configured them in the best way for your environment. The longer the Follow Up list is, the more difficult it is to use it as a workable task list

To manually mark protections for follow up:

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

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

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

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

Automatically Marking New Protections for Follow Up

Check Point provides new and updated protections as they become available (see *"Updating IPS Protections" on page 324*). To give you complete control over the process of integrating new IPS protections, you can have them automatically marked for Follow Up, which gives you time to evaluate the impact the protections have on your environment.

To have new protections marked automatically

In SmartConsole, go to **Security Policies** > **Threat Prevention** > **Autonomous Policy Tools**

Step	Instructions
1	Go to **Updates > IPS** > **Follow Protections**

Threat Prevention and UserCheck - Autonomous Threat Prevention

UserCheck handles specific 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.

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 Security 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.

Using Threat Prevention UserCheck

On the UserCheck page, you can preview UserCheck interaction objects and their messages: **Security Policies** > **Autonomous Policy Tools** >**UserCheck**.

These are the default UserCheck Interaction objects:

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 the company policy for the specific 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:

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

Configuring the Security Gateway for UserCheck

UserCheck is enabled by default in Autonomous Threat Prevention.

If users connect to the Security Gateway remotely, set the internal interface of the Security Gateway (on the **Topology** page) to be the same as the **Main URL** for the UserCheck Portal.

To configure UserCheck on a Security Gateway

Step	Instructions
1	In the **UserCheck Web Portal** section: The **Main URL** field shows the primary URL for the web portal that shows the UserCheck notifications. You can use the suggested **Main URL** or manually enter a different **Main URL**. ⓘ **Note** - The **Main URL** field contains an IP address and not a DNS name. Update the **Main URL** field If you change a Security Gateway's IPv4 address to IPv6 address, or the other way around, .
2	Optional: Click **Aliases** to add URL aliases that redirect different hostnames to the **Main URL**. For example: `Usercheck.mycompany.com` The aliases must be resolved to the portal IP address on the corporate DNS server.
3	In the **Certificate** section, click **Import** to import a certificate that the portal uses to authenticate to the Security Management Server. By default, the portal uses a certificate from the Check Point Internal Certificate Authority (ICA). This might generate warnings if the user browser does not recognize Check Point as a trusted Certificate Authority. To prevent these warnings, import your own certificate from a recognized external authority. ⓘ **Note** - After you download your certificate, you can click **Replace** to replace it with a different certificate, and click **View** to see the certificate information.

Step	Instructions
4	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) - Interfaces used for establishing route-based VPN tunnels (VTIs). ■ **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**
5	**UserCheck Client** - The UserCheck Client is installed on Endpoint devices to communicate with the Security Gateway and show UserCheck Interaction notifications to users. ■ **Activate UserCheck Client support**. This enables UserCheck through the client. ■ Click **Download Client** to download the installation file for the UserCheck Client. **Note** - The link is not active until the UserCheck Portal is up. For more information about installation and configuration of the UserCheck Client, see .

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>6</td><td>In the <b>Mail Server</b> section, configure a mail server for UserCheck. This server sends notifications to users that the Security 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 Security Gateway cannot redirect the user to the UserCheck Portal because the traffic is not HTTP.
<b>If the user does not have a UserCheck Client, UserCheck sends an email notification to the user.</b><ul><li><b>Use the default settings</b> - Click the link to see which mail server is configured.</li><li><b>Use specific settings for this gateway</b> - Select this option to override the default mail server settings.</li><li><b>Send emails using this mail server</b> - Select a mail server from the list, or click <b>New</b> and define a new mail server.</li></ul></td></tr>
<tr><td>7</td><td>Click <b>OK</b>.</td></tr>
<tr><td>8</td><td>If there is encrypted traffic through an internal interface, add a new rule to the FirewallLayer of the Access Control Policy.
<b>This is a sample rule</b><table><tr><th>Source</th><th>Destination</th><th>VPN</th><th>Services & Applications</th><th>Action</th></tr><tr><td>Any</td><td>Security Gateway on which UserCheck Client is enabled</td><td>Any</td><td>UserCheck</td><td>Accept</td></tr></table></td></tr>
<tr><td>9</td><td>Install the Access Control Policy.</td></tr>
</table>

Selecting Approved and Cancel UserCheck Messages

The 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 the Approved Page and Cancel Page:

Step	Instructions
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.

Send Email Notifications in Plain Text

Not all emails clients can handle emails in rich text or HTML format.

To accommodate such clients, you can configure the Security Gateway to send email notification in plain text without images, in addition to the HTML format. The user's email client decides which format to show.

1. Connect to the command line to the Security Gateway / each Cluster Member.
2. Log in to the Expert mode.
3. Back up the configuration file:

   ```
   cp -v $FWDIR/conf/usrchkd.conf{,_BKP}
   ```

4. Edit the configuration file:

   ```
   vi $FWDIR/conf/usrchkd.conf
   ```

5. Change the value of the applicable parameter:

   from

   ```
   :send_emails_with_no_images (false)
   ```

   to

   ```
   :send_emails_with_no_images (true)
   ```

6. Save the changes in the file and exit the editor.

7. Kill the `userchkd` process to load the new configuration:

   ```
   killall userchkd
   ```

   The Security Gateway automatically restarts this process.

UserCheck Client

The UserCheck Client is installed on endpoint computers to communicate with the Security Gateway and show notifications to users.

UserCheck Client sends notifications for applications that are not in a web browser, such as Skype, iTunes, or browser add-ons (such as radio toolbars). The UserCheck Client can also work together with the UserCheck Portal to show notifications on the computer itself in these cases:

- It is not possible to show the notification in a web browser.
- The UserCheck engine determines that the notification does not appear correctly in the web browser.

Notifications of incidents are shown in a pop up from the UserCheck Client in the system tray.

Users select an option in the notification message to respond in real-time.

UserCheck Client Requirements

See the *R81.20 Release Notes* > *UserCheck Client Requirements*.

Workflow for installing and configuring UserCheck Clients:

1. Open the Security Gateway object.
2. Enable UserCheck and the UserCheck Client in the Security Gateway object. See *UserCheck in the Access Control Policy*.
3. Configure how the UserCheck Clients communicate with the Security Gateway and create trust with it.

   See *"Client and Gateway Communication" on the next page*.
4. Install the UserCheck Client on the endpoint computers.

   See *"Installing UserCheck Client" on page 340*.
5. Connect the UserCheck Client to the Security Gateway.

   See *"Connecting UserCheck Client to the Security Gateway" on page 344*.
6. Make sure the UserCheck Clients can receive notifications.

Perform a simplest action on the endpoint computers that violates the configured Security Policy.

Client and Gateway Communication

In an environment with UserCheck Clients, the Security Gateway acts as a server for the clients. Each client must be able to *discover* the server and create *trust* with it.

To create trust, the client makes sure that the server is the correct one. It compares the server fingerprint calculated during the SSL handshake with the expected fingerprint. If the server does not have the expected fingerprint, the client asks the user to manually confirm that the server is correct.

Here is a list of the methods that you can use for clients to discover and trust the server.

Option Comparison

Configuration	Must Have AD	Manual User Trust (one time) Necessary?	Multi-Site	Client Stays Signed?	Still works after Gateway Changes	Level	Recommended for...
File name based	No	Yes	No	Yes	No	Very Simple	Single Security Gateway configurations
AD based	Yes	No	Yes	Yes	Yes	Simple	Configurations with AD that you can modify
DNS based	No	Yes	Partially (per DNS server)	Yes	Yes	Simple	Configurations without AD With an AD you cannot change, and a DNS that you can change

Configuration	Must Have AD	Manual User Trust (one time) Necessary?	Multi-Site	Client Stays Signed?	Still works after Gateway Changes	Level	Recommended for...
Remote registry	No	No	Yes	Yes	Yes	Moderate	Where remote registry is used for other purposes

1. **File name based server configuration**

   If no other method is configured (default, out-of-the-box situation), all UserCheck Clients downloaded from the portal are renamed to have the portal machine IP address in the filename. During installation, the client uses this IP address to connect to the Security Gateway. Note that the user has to click **Trust** to manually trust the server.

   Explanation

   This option is the easiest to configure, and works out-of-the-box. It tells users to manually click **Trust** to trust the server the first time they connect. You can use this option if your configuration has only one Security Gateway with the relevant Software Blades.

   How does it work?

   When a user downloads the UserCheck Client, the address of the Security Gateway is inserted in the filename. During installation, the client finds if there is a different discovery method configured (AD based, DNS based, or local registry). If no method is configured, and the Security Gateway can be reached, it is used as the server. In the UserCheck Settings window, you can see that the server you connect to is the same as the Security Gateway in the UserCheck Client filename.

   Users must manually make sure that the trust data is valid, because the filename can be easily changed.

Renaming the MSI

You can manually change the name of the MSI file before it is installed on a computer.

This connects the UserCheck Client to a different Security Gateway.

a. Make sure the Security Gateway has a DNS name.

b. Rename the MSI using this format:

UserCheck_~*GWname*.msi

Where *GWname* - is the DNS name of the Security Gateway.

Optional format:

UserCheck_~*GWname-port*.msi

Where *port* is the port number of notifications.

For example:

```
UserCheck_~mygw-18300.msi
```

Notes:

- The prefix does not have to be "UserCheck". The important part of the format is underscore tilde (_~), which indicates that the next string is the DNS of the Security Gateway.
- If you want to add the port number for the notifications to the client from the Security Gateway, the hyphen (-) indicates that the next string is the port number.

2. **Active Directory Based Configuration**

If client computers are members of an Active Directory domain, you can configure the server addresses and trust data using a dedicated tool.

Explanation

If your client computers are members of an Active Directory domain and you have administrative access to this domain, you can use the Distributed Configuration tool to configure connectivity and trust rules.

The Distributed Configuration tool has three windows:

- **Welcome** - Describes the tool and lets you enter different credentials that are used to access the AD.
- **Server configuration** - Configure which Security Gateway the client connects to, based on its location.
- **Trusted Security Gateways** - View and change the list of fingerprints that the Security Gateways consider secure.

To enable Active Directory based configuration for clients:

a. Download and install the UserCheck Client MSI on a computer.

   From the command line on that computer, run the client configuration tool with the AD utility.

   For example, on a Windows 7 computer:

   ```
   "C:\Users\%USERNAME%\Local Settings\Application
   Data\Checkpoint\UserCheck\UserCheck.exe" -adtool
   ```

   The **Check Point UserCheck - Distributed Configuration** tool opens.

b. In the **Welcome** page, enter the credentials of an AD administrator.

   By default, your AD username is shown. If you do not have administrator permissions, click **Change user** and enter administrator credentials.

c. In the **Server Configuration** page, click **Add**.

   The **Identity Server Configuration** window opens.

d. Select **Default** and then click **Add**.

e. Enter the IP address or Fully Qualified Domain Name (FQDN) and the port of the Security Gateway.

f. Click **OK**.

   The identity of the AD Server for the UserCheck Client is written in the Active Directory and given to all clients.

Note - The entire configuration is written under a hive named **Check Point** under the **Program Data** branch in the AD database that is added in the first run of the tool. Adding this hive does not affect other AD based applications or features.

Server Configuration Rules

If you use the Distributed Configuration tool and you configure the client to **Automatically discover** the server, the client fetches the rule lists. Each time it must connect to a server, it tries to match itself against a rule, from top to bottom.

When the tool matches a rule, it uses the servers shown in the rule, according to the priority specified.

The configuration in this example means:

a. If the user is coming from `'192.168.0.1 - 192.168.0.255'`, then try to connect to `US-GW1`.

   If it is not available, try `BAK-GS2` (it is only used if `US-GW1` is not available, as its priority is higher).

b. If the user is connected from the Active Directory site `'UK-SITE'`, connect either to `UK-GW1` or `UK-GW2` (select between them randomly, as they both have the same priority). If both of them are not available, connect to `BAK-GS2`.

c. If rules 1 and 2 do not apply, connect to `BAK-GS2` (the default rule is always matched when it is encountered).

Use the **Add**, **Edit** and **Remove** buttons to change the server connectivity rules.

Trusted Gateways

The **Trusted Gateways** window shows the list of servers that are trusted - no messages open when users connect to them.

You can add, edit or delete a server. If you have connectivity to the server, you can get the name and fingerprint. Enter its IP address and click **Fetch Fingerprint** in the **Server Trust Configuration** window. If you do not have connectivity to the server, enter the same name and fingerprint that is shown when you connect to that server.

3. **DNS SRV Record Based Server Discovery**

Configure the server addresses in the DNS server. Note that the user has to click **Trust** to manually trust the server.

Explanation

If you configure the client to **Automatic Discovery** (the default), it looks for a server by issuing a DNS SRV query for the address of the Security Gateway (the DNS suffix is added automatically). You can configure the address in your DNS server.

To configure DNS based configuration on the DNS server:

a. Go to **Start** > **All Programs** > **Administrative Tools** > **DNS**.

b. Go to **Forward lookup zones** and select the applicable domain.

c. Go to the **_tcp** subdomain.

d. Right-click and select **Other new record**.

e. Select **Service Location**, **Create Record**.

f. In the **Service** field, enter **CHECKPOINT_DLP**.

g. Set the **Port number** to 443.

h. In **Host offering this server**, enter the IP address of the Security Gateway.

i. Click **OK**.

To configure Load Sharing for the Security Gateway, create multiple SRV records with the same priority.

To configure High Availability, create multiple SRV records with different priorities.

Note - If you configure AD based and DNS based configuration, the results are combined according to the specified priority (from the lowest to highest).

Troubleshooting DNS Based Configuration

To troubleshoot issues in DNS based configuration, you can see the SRV records that are stored on the DNS server.

To see SRV records on the DNS server:

Run:

```
C:\> nslookup
 > set type=srv
 > checkpoint_dlp._tcp
```

Example result:

```
C:\> nslookup
 > set type=srv
 > checkpoint_dlp._tcp
Server: dns.company.com
Address: 192.168.0.17
checkpoint_dlp._tcp.ad.company.com SRV service location:
          priority = 0
          weight = 0
          port = 443
          svr hostname = dlpserver.company.com
dlpserver.company.com internet address = 192.168.1.212
>
```

Remote Registry

All of the client configuration, including the server addresses and trust data reside in the registry. You can configure the values before installing the client (by GPO, or any other system that lets you control the registry remotely). This lets you use the configuration when the client is first installed.

Explanation

If you have a way to configure registry entries to your client computers, for example, Active Directory or GPO updates, you can configure the Security Gateway addresses and trust parameters before you install the clients. Clients can then use the configured settings immediately after installation.

To configure the remote registry option:

1. Install the client on one of your computers. The agent installs itself in the user directory, and saves its configuration to `HKEY_CURRENT_USER`.
2. Connect manually to all of the servers that are configured, verify their fingerprints, and click **Trust** on the fingerprint verification dialog box.
3. Configure the client to manually connect to the requested servers (use the **Settings** window).
4. Export these registry keys:
   1. The entire tree:

      `HKEY_CURRENT_USER\SOFTWARE\CheckPoint\UserCheck\Trusted Gateways`
   2. The branch:

      `HKEY_CURRENT_USER\SOFTWARE\CheckPoint\UserCheck\`
      1. The key:

         `Default Gateway`
      2. The key:

         `DefaultGatewayEnabled`
5. Import the exported keys to the endpoint computers before you install the UserCheck Client.

Installing UserCheck Client

After configuring the clients to connect to the Security Gateway, install the clients on the user machines.

1. Get the UserCheck Client MSI file from the Security Gateway in **one** of these ways:

   Download the UserCheck Client from the Security Gateway using an SCP client

   ℹ **Important** - The SCP user must have the default shell `/bin/bash` in Gaia OS on the Security Gateway.

a. Go to this directory:

```
/opt/CPUserCheckPortal/htdocs/UserCheck/client/
```

b. Download this file:

```
Check_Point_UserCheck.msi
```

Download the UserCheck Client from the Security Gateway object in SmartConsole

> **Important** - Before you can use this link, you must install an Access Control policy at least one time so that the UserCheck Portal starts.

a. From the left navigation panel, click **Gateways & Servers**.

b. Double-click the Security Gateway object.

c. From the left tree, click **General Properties**.

d. Enable at least one of these Software Blades:

- Data Loss Prevention
- Access Control:
  - Application Control
  - URL Filtering
  - Content Awareness
- Threat Prevention:
  - Anti-Bot
  - Anti-Virus
  - Threat Emulation
  - Threat Extraction
  - Zero Phishing

e. From the left tree, click **UserCheck**.

f. In the section **UserCheck Client**, click the link **Download Client**.

g. The download opens in your default web browser.

2. Install the UserCheck Client on the user endpoint computers.

   You can use any method of MSI mass configuration and installation that you select.

For example, you can send users an email with a link to install the client. When a user clicks the link, the MSI file automatically installs the client on the computer.

Notes:

- The installation is silent.
  Reboot is not necessary.
- To install the UserCheck Client for all user accounts on a Windows computer, see sk96107.
- To uninstall the UserCheck Client from a Windows computer, see *"Uninstalling UserCheck Client" below*.

Uninstalling UserCheck Client

Default Uninstall Procedure

1. Go to the **Start** menu > **Check Point** > **UserCheck**.
2. Click the "**Uninstall**" shortcut.
3. Follow the instructions on the screen.
4. Restart the endpoint computer.

Manual Uninstall Procedure

If there is no "**Uninstall**" shortcut in the **Start** menu, follow **one** of these procedures:

Uninstall the UserCheck Client manually using Windows Installer

1. Make sure the **UserCheck.exe** application is not running.

   Use Windows Task Manager, or any similar 3rd-party tool.

   If it is currently running, end / kill it.

2. Get the UserCheck Client GUID from the Windows Registry Editor:

   a. Open the Windows Registry Editor (**regedit**):

      i. Click the **Start** menu.

      ii. Enter **regedit**.

      iii. Click **Registry Editor**.

   Alternatively, press the **Windows + R** keys > type **regedit** > click OK / press the Enter key.

   b. Navigate to:

      ```
      Computer\HKEY_CURRENT_
      USER\Software\CheckPoint\UserCheck\1.0
      ```

   c. Right-click the key **PRODUCT_GUID** > click **Modify**.

   d. Copy the entire string **{<GUID>}** and paste it in a plain-text editor.

   e. Click **Cancel** in the Windows Registry Editor.

   f. Close the Windows Registry Editor.

3. In the plain-text editor, prepare the required syntax:

   ```
   %SystemRoot%\SysWOW64\msiexec.exe /x {<GUID you copied from
   Windows Registry Editor>}
   ```

   Dummy example:

   ```
   C:\Windows\SysWOW64\msiexec.exe /x {AAD3D77A-7476-469F-ADF4-
   04424124E91D}
   ```

   Reference:

   https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/msiexec

4. Open Windows Command Prompt:

   a. Click the **Start** menu.

   b. Enter **cmd**.

   c. Click **Command Prompt**.

   Alternatively, press the **Windows + R** keys > type **cmd** > click OK / press the Enter key.

5. Paste the required syntax from the plain-text editor and press the Enter key.

6. Restart the endpoint computer.

Delete the UserCheck client manually from the endpoint computer

1. Make sure the **UserCheck.exe** application is not running.

   Use Windows Task Manager, or any similar 3rd-party tool.

   If it is currently running, end / kill it.

2. Delete the **UserCheck** folder:

> ⓘ **Important** - You must delete this folder for each user on the computer.

   a. In Windows File Manager (or any file manager), go to:

   ```
   C:\Users\%USERNAME%\AppData\Local\CheckPoint\
   ```

   b. Delete this folder:

   ```
   UserCheck
   ```

3. Delete the **UserCheck** branch in the Windows Registry:

   a. Open the Windows Registry Editor (**regedit**):

      i. Click the **Start** menu.

      ii. Enter **regedit**.

      iii. Click **Registry Editor**.

      Alternatively, press the **Windows + R** keys > type **regedit** > click OK / press the Enter key.

   b. Navigate to:

   ```
   Computer\HKEY_CURRENT_
   USER\Software\CheckPoint\UserCheck
   ```

   c. Back up the Windows Registry.

      Refer to the Microsoft article "Windows registry information for advanced users".

   d. Right-click the **UserCheck** branch > click **Delete** > confirm.

   e. Close the Windows Registry Editor.

4. Restart the endpoint computer.

Connecting UserCheck Client to the Security Gateway

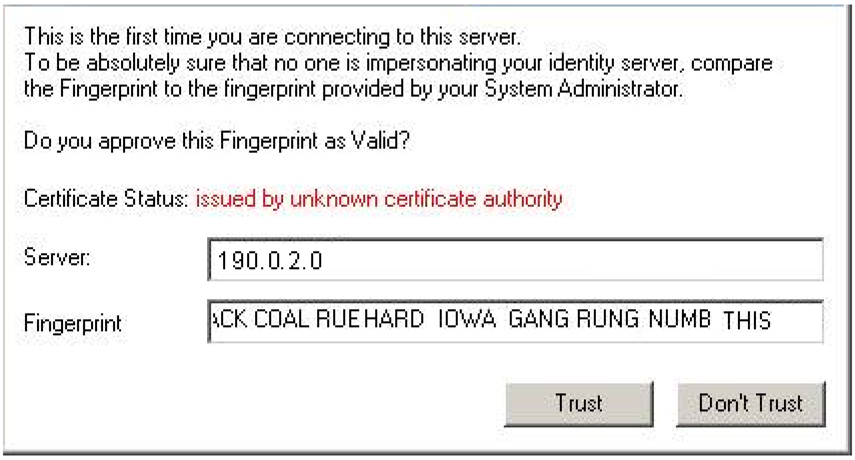
If UserCheck for DLP is enabled on the Security Gateway, users must enter their username and password after the client installs.

When the UserCheck Client is first installed, the UserCheck Client tray icon indicates that it is not connected.

When the UserCheck Client connects to the Security Gateway, the UserCheck Client tray icon shows that the client is active.

The first time that the UserCheck Client connects to the Security Gateway, it asks user to approve of the Security Gateway fingerprint.

Example:



This is the first time you are connecting to this server.
To be absolutely sure that no one is impersonating your identity server, compare the Fingerprint to the fingerprint provided by your System Administrator.

Do you approve this Fingerprint as Valid?

Certificate Status: issued by unknown certificate authority

Server: 190.0.2.0

Fingerprint: \CK COAL RUE HARD IOWA GANG RUNG NUMB THIS

Best Practices:

- Let the users know this happens.
- Use a certificate that is trusted by the certificate authority installed on users' computers.
  Then users do **not** see a message "`Issued by unknown certificate authority`".

Example of message to users about the UserCheck Client installation (for DLP):

```
Dear Users,
Our company has implemented a Data Loss Prevention automation to
protect our confidential data from unintentional leakage. Soon you
will be asked to verify the connection between a small client that
we will install on your computer and the computer that will send
you notifications.
This client will pop up notifications if you try to send a message
that contains protected data. It might let you to send the data
anyway, if you are sure that it does not violate our data-security
guidelines.
When the client is installed, you will see a window that asks if
you trust the DLP server. Check that the server is SERVER NAME and
then click Trust.
In the next window, enter your username and password, and then
click OK.
```

Note - If the UserCheck Client is not connected to the Security Gateway, the behavior is as if the client was never installed. Email notifications are sent for SMTP incidents and the Gaia Portal is used for HTTP incidents.

UserCheck and Check Point Password Authentication

To enable Check Point password authentication:

1. SmartConsole Configuration:

   a. From the top, click **Objects** > **Object Explorer**.

   b. In the left pane, select only **Users/Identities**.

   c. Configure the required settings:

      If the required User object already exists

      i. Double-click the applicable **User** object.

      ii. From the left, click **General**.

      iii. In the **General properties** section, make sure to configure a valid email address.

      iv. Click **OK**.

      If the required User object does not exist yet

      i. Make sure the applicable **User Template** object exists.

         If it does not, from the top toolbar, click **New** > **Users/Identity** > **User Template** > configure the required settings > click **OK**.

      ii. From the top toolbar, click **New** > **Users/Identity** > **User**.

      iii. Select the required **User Template** and click **OK**.

      iv. Configure the required settings:

         - At the top, configure the object name
         - On **General** page, in the **General properties** section, make sure to configure a valid email address.
         - On **Authentication** page, in the **Authentication Method** section, select **Check Point Password** > click **Set new password** > enter the password > click **OK**.

      v. Click **OK**.

   d. Close the **Object Explorer** window.

2. UserCheck Client Configuration:

a. On the endpoint computer, right-click the UserCheck Client icon in the Notification Area (next to the system clock).

b. Click **Settings**.

c. Click **Advanced**.

d. Select **Authentication with Check Point user accounts defined internally in SmartConsole**.

Helping Users

If users require assistance to troubleshoot issues with the UserCheck Client, you can ask them to send you the logs.

To configure the UserCheck Client to generate logs:

1. Right-click the UserCheck Client tray icon and select **Settings**.
2. Click **Log to** and browse to a pathname where the logs are saved.
3. Click **OK**.
4. Make sure that the UserCheck Clients can connect to the Security Gateway and receive notifications.

   See *"Connecting UserCheck Client to the Security Gateway" on page 344*.

To send UserCheck Client logs from the endpoint computer:

1. Right-click the UserCheck Client tray icon and select **Status**.
2. Click **Advanced**.
3. Click the link **Collect information for technical support**.

   The default email client opens, with an archive of the collected logs attached.

Localizing and Customizing the UserCheck Portal

For more information, see sk83700.

Configuring Advanced Threat Prevention Settings

Threat Prevention Engine Settings - Autonomous Threat Prevention

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.

By default, all Security Gateways that are controlled by a single Security Management Server, act the same according to t fail mode configuration of the Security Management Server.

Starting from R81.20, you can control the fail mode configuration for each individual Security Gateway by using the *malware_config* file.

Valid Values

Value	Description
by_policy	This is the default value. Fail mode is determined by the policy.
open	All connections to the specific Security Gateway are allowed in a situation of engine overload or failure.
close	All connections to the specific Security Gateway are blocked in a situation of engine overload or failure.

To set fail mode on a specific Security Gateway:

1. Connect to the command line on the Security Gateway.
2. Log in to the Expert mode.
3. Backup the current `$FWDIR/conf/malware_config` file:

   ```
   [Expert@HostName]# cp $FWDIR/conf/malware_config
   $FWDIR/conf/malware_config_ORIGINAL
   ```

4. Set the required fali mode for the specific Security Gateway:

   To set the fail mode to be controlled by the policy, run:

   ```
   [Expert@HostName]# sed -ie 's/^fail_close=.*$/fail_close=by_
   policy/' $FWDIR/conf/malware_config
   ```

   To set the fail mode to "open", run:

   ```
   [Expert@HostName]# sed -ie 's/^fail_close=.*$/fail_close=open/'
   $FWDIR/conf/malware_config
   ```

   To set fail mode to "close", run:

   ```
   [Expert@HostName]# sed -ie 's/^fail_close=.*$/fail_close=close/'
   $FWDIR/conf/malware_config
   ```

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. Access to the cloud is required if the response is not cached. Resource classification mode determines if the connection is allowed or suspended while the Security Gateway queries the Check Point Online Web Service.

- 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.

  These settings are relevant for Anti-Virus, Anti-Bot and Zero Phishing.

  - **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, and in the background, the Check Point Online Web Service continues the categorization procedure. After the classification is complete, a "Detect" log is generated. The log includes this description: "Connection was allowed because background classification mode was set". 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-Virus, Anti-Bot and Zero Phishing. For example, click **Customize** to set Anti-Bot to Hold mode and Anti-Virus and Zero Phishing to Background mode.

  If you change Background mode to Hold mode, the Security Gateway holds the file and does not send it to the client browser. The Browser shows the file as still being downloaded, but the download is stuck at some point. The Security Gateway continues the download only after the scan is complete or if a timeout occurred at the Security Gateway. If the file is malicious, the Security Gateway stops sending the file.

  Note - If the "Prevent" action is used in the Threat Prevention policy, then a file that Threat Emulation identified as malware in the past, is blocked. The file will not be sent to the destination even in the "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 the Anti-Bot, Threat Emulation, and Anti-Virus, the default session is 10 hours (600 minutes).

To adjust the length of a session

Step	Instructions
1	Go to **Manage & Settings > Blades > Threat Prevention > Advanced Settings > General > Connection Unification > Session unification timeout (minutes)**.
2	Enter the required value.
3	Click **OK**.

Configuring Anti-Bot Whitelist

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

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

Step	Instructions
1	Go to the **Manage & Settings > Blades > Threat Prevention > Advanced Settings > Anti-Bot**.
2	Click the **+** sign.

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

File Type Support for Threat Emulation and Threat Extraction

File Type Support for Threat Emulation and Threat Extraction in Autonomous Threat Prevention is not configured in Engine Settings. To configure file type support settings for Autonomous Threat Prevention, go to Security Policies > Autonomous Policy > File Protections.

Optimizing IPS - Autonomous Threat Prevention

IPS is a robust solution which protects your network from threats. Implementation of the recommendations in this chapter helps maintaining 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

Step	Instructions
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.

Step	Instructions
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 the Threat Prevention Policy.

Configuring Advanced Threat Emulation Settings - Autonomous Threat Prevention

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

In SmartConsole, go to **Security Policies > Threat Prevention** > **Autonomous Policy** > **Autonomous Policy Tools**.

Step	Instructions
1	Go to **Updates**. The **Updates** page opens.
2	Under **Threat Emulation**, click **Schedule Update**.
3	Select or clear these settings: ■ **Enable Threat Emulation engine scheduled update** ■ **Enable Threat Emulation images scheduled update**

Step	Instructions
4	To configure the schedule for Threat Emulation engine or image updates, click **Configure**.
5	Configure the automatic update settings to update the database: ■ To update every few hours, select **Update every**, and configure the number of hours, minutes, and seconds. ■ To update daily, select **Update at** > **Daily** and select the hour of update. ■ To update once or more for each week or month: 1. Select **At** and enter the time of day. 2. Click **Days**. 3. Click **Days of week** or **Days of month**. 4. Select the applicable days.
6	Click **OK**, and install the Threat Prevention policy.

Updating Threat Emulation Images Manually

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

The default setting is to download the package once a week on Sunday. If Sunday is a work day, we recommend that you change the update setting to a non-work day.

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

In SmartConsole, go to **Security Policies > Threat Prevention** >**Autonomous Policy** > **Autonomous Policy Tools**.

Step	Instructions
1	Go to **Updates**. The **Updates** page opens.
2	Under **Threat Emulation**, click **Update Images**.
3	Select a gateway. Click **OK**.
4	Install the Threat Prevention policy.

Fine-Tuning the Threat Emulation Appliance

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

Configuring the Emulation Limits

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

- Maximum file size (up to 100,000 KB)
- Maximum time that the Software Blade does emulation
- Maximum time that a file waits for emulation in the queue (for Threat 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:

- **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.

To configure the emulation limits

Step	Instructions
1	In SmartConsole, go to **Manage & Settings** > **Blades** > **Threat Prevention** > **Advanced Settings**. The **Threat Prevention Engine Settings** window opens.
2	Go to **Threat Emulation** tab > **Emulation Limits**.
3	Configure the **Maximum file size for emulation** and the **Maximum file time in queue**.
4	From **When limit is exceeded traffic is accepted with track**, select the action if a file is not sent for emulation: ■ **None** - No action is done ■ **Log** - The action is logged ■ **Alert** - An alert is sent to SmartView Monitor
5	Click **OK**, and then install the policy.

Changing the Size of the Local Cache

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

To change the size of the local cache

Step	Instructions
1	In SmartConsole, select **Manage & Settings** > **Blades** > **Threat Prevention** > **Advanced Settings**. The **Threat Prevention Engine Settings** window opens.
2	Go to the **Threat Emulation** tab > **Advanced Settings**.
3	In **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 install the policy.

Threat Prevention Scheduled Updates - Autonomous Threat Prevention

Introduction to Scheduled Updates

Check Point wants the customer to be protected. When a protection update is available, Check Point wants the configuration to be automatically enforced on the gateway. You can configure automatic gateway updates for Anti-Virus, Anti-Bot, Threat Emulation and IPS.

For Anti-Virus, Anti-Bot and Threat Emulation, the gateways download the updates directly from the Check Point cloud.

For IPS, prior to R80.20, the updates were downloaded to the Security Management Server, and only after you installed policy, the gateways could enforce the updates. Starting from R80.20, the gateways can directly download the updates. For R80.20 gateways and higher with no internet connectivity, you must still install policy to enforce the updates.

When you configure automatic IPS updates on the gateway, the action for the newly downloaded protections is by default according to the profile settings.

IPS, Anti-Virus and Anti-Bot updates are performed every two hours by default. Threat Emulation engine updates are performed daily at 05:00 by default, and Threat Emulation image updates are performed daily at 04:00 by default.

Configuring Threat Prevention Scheduled Updates

To configure Threat Prevention scheduled updates

In SmartConsole, go to **Security Policies** > **Threat Prevention** > **Autonomous Policy** > **Autonomous Policy Tools**

Step	Instructions
1	Go to **Updates**.
2	Go to the section about the required Software Blade, click **Schedule Update**. The **Scheduled Updates** window opens.
3	Make sure **Enable <blade> scheduled updates** is selected.
4	**For IPS, there are 2 more configuration options for scheduling Security Management Server updates** ■ **On successful IPS update on the Security Management Server, install policy on the Security Gateway** - automatically installs the policy on the devices you select after the IPS update is completed. Click **Configure** to select these devices. **Note** - In pre-R80 gateways, IPS was part of the Access Control policy. Therefore, when you select this option, a message shows which indicates that for pre-R80 gateways, the Access Control policy is installed and for R80 and above gateways, the Threat Prevention policy is installed. ■ **Perform retries on the Security Management Server when the update fails** - lets you configure the number of tries the scheduled update makes if it does not complete successfully the first time.
5	Click **Configure**.
6	**In the window that opens, set the Time of event** ■ **Update every**: set the update frequency by hours OR - ■ **Update at**: set the update frequency by days: • **Daily** - Every day • **Days in week** - Select days of the week • **Days in month** - Select dates of the month
7	Click **OK**.
8	Click **Close**.
9	Install the Threat Prevention policy.

Checking Update Status

In **Autonomous Policy Tools** > **Updates**, a message shows which indicates the number of gateways which are up-to-date.

To check if the protections are updated on a specific gateway

Step	Instructions
1	In the **Gateways & Servers** view, select a gateway.
2	Right-click the gateway, and select the **Monitor** button. The **Device & License Information** window opens.
3	The **Device Status** page shows the gateway status.

Turning Off IPS Automatic Updates on a Gateway

You can turn off automatic IPS updates on a specific gateway.

To turn off automatic IPS updates on a specific gateway

Step	Instructions
1	In SmartConsole, to the **Gateways & Servers** view, and double-click a gateway. The gateway properties window opens.
2	In the navigation tree, go to **IPS**.
3	In **IPS Update Policy**, select **Use IPS management updates**.
4	Click **OK**.
5	Install the Threat Prevention Policy.

IPS Updates Use Cases

These scenarios explain how an upgrade of the Security Gateways or the Security Management Server or both, affects the Scheduled Updates configuration.

Scenario 1:

Upgrading the Security Management Server to R80.20, and not upgrading the gateways to R80.20

If you do not upgrade the Security Gateways, then after the upgrade, the Security Gateways are still not able to receive the updates independently, only through the Security Management Server. In this case, the configuration stays the same compared to before the upgrade: Scheduled Updates will be enabled or disabled on the Security Management Server, depending on the configuration before the upgrade.

Scenario 2:

Upgrading the Security Gateways to R80.20 (with or without Security Management Server upgrade)

- If, before the upgrade, Scheduled Updates were configured on the Security Management Server with automatic policy installation, then after the upgrade, automatic IPS updates are still enabled on the Security Management Server, and are also applied to the upgraded gateways.
- If Scheduled Updates were disabled on the Security Management Server before the upgrade, then they remain disabled after the upgrade, both on the Security Management Server and the gateways.
- If, before the upgrade, Scheduled Updates were configured on the Security Management Server without automatic policy installation - then during the first policy installation after upgrade, a message shows which indicates that Security Gateways R80.20 and higher automatically update the IPS Protections. For Security Gateways R80.10 and lower, you must install policy to apply the updates.

SSH Deep Packet Inspection - Autonomous Threat Prevention

You can use the SSH Deep Packet Inspection ("SSH DPI") feature to decrypt and encrypt SSH traffic and let the Threat Prevention solution protect against advanced threats, bots, and other malware.

Key Motivation and Goals for SSH DPI

- Block SSH attacks
- Block the transmission of viruses through SCP and SFTP protocols
- Prevent brute force password cracking of SSH/SFTP servers
- Prevent the dangerous use of SSH Port forwarding
- Prevent using simple passwords like "password" when connecting to SSH/SFTP
- Prevent using vulnerable cryptography
- Prevent using vulnerable SSH clients and servers
- Prevent using port 22 for other protocols except for SSH

Note - Currently, these blades are supported: Anti-Virus, IPS and Threat Emulation.

SSH DPI Architecture

Similar to HTTPS Inspection, SSH DPI works as the man-in-the-middle.

```
SSH_CLIENT <=> Security Gateway <=> SSH_SERVER
```

Note - All TCP traffic should pass through the Security Gateway.

Enabling SSH Deep Packet Inspection on the Security Gateway

To enable SSH DPI

1. On the Security Gateway, Run:

   ```
   cpssh_config ion
   ```

2. Run this command:

   ```
   fw fetch local
   ```

   Or install the Access Control policy in SmartConsole

Disabling SSH Deep Packet Inspection on the Security Gateway

To disable SSH DPI

On the Security Gateway, run:

```
cpssh_config ioff
```

Viewing SSH DPI Status

To view the status of SSH DPI

On the Security Gateway, run:

```
cpssh_config istatus
```

Note - All SSH inspection settings will be saved after Security Gateway reboot.

Configuring SSH Deep packet Inspection

Add an inspected SSH server

To add a non-transparent inspected SSH sever

Note - The Security Gateway introduces the Server to the Client with a new public key.

Step	Instructions
1	Copy the SSH server's public key to the Security Gateway **Note** - In Linux, the key on the Security Gateway is `/etc/ssh/ssh_host_rsa_key.pub`

2	On the Gateway, run this command:
	`cpssh_config -s -g SERVER_NAME -e /PATH/TO/RSA/KEY/THAT/YOU/COPIED.pub`
	For example:
	If your ssh sever host is `my_ssh_server_host.com`, and you copy the key to `/home/admin/mykey.pub`, then you must run this command:
	`cpssh_config -s -g my_ssh_server_host.com -e /home/admin/mykey.pub`

3	Repeat steps 1 and 2 for every SSH server to be added.

To add a transparent inspected SSH sever

Note - The Security Gateway introduces the Server to the Client with the original public key.

Step	Instructions
1	Copy the SSH server's public and private key to the Security Gateway. **Note** - The keys on the Security Gateway are: - `/etc/ssh/ssh_host_rsa_key.pub` - `/etc/ssh/ssh_host_rsa_key`

2	Run this command:
	`cpssh_config -s -a <SERVER_NAME> -e </PATH/TO/RSA/KEY/THAT/YOU/COPIED>.pub -i </PATH/TO/RSA/PRIVATE_KEY/THAT/YOU/COPIED>.pub`
	For example:
	If your ssh sever host is `my_ssh_server_host.com` and you copy the keys to `/home/admin/mykey.pub`, then you must run this command:
	`cpssh_config -s -a my_ssh_server_host.com -e /home/admin/mykey.pub -i /home/admin/mykey`

3	Repeat steps 1 and 2 for every SSH server to be added.

To disable SSH port forwarding

On the Security Gateway, run:

```
cpssh_config -w Global -y Port_fowarding_Enabled -u 0
```

To run SSH DPI on a non-standard port (not TCP port 22)

Step	Instructions
1	In SmartConsole, from the right panel, select **Objects** > **Services**.
2	Right-click on the **TCP**, and then choose **NEW TCP**.
3	Enter a name for the new TCP service: 1. Select **General** > **Protocol** as **SSH2**. 2. Choose **Match By** > **Customize to new port**, and then set the port. For example, `22222`
4	Install the Access Control Policy.

SSH Deep Packet Inspection Settings

To view all settings

```
cpssh_config -q
```

To view available options for key exchange

On the Security Gateway, run:

```
cpssh_config -w KeyExchange
```

To view available options for cipher

On the Security Gateway, run:

```
cpssh_config -w Cipher
```

To view available options for MAC

On the Security Gateway, run:

```
cpssh_config -w Mac
```

To view available options for Hostkey

On the Security Gateway, run:

```
cpssh_config -w Hostkey
```

To set option

On the Gateway, run:

```
cpssh_config -w Cipher -y <OPTION> -u <VALUE>
```

For example, to disable `aes128-cbc`:

```
cpssh_config -w Cipher -y aes128-cbc -u 0
```

Client Authorization (authorization by keys - without passwords)

To enable client authorization

Step	Instructions
1	Configure the SSH server to do the authorization through keys. This is done by copying the public key from the client to the server in `~/.ssh/authorized_keys/`. For more details, see askubuntu.com.
2	Copy SSH client public and private keys (`mykey.pub` and `mykey`) to the Security Gateway.
3	Copy the SSH server public key (`serverkey.pub`) to the Security Gateway.
4	Run this command: `cpssh_config -c -a <admin_username>@<my_ssh_server> -e /home/admin/mykey.pub -l /home/admin/serverkey.pub -i /home/admin/mykey` Where: ▪ `admin_username` is the username on the SSH server ▪ `my_ssh_server` is the resolvable hostname of IP address of the SSH server ▪ `mykey.pub` and `mykey` are pairs of client keys

Cluster

Currently, we do not support keys syncing between cluster nodes automatically.

To manually sync the Cluster Members (after adding/modify/deleting keys)

On the Cluster Member, on which the keys were added, run these commands in the Expert mode:

```
cd /etc/
tar -cvvf ssh.tar ssh
scp ssh.tar admin@<IP_OF_OTHER_CLUSTER_MEMBER>:/tmp
```

On the other cluster members, run these commands in the Expert mode:

```
mv -v /tmp/ssh.tar /etc/
cd /etc/
mv -v ssh ssh_backup
tar -xvvf ssh.tar
killall -s HUP cpsshd
```

Troubleshooting

To make sure that SSH DPI is enabled

Connect to an SSH server with the `telnet` command.

The output should show "**SSH-2.0-cpssh**"

Example:

```
$ telnet 172.23.43.29 22
Trying 172.23.43.29...
Connected to 172.23.43.29.
Escape character is '^]'.
SSH-2.0-cpssh
```

Debugging

To collect Kernel Debug

1. Enable the debug flag "`cpsshi`" in the kernel debug module "`fw`".
2. Enable all the debug flags in the kernel debug module "`CPSSH`".

For instructions on the debugging procedures, see the *R81.20 Quantum Security Gateway Guide* > Chapter *Kernel Debug on Security Gateway*.

To collect User Space Debug

1. Create and then run this shell script:

   ```
   #!/bin/sh
   echo > $FWDIR/log/cpsshd.elg
   for PROC in $(pidof cpsshd)
   do
       fw debug $PROC on ALL=6
   done
   tail -f $FWDIR/log/cpsshd.elg
   ```

   To stop the output, press the **CTRL+C** keys.

2. Replicate the issue, or wait for it to occur.

3. Disable the User Space logs with this command:

   ```
   for PROC in $(pidof cpsshd) ; do fw debug $PROC off ALL=6 ;
   done
   ```

4. Examine the log files:

   ```
   $FWDIR/log/cpsshd.elg*
   ```

The Check Point ThreatCloud - Autonomous Threat Prevention

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-VirusSoftware 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.

You can access the ThreatCloud repository from ThreatWiki: In a web browser, go to *Check Point ThreatWiki*.

- In SmartConsole, go to **Security Policies** > **Threat Prevention** > **Autonomous Policy** > in the **Autonomous Policy Tools** section, click **ThreatWiki**.

Data which Check Point Collects

When you enable information collection, the Check Point Security Gateway collects and securely submits event IDs, URLs, and external IP addresses 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 PointSecurity Gateway. It includes the event ID, URL, and external IP addresses. Note that the data does not contain confidential data or internal resource information. The source IP address is obscured. Information sent to the Check Point Lab is stored in an aggregated form.

Configuring Check Point ThreatCloud on a Gateway

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

Step	Instructions
1	Double-click the Security Gateway. The gateway window opens and shows the **General Properties** page.

Step	Instructions
2	Configure the settings for the Anti-Bot and Anti-Virus: 1. From the navigation tree click **Anti-Bot and Anti-Virus**. The **Anti-Bot and Anti-Virus** page opens. 2. To configure a Security Gateway to share Anti-Bot and Anti-Virus information with the ThreatCloud, select **Support the global community by sharing attack data with Check Point ThreatCloud**. - If you do not select this check box, no information is shared with Check Point about the attack. If you select this checkbox, you can select which information is exposed about the attack: ■ **Receive alerts about threats (requires sharing additional end-user data)** - all attack information is exposed. ■ **Anonymize collected data** (selected by default). Select one of these options: • **End-user data** (selected by default) - End-user information is anonymized, gateway is exposed. • **End-user data and customer identity** - both end-user and gateway data are hidden.
3	Configure the settings for IPS: 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**. **Note** - To disable sharing IPS information with the Check Point cloud, clear this option.
4	Click **OK**.

Check Point ThreatCloud Network

Check Point ThreatCloud is a dynamically updated service that is based on an innovative global network of threat sensors and organizations that share threat data and collaborate to fight against modern malware. Customers can send their own threat data to the ThreatCloud and receive protection updates with enriched threat intelligence.

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

When you send files to the ThreatCloud service for emulation, your network gets up-to-date threat information and operating system environments. The connection to the ThreatCloud is enabled by default. This connection gives many management features. We recommend to enable it. If you want to block this connection, you can change the default setting.

To block ThreatCloud

Step	Instructions
1	From the menu bar, click **Global Properties**.
2	In the navigation tree, go to **Data Access Control**
3	Clear: **Help Check Point Improve the product by sending anonymous information**.
4	Publish the SmartConsole session.
5	Restart SmartConsole.
6	Install the Policy.

Autonomous Threat Prevention Overview Section

The **Overview** section in the Autonomous Threat Prevention view provides information about how Autonomous Threat Prevention handles malware attacks.

The **Overview** section shows the number of files which were deleted, inspected, sandboxed and so on, and other information on blocking attacks. To see the logs for each type of action done by Autonomous Threat Prevention, enter these queries in the **Logs & Monitor** view > **Logs** view or **Logs & Monitor** > **SmartView** > **Logs** view:

Inspected Files

```
'(blade:"Anti-Virus" AND file_name:*) OR (blade:"Threat Emulation"
AND NOT verdict:Error) AND action:(Accept OR Allow OR Block OR
Detect OR Drop OR "HTTPS Inspect" OR Inspect OR Prevent OR
Reject)'
```

Sandboxed Files

```
'blade:"Threat Emulation" AND NOT verdict:Error AND action:(Accept
OR Allow OR Block OR Detect OR Drop OR "HTTPS Inspect" OR Inspect
OR Prevent OR Reject)'
```

Sanitized Files

```
'blade:"Threat Extraction" AND action:Extract'
```

Blocked Malicious Files

```
'((blade:"Threat Emulation") OR (blade:"Anti-Virus" AND
"signature") OR (blade:IPS AND (("Adobe Reader Violation" OR
"Content Protection Violation" OR "Instant Messenger" OR "Adobe
Flash Protection Violation")))) AND action:(Block OR Drop OR
Prevent)'
```

Detected Malicious Files

```
'(blade:"Anti-Virus" AND file_name:*) OR (blade:"Threat Emulation"
AND NOT verdict:Error) AND action:Detect'
```

Blocked Attempts To Access Malicious Sites

```
'NOT SMTP AND action:(Block OR Drop OR Prevent) and ((blade:IPS
AND ("Adobe Flash Protection Violation" OR "Adobe Shockwave
Protection Violation" OR "Web Client Enforcement Violation" OR
"Exploit Kit")) OR (blade:"Anti-Virus" AND ("URL Reputation" OR
"DNS Reputation")))'
```

Detected Phishing Attempts

```
'blade:"Zero Phishing" AND action:(Detect)'
```

Blocked Phishing Attempts

```
'blade:"Zero Phishing" AND action:(Prevent)'
```

Blocked Targeted Host Attacks

```
'blade:IPS AND action:(Block OR Drop OR Prevent) NOT ("SMTP" OR
"Adobe Reader Violation" OR "Content Protection Violation" OR
"Mail Content Protection Violation" OR "SMTP Protection Violation"
OR "Phishing Enforcement Protection" OR "Adobe Flash Protection
Violation" OR "Adobe Reader Violation" OR "Content Protection
Violation" OR "Instant Messenger" OR "Adobe Flash Protection
Violation" OR "Scanner Enforcement Violation" OR "Port Scan" OR
"Novell NMAP Protocol Violation" OR "Adobe Flash Protection
Violation" OR "Adobe Shockwave Protection Violation" OR "Web
Client Enforcement Violation" OR "Exploit Kit")'
```

Monitoring Threat Prevention - Autonomous Threat Prevention

Networks today are more exposed to cyber-threats than ever. This creates a challenge for organizations in understanding the security threats and assessing damage. SmartConsole helps the security administrator find the cause of cyber-threats, and remediate the network.

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

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

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

Log Sessions

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

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

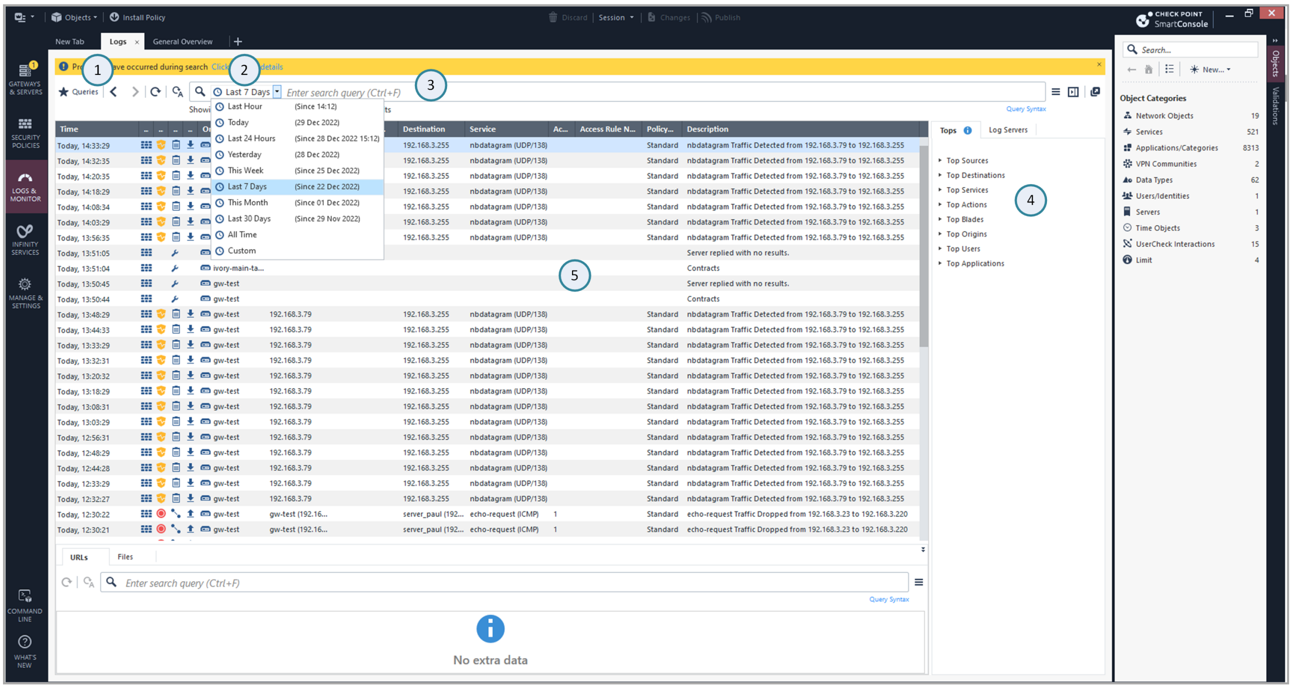
Session duration for all connections that are prevented or detected in the Rule Base is, by default, 10 hours. You can change this in the **Manage & Settings** view in SmartConsole > **Blades** > **Threat Prevention > Advanced Settings > General > Connection Unification**.

Using the Log View

In SmartConsole

Step	Instructions
1	Go to **Logs and Monitoring** > **View**.
2	Click **New**, and then select **New View**.
3	In the **New View** window, enter: ■ **Name** ■ **Category** - For example, select **Access Control** ■ **Description** - (optional)
4	In the new window that opens, create a query. Click **Options** > **View Filter** and select **Blade and App control**.
5	To customize how you see the data that comes back from the query, click **Add Widget**. Start with a Timeline of all events. In **Table**, you can create a table that contains multiple field such as user, application name, and the amount of traffic. Additional widgets for use: map, infographic, rich text, chart, and container (for multiple widgets). After you save the changes in SmartConsole, you can schedule and get an automatic email at multiple intervals.

This is an example of the Log view:



Time	Or		Destination	Service	Ac...	Access Rule N...	Policy...	Description
Today, 14:33:29			192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 14:32:35			192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 14:20:35			192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 14:18:29			192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 14:08:34			192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 14:03:29			192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:56:35			192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:51:05								Server replied with no results.
Today, 13:51:04	ivory-main-ta...							Contracts
Today, 13:50:45	gw-test							Server replied with no results.
Today, 13:50:44	gw-test							Contracts
Today, 13:48:29	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:44:33	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:33:29	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:32:31	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:20:32	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:18:29	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:08:31	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 13:03:29	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 12:56:31	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 12:48:29	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 12:44:28	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 12:33:29	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 12:32:27	gw-test	192.168.3.79	192.168.3.255	nbdatagram (UDP/138)			Standard	nbdatagram Traffic Detected from 192.168.3.79 to 192.168.3.255
Today, 12:30:22	gw-test	gw-test (192.16...	server_paul (192...	echo-request (ICMP)	1		Standard	echo-request Traffic Dropped from 192.168.3.23 to 192.168.3.220
Today, 12:30:21	gw-test	gw-test (192.16...	server_paul (192...	echo-request (ICMP)	1		Standard	echo-request Traffic Dropped from 192.168.3.23 to 192.168.3.220

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.

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.

Example

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

Creating Custom Queries

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

To modify a predefined query:

Click inside the query box to add search filters.

To save the new query in the Favorites list

Step	Instructions
1	Click **Queries** > **Add to Favorites**. The **Add to Favorites** window opens.
2	Enter a name for the query.

Step	Instructions
3	Select or create a new folder to store the query.
4	Click **Add**.

Selecting Criteria from Grid Columns

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

To select query criteria from grid columns

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

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

Manually Entering Query Criteria

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

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

Selecting Query Fields

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

To select field criteria

Step	Instructions
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.

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 at a later time.

To see a packet capture

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

Advanced Forensics Details

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

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

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

Example

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

Threat Analysis in the Logs & Monitor View

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

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

Available options

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

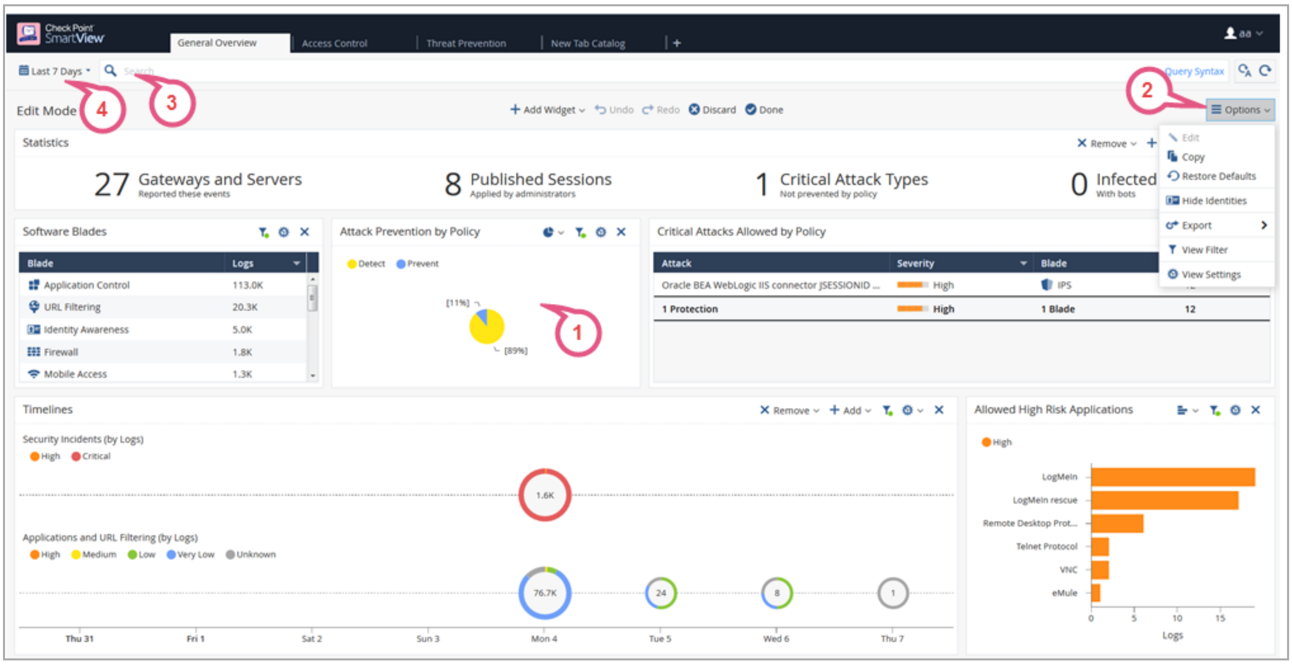
Views

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

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

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

Example View window



Blade	Logs
Application Control	113.0K
URL Filtering	20.3K
Identity Awareness	5.0K
Firewall	1.8K
Mobile Access	1.3K

Attack	Severity	Blade	
Oracle BEA WebLogic IIS connector JSESSIONID ...	High	IPS	
1 Protection	High	1 Blade	12

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

For more information on using and customizing reports, see the *R81.20 Logging and Monitoring Administration Guide*.

Reports

A report consists of multiple views and a cover page. There are several predefined reports, and you can create new reports. A report gives more details than a view. Reports can be customized, filtered, generated and scheduled. You cannot drill down into a report.

Click the (+) tab to open a catalog of all views and reports, predefined and customized. To open a report, double-click the report or select the applicable report and click **Open**.

For more information on using and customizing reports, see the *R81.20 Logging and Monitoring Administration Guide*

Log Fields

See *"Log Fields" on page 496*.

How to Investigate Threat Prevention Events

- *"Cyber Attack View - Gateway" on page 433*
- *"MITRE ATT&CK" on page 490*

Troubleshooting - Autonomous Threat Prevention

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.

Users stopped receiving emails

Step	Instructions

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 Security 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 the scrub daemon, 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`
	Important - When empty the queue, you lose 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 Security 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.

Step	Instructions
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 Security 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 Security Gateway:

Step	Instructions

1	Make sure that the disk or directories on the Security Gateway are not full.
	1. Run:
	`df -h /`
	2. Run:
	`df -h /var/log`

2	Make sure directories used by Threat Extraction can be written to. Run: 1. `touch /tmp/scrub/test` 2. `touch /var/log/jail/tmp/scrub/test` 3. `touch $FWDIR/tmp/email_tmp/test`

CPView shows Threat Extraction errors

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

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**.

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

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

Step	Instructions
1	In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway
2	From the left tree, click **IPS**.
3	In the **Activation Mode** section, click **Detect Only**.
4	Click **OK**.
5	Install the Access Control policy. All protections set to Prevent allow traffic to pass, but continue to track threats according to the Track setting.

Common Features in Custom Threat Prevention and Autonomous Threat Prevention

The sections in this chapter describe features that apply in the same way to Custom Threat Prevention and Autonomous Threat Prevention.

Using Anti-Spam and Mail

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.

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

Step	Instructions
1	In SmartConsole, select **Manage & Settings > Blades > Anti-Spam & Mail** > and click **Configure in SmartDashboard**. SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2	On the **Overview** page, under **Content based Anti-Spam**, click **Settings**.
3	Use the slider to select an Anti-Spam policy protection level.
4	Select flagging options.
5	In the **Security Gateway Engine settings** section, set a maximum data size to scan.

Step	Instructions
6	Select **Tracking Options** for **Spam**, **Suspected Spam**, or **Non Spam**. Tracking options include ■ **None (no logging)** ■ **Log** ■ **Popup Alert** ■ **Mail Alert** ■ **SNMP Trap Alert** ■ **User Defined Alert**
7	Click **Save**, and then close SmartDashboard.
8	In SmartConsole, install the Access Control policy.

Configuring an IP Reputation Policy

This window enables IP reputation, an Anti-Spam mechanism that checks the IP address of the message sender (contained in the opening SYN packet) against a dynamic database of suspect IP addresses. If, according to the IP reputation service, the originating network has a reputation for sending spam, then the spam session is blocked at connect time. This way, the IP reputation feature creates a list of trusted email sources.

To configure an IP reputation policy

Step	Instructions
1	In SmartConsole, select **Manage & Settings > Blades > Anti-Spam & Mail** > and click **Configure in SmartDashboard**. SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2	On the **Overview** page, under **IP Reputation Anti-Spam**, click **Settings**.
3	Use the slider to select an IP Reputation Policy ■ **Off** - IP Reputation service is disabled ■ **Monitor only** - 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

Step	Instructions
4	Select tracking options for **Spam**, **Suspected Spam**, or **Non spam**. Tracking options include ▪ **None (no logging)** ▪ **Log** ▪ **Popup Alert** ▪ **Mail Alert** ▪ **SNMP trap alert** ▪ **User Defined Alert**
5	Click **Save**, and then close SmartDashboard.
6	In SmartConsole, install the Access Control policy.

Configuring a Block List

You can configure a list of email sources to block according to the sender's name, domain name, or IP address.

To configure a block list

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

Step	Instructions
7	Click **Save**, and then close SmartDashboard.
8	In SmartConsole, install the Access Control policy.

Configuring Anti-Spam SMTP

SMTP traffic can be scanned according to direction or IP addresses.

To configure Anti-Spam SMTP

Step	Instructions
1	In SmartConsole, select **Manage & Settings > Blades > Anti-Spam & Mail** > and click **Configure in SmartDashboard**. SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2	From the navigation tree, click **Advanced** > **SMTP**.
3	Make sure that **Scan SMTP traffic with Anti-Spam engine for Anti-Spam, IP reputation and Block list protection** is selected.
4	Select to scan SMTP traffic **By Mail Direction** or **By IPs**. 1. If you selected scan **By IPs**, click **Add Rule** to configure rules for IP addresses to scan. 2. If you selected scan **By Mail Direction**, select a scanning direction for: ■ Incoming files ■ Outgoing files ■ Internal files through the gateway
5	Select **Activate Continuous Download** to avoid client time-outs when large files are scanned. (See *"Adaptive Continuous Download" on page 383* for further information).
6	Click **Save**, and then close SmartDashboard.
7	In SmartConsole, install the Access Control policy.

Configuring Anti-Spam POP3

POP3 traffic can be scanned according to direction

Step	Instructions
1	In SmartConsole, select **Manage & Settings > Blades > Anti-Spam & Mail** > and click **Configure in SmartDashboard**. SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2	From the navigation tree, click **Advanced** > **POP3**.
3	Make sure that **Scan POP3 traffic with Anti-Spam engine for Anti-Spam, IP reputation and Block list protection** is selected.
4	Select to scan POP3 traffic **By Mail Direction** or **By IPs**.
5	If you selected scan **By IPs**, click **Add Rule** to configure rules for IP addresses to scan.
6	If you selected scan **By Mail Direction**, select a scanning direction for: ■ Incoming mail ■ Outgoing mail ■ Internal mail
7	Select **Activate Continuous Download** to avoid client time-outs when large files are scanned. (See *"Adaptive Continuous Download" on page 383* for further information).
8	Click **Save**, and then close SmartDashboard.
9	In SmartConsole, install the Access Control policy.

Configuring Network Exceptions

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

To exclude sources and destinations

Step	Instructions
1	In SmartConsole, select **Manage & Settings > Blades > Anti-Spam & Mail** > and click **Configure in SmartDashboard**. SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2	From the navigation tree click **Advanced** > **Network Exceptions**.

Step	Instructions
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.
	In SmartConsole, install the Access Control policy.

Configuring an Allow List

You can configure a list of allowed email sources according to the sender's name and name, or according to the IP address.

To configure an allow list

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

Selecting a Customized Server

You can select an alternative Detection Center for Anti-Spam analysis.

To select a Detection Center

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

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 a Disclaimer

You can create your own custom disclaimer notice.

To configure a disclaimer

Step	Instructions
1	In SmartConsole, select **Manage & Settings > Blades > Anti-Spam & Mail** > and click **Configure in SmartDashboard**. SmartDashboard opens and shows the **Anti-Spam & Mail** tab.
2	From the navigation tree, select **Advanced** > **Disclaimer**.
3	Select **Add disclaimer to email scanned by Anti-Virus and Anti-Spam engines**.
4	In the text box, type your disclaimer notice.
5	Click **Save**, and then close SmartDashboard.
6	In 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 and reports of the Anti-Spam activity, customize these views and reports, or generate new ones (see *"Threat Analysis in the Logs & Monitor View" on page 276*).

Threat Prevention API

What is the Threat Prevention Web API?

The Security Gateways inspect files intercepted from traffic. With the Threat Prevention API, you can upload files which were intercepted by traffic for inspection by the Security Gateways.

For example: The organizational Human Resources portal receives CVs from external users. When the files are sent directly to the Security Gateway, the Threat Emulation process can take a few minutes, during which the user must wait for a message that the file was uploaded. To improve user experience and prevent the wait, you can keep these files in a separate container, let the user know that the files were uploaded, and only then use the API to send the files for inspection by the Security Gateway.

There are two types of Threat Prevention APIs:

- **Cloud API** - Used for:
    - Accessing the Security Gateway - Supports Anti-Virus and Threat Emulation. For more details, see the Threat Prevention API Reference Guide.
    - Directly accessing ThreatCloud - Supports Threat Extraction, Anti-Virus and Threat Emulation. For more details, see the *Threat Prevention API Reference*
- **Local API on the Security Gateway** - Supports Threat Extraction, Anti-Virus and Threat Emulation. For more details, see *"Using the Local Threat Extraction Web API" below* and sk137032.

Using the Local Threat Extraction Web API

To use the Threat Extraction API, you need to create an API key. After you create the API key, you can use it to connect to the gateway and send files for extraction.

To create the Threat Extraction Web API key

Step	Instructions
1	In SmartConsole, double-click the Security Gateway.
2	From the navigation tree, select **Threat Extraction**.
3	Select **Enable API**.
4	Install Policy.

The Web API key is created.

After the Web API key is created, you can deploy it to the clients.

To find the Web API key

Step	Instructions
1	Open the CLI.
2	Edit this file: `vi /opt/CPUserCheckPortal/phpincs/conf/TPAPI.ini`
3	The API key is in the `api_key` field. **Note** - You can change the api_key in the `TPAPI.ini` file. Changes are effective immediately.

For more information, see sk113599.

HTTPS Inspection

HTTPS Internet traffic uses the TLS (Transport Layer Security) 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. HTTPS Inspection lets the Security Gateway intercept TLS connections and decrypt their traffic for inspection by the enabled Software Blades.

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.

The 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.

For information on what's new in HTTPS Inspection starting from R80.20, see sk163594.

Intercepting HTTPS Connections

Outbound HTTPS Connections

Outbound connections are HTTPS connections that arrive from an internal client and connect to an external server.

Outbound connection flow

1. An HTTPS request (from an internal client to an external server) arrives at the Security Gateway.
2. The Security Gateway intercepts the HTTPS request.
3. The Security Gateway determines whether the HTTPS request matches an existing HTTPS Inspection rule:
   - If the HTTPS request does **not** match a rule, the Security Gateway does not intercept the HTTPS connection. In this case, HTTPS Inspection is bypassed.
   - If the HTTPS request matches a rule, the Security Gateway intercepts the HTTPS connection and continues to the next step.
4. The Security Gateway validates the certificate of the external server.

   By default, the Security Gateway uses the Online Certificate Status Protocol (OCSP) standard to check for certificate revocation.

   If the certificate does not support OCSP, the Security Gateway uses the Certificate Revocation List (CRL) to check for certificate revocation.
5. The Security Gateway creates a new certificate for the connection to the external server.
6. The Security Gateway decrypts HTTPS traffic.
7. The Security Gateway calls the enabled Software Blades to inspect the decrypted HTTPS connection.
8. If the Security Policy allows this traffic, the Security Gateway encrypts the HTTPS connection.
9. The Security Gateway sends the HTTPS request to the external server.

Inbound HTTPS Connections

Inbound connections are HTTPS connections that arrive from an external client and connect to a server in the DMZ or the internal network.

Inbound connection flow

1. An HTTPS request (from an external client to an internal server) arrives at the Security Gateway.

   Note - By design, the Security Gateway/Cluster is intentionally configured not to perform HTTPS Inspection on traffic directed towards it. To change this behavior, follow sk114574.

2. The Security Gateway intercepts the HTTPS request.
3. The Security Gateway determines whether the HTTPS request matches an existing HTTPS Inspection rule:
   - If the HTTPS request does **not** match a rule, the Security Gateway does not intercept the HTTPS connection.
   - If the HTTPS request matches a rule,the Security Gateway intercepts the HTTPS connection and continues to the next step.
4. The Security Gateway uses the certificate for the internal server to create an HTTPS connection with the external client.
5. The Security Gateway creates a new HTTPS connection with the internal server.
6. The Security Gateway decrypts the HTTPS connection.
7. The Security Gateway calls the enabled Software Blades to inspect the decrypted HTTPS traffic.
8. If the Security Policy allows this traffic, the Security Gateway encrypts the HTTPS connection.
9. The Security Gateway sends the HTTPS request to the internal server.

Getting Started with HTTPS Inspection

This section gives an example of how to configure a Security Gateway to intercept outbound and inbound HTTPS traffic.

Workflow Overview

Step	Instructions
1	Enable HTTPS Inspection on the Security Gateway. See *"Enabling HTTPS Inspection on the Security Gateway" below*
2	Configure the Security Gateway to use the inbound and outbound certificates: ■ **Outbound Inspection** - Generate a new certificate for the Security Gateway and deploy it in your organization. See *"Working with Outbound CA Certificate" on the next page* ■ **Inbound Inspection** - Import the certificate for the internal server. See *"Configuring Inbound HTTPS Inspection" on page 402*
3	Configure the HTTPS Inspection Rule Base. *"HTTPS Inspection Policy" on page 403*
4	Install the Access Control Policy. See *Installing the Access Control Policy.*

Enabling HTTPS Inspection on the Security Gateway

You must configure HTTPS Inspection on each Security Gateway separately.

Important - You must enable HTTPS Inspection on the Security Gateway for the Software Blades to inspect HTTPS traffic. Without HTTPS Inspection, the Security Gateway cannot decrypt and inspect encrypted traffic, preventing any policy enforcement.

To enable HTTPS Inspection on a Security Gateway:

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

Working with Outbound CA Certificate

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 CER 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 receive TLS 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, use it in rules that intercept outbound HTTPS traffic in the HTTPS Inspection policy.

To create an outbound CA certificate

Step	Instructions
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 (see *"Exporting an Outbound Certificate from the Security Management Server" on page 399*).

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 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

Step	Instructions
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 (see *"Exporting an Outbound Certificate from the Security Management Server" on the next page*).
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 (see *"Deploying the Generated CA" on page 400*).

Exporting an Outbound 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 -help
```

```
export_https_cert {[-local] | [-s server]} [-f <certificate file name in the FWDIR/tmp/ directory>]
```

To export the CA certificate

On the Security Management Server, run this command:

```
$FWDIR/bin/export_https_cert -local -f <certificate file name in the FWDIR/tmp/ directory>
```

Example:

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

Note - On a Multi-Domain Security Management Server, you must run this command in the context of the applicable Domain Management Server (`mdsenv <IP Address of Domain Management Server>`).

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 is in the CA list and they do not receive browser certificate warnings.

To distribute a certificate with a GPO

Step	Instructions
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 to add the certificate to the Trusted Root Certification Authorities certificate store (see *"Deploying Certificates using Group Policy" on the next page*).
4	Push the Policy to the client computers in the organization. ℹ **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. Also, make sure the CA certificate shows the name you entered for the CA certificate that you created in the **Issued by** field.

Deploying Certificates 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

Step	Instructions
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

By design, the Security Gateway / Security Cluster is intentionally configured not to perform HTTPS Inspection on traffic directed towards it. To change this behavior, follow sk114574.

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 intercepts 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 TLS connections to the internal servers.

After you import a server certificate (with a CER 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

Step	Instructions
1	In SmartConsole, go to **Security Policies** > **HTTPS Inspection** > **HTTPS Tools** > **Additional Settings**.
2	Click **Open HTTPS Inspection Policy In SmartDashboard**. SmartDashboard 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 intercepts the HTTPS connections.

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.

For HTTPS Inspection to be enforced on a gateway on a specific blade, you must:

1. Enable HTTPS Inspection on the gateway.
2. Create a rule in the HTTPS Inspection policy with the required blade.
3. Enable the required blade on the gateway.

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
    - Threat Extraction
    - Zero Phishing
- Data Loss Prevention

Starting from R80.40, the HTTPS Inspection policy is in SmartConsole > the **Security Policies** view > **HTTPS Inspection**. Starting from R80.40 you can create different HTTPS Inspection layers per different policy packages. When you create a new policy package, you can use the pre-defined HTTPS Inspection layer, or customize the HTTPS Inspection layer to fit your security needs.

You can share an HTTPS Inspection layer across multiple policy packages.

Note - When you go to the **Security Policies** view > **HTTPS Inspection** > **HTTPS Tools** > **Additional Settings** > **Open HTTPS Inspection Policy In SmartDashboard**, SmartDashboard unexpectedly closes, if there are more than 100,000 network objects configured in the management database of the Management Server.

Fields

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 intercepted or bypassed. By default, the services `HTTPS` on port 443 and `HTTP_and_HTTPS proxy` on port 8080 are intercepted. You can add or delete services from the list.
Site Category	Categories for applications or web sites that are intercepted or bypassed.
Action	The action taken by the Security Gateway when it matches HTTPS traffic to a rule. ■ **Inspect** - The Security Gateway intercepts the HTTPS connection. ■ **Bypass** - The Security Gateway does not intercept the HTTPS connection. **Important** - For more information about the connection flow and this action, see: ■ *"Outbound HTTPS Connections" on page 394* ■ *"Inbound HTTPS Connections" on page 395*
Track	Tracking and logging action that is done when traffic matches the rule.
Install On	Network objects that will enforce the HTTPS Inspection Policy. You can only select Security Gateways that have HTTPS Inspection enabled (by default, the gateways which appear in the Install On column have HTTPS Inspection enabled).

Field	Description
Certificate	The certificate that is used for this rule. - Inbound HTTPS Inspection - Select the certificate that the internal server uses. You can create server certificates from the SmartDashboard > **HTTPS Inspection** > **Server Certificates** > **Add**. - 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.
Comment	An optional field to add a summary for the rule.

Configuring HTTPS Inspection Policy

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 should not be intercepted. Make sure that the bypass rules are at the top of the HTTPS Inspection Rule Base.

After you create 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.

No	Name	Source	Destination	Services	Site Category	Action	Blade	Certificate	Track	Install On
1	Financial sites	Any	Internet	HTTPS HTTP_HTTPS_proxy	Financial Services	Bypass	Any	Outbound CA	Log	HTTPS Policy Targets
2	Outbound traffic	Any	Internet	HTTPS HTTP_HTTPS_proxy	Any	Inspect	Any	Outbound CA	Log	HTTPS Policy Targets
3	Inbound traffic	Any	WebCalendarServer	HTTPS	Any	Inspect	Any	WebCalendarServer CA		

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

HTTPS Inspection Policy Enforcement

HTTPS Inspection Rule Base enforcement consists of two steps:

1. Matching the connection against the Rule Base.
2. Calculating the action to be performed.

The action is calculated according to the matched rule, the Software Blades defined on the matched rule and the rule exceptions. In certain scenarios, the action in the matched rule is Inspect, but as a result of Step 2, the action is changed to Bypass. In such case, the HTTPS Inspection log is sent with data from the matched rule, but the action in the log is Bypass.

Example 1:

The rule in the HTTPS Inspection policy defines Action: Inspect and Blade: Threat Emulation. The Threat Emulation blade is not enabled on a specific gateway. On that gateway, the traffic is not inspected by Threat Emulation, and the log indicates Action: Bypass.

Example 2:

The administrator defined one rule in the HTTPS Inspection Policy:

Source	Destination	Services	Action	Track	Blade
Any	Any	HTTPS	Inspect	Log	IPS

The administrator also added the 10.1.1.0/24 net to the Global Exceptions for the IPS blade. User with IP 10.1.1.2 surfs to some HTTPS websites.

HTTPS Inspection Rule Base execution:

The connection was matched to the rule with action Inspect.

IPS is the only active blade on the matched rule, but the connection is in exception for the IPS blade. Therefore the updated action is Bypass.

Performed action: SSL is not terminated, HTTPS Inspection log is sent with data from the matched rule, and the action sent is Bypass.

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

Step	Instructions
1	In SmartConsole, go to **Security Policies** > **HTTPS Inspection**> **HTTPS Tools** > **Additional Settings** > **Open HTTPS Inspection Policy in SmartDashboard**.
2	In SmartDashboard, click the **HTTPS Inspection** tab.
3	Click **HTTPS Validation**.
4	Go to **Whitelisting** and 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 in the HTTPS Inspection tab in SmartDashboard lists the gateways with HTTPS Inspection enabled.

In the CA Certificate section, in the lower part of the Gateways pane, 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 it from the Security Management Server on which it was created (see *"HTTPS Inspection " on page 393*).

Working with Trusted CAs for Outbound HTTPS Inspection

When a client initiates a TLS connection to a server, the Security Gateway intercepts the connection. The Security Gateway intercepts the traffic and creates a new TLS connection from the Security Gateway to the designated server.

When the Security Gateway establishes a secure TLS connection to the designated server, 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 downloaded automatically from the Check Point Download Center to the Management Server. After you get the Trusted CA update on the Security Management Server, you must install the policy on the Security Gateways. You can select to disable the automatic update option and manually update the Trusted CA list. See sk64521.

If the Security Gateway receives a non-trusted server certificate, 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 server security certificate, but lets the user continue to the server.

You can change the default setting to block untrusted server certificates. Go to **Manage & Settings** > **Blades** > **HTTPS Inspection** > **Configure in SmartDashboard** > **HTTPS Validation** > **Server Validations** > select **Untrusted server certificates**.

To manage the list of Trusted Certificates, in SmartConsole, go to **Manage & Settings** > **Blades** > **HTTPS Inspection** > **Configure in SmartDashboard** > **Trusted CAs**.

In the Trusted CAs page, you can view all the certificates included in the package and certificates that were added by the user. You can do these actions on this page:

- **Add** - Lets you add a CA certificate to the Trusted CAs list that was previously added by Check Point and removed from the list.
- **View** - Lets you see the details of a selected certificate.
- **Remove** - Lets you remove a CA certificate from the list:
  - If the certificate was added by Check Point (see '**Added By**' column), you can later add it to the list with the **Add** option.
  - If the certificate was added by the user, the certificate will be deleted.
- **Actions**:

    - **Import certificate** - Lets you add custom trusted certificates (non-trusted website's certificates) to the Trusted CAs list.
    - **Export to file** - Lets you save a selected certificate in the list to the local file system.
    - **Update certificate list** - Lets you upload a zip file that contains Check Point updates for the Trusted CAs list.
- Configure **Automatic Updates** settings:
    - **Do not download updates** - The system does not automatically check for or download updates to the Trusted CAs list. This option is useful if you prefer to manage and update the Trusted CAs list manually. It gives you full control over which CA certificates are trusted and when updates are applied.
    - **Download updates automatically and notify when an update file is available for installation** - The system automatically checks for updates to the Trusted CAs list and download them when they become available. This option is useful if you want to ensure that your Trusted CAs list is always up-to-date with the latest certificates, but you also want to have control over when the updates are actually installed. It allows you to review the updates before applying them, ensuring that you are aware of any changes made to the Trusted CAs list.
    - **Download and install updates automatically** - The system automatically checks for updates to the Trusted CAs list, downloads them, and installs them without requiring any manual intervention. This option is ideal for ensuring that your Trusted CAs list is always up-to-date with the latest certificates. It helps maintain security by automatically incorporating new trusted CAs and removing outdated or compromised ones.

Note - To apply changes in the Trusted CAs settings, install policy on the applicable Security Gateway.

HTTPS Validation

In the HTTPS Validation page of SmartDashboard you can set options for

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

To learn more about these options, see the Help. Click the **?** symbol 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

Step	Instructions
1	In the SmartConsole **Logs & Monitor** view, go to the **Logs** tab, and click **Queries**.
2	Select the **HTTPS Inspection** query.

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

SNI support for Site Categorization

Starting from R80.30, a new functionality allows the categorization of HTTPS sites before the HTTPS Inspection begins, and prevents connectivity failure if the inspection does not succeed.

SNI is an extension to the TLS protocol, which indicates the hostname at the start of the TLS handshaking process.

The categorization is performed by examining the SNI field in the client hello message at the beginning of the TLS handshaking process. To make sure that you reached the right site, the SNI is verified against the Subject Alternative Name of the host, which appears in the certificate.

After the identity of the host is known and verified, the site is categorized, and it is determined whether the connection should be intercepted or not.

SNI support is enabled by default.

HTTPS 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.

The security policies inspect 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** > **General** > **HTTPS Inspection**.

Inspection of TLS v1.3 Traffic

From R81, the Check Point Security Gateway can intercept traffic that relies on Transport Layer Security (TLS) v1.3 (see RFC 8446).

From R81.10, this feature is enabled by default for Security Gateways (and Cluster Members) that use the User-Space Firewall Mode (USFW)).

For the list of supported platforms, see sk167052.

Important - In a Cluster, you must configure all the Cluster Members in the same way.

Note - To disable the inspection of the TLS v1.3 traffic for testing purposes, set the value of the global parameter **fwtls_enable_tlsio** to **0** and reboot.

The HTTPS Inspection feature decrypts traffic for better protection against advanced threats, bots, and other malware.

Configuring Threat Indicators

Threat Indicators lets you add feeds to the Anti-Bot and Anti-Virus engines, in addition to the feeds included in the Check Point packages and ThreatCloud feeds. You can create your own threat indicator files or import them from external sources. You can upload the files both through SmartConsole and through the CLI.

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

An Observable is an event or a stateful property that can be observed in an operational cyber domain. Such as: IP address, MD5 file signature, SHA1 file signature, SHA256 file signature, URL, Mail sender address.

Threat Indicators demonstrate an attack by:

- Specific observable patterns
- Additional information intended to represent objects and behaviors of interest in a cyber-security context

Indicators are derived from intelligence, self-analysis, governments, partners, and so on.

Importing Threat Indicator Files through SmartConsole

When you manually upload threat indicator files through SmartConsole, the files must be in a CSV Check Point format or STIX XML (STIX 1.0) format. The files must contain records of equal size. If an indicator file has records which do not have the same number of fields, it does not load.

To load indicator files through SmartConsole

> **Before you start** - Go to the applicable profile > **Indicators** > **Activation** > make sure that **Enable indicator scanning** is selected.

Step	Instructions
1	In the SmartConsole main view, go to **Security Policies**>**Threat Prevention**> **Custom Policy** >**Custom Policy Tools**> **Indicators**. If you are working with Autonomous Threat Prevention, go to **Security Policies > Threat Prevention > Autonomous Policy > Autonomous Policy Tools > Indicators**.
2	Click **New**, and select **New IoC file**. The **Indicator** 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: ▪ **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 are used in the empty fields. Click **OK**. The Indicator file loads.
9	Install the Threat Prevention Policy.

To delete Indicators

Step	Instructions
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.

Importing External Custom Intelligence Feeds

Custom Intelligence Feeds lets you fetch feeds from a third-party server directly to the Security Gateway to be enforced by the Anti-Virus and Anti-Bot blades. The Custom Intelligence Feeds feature helps you manage and monitor indicators with minimal operational overhead.

Note - Starting from R81.20, the Check Point Security Gateway can support at least 2 million patterns/observables for these observable types: URL, Domain, IP addresses, and Hashes. The maximum number of supported patterns/observables is limited by the available memory on the Security Gateway. Before the Security Gateway loads more than 2 million patterns/observables, it checks if 50% of the total memory is free.

Importing External Custom Intelligence Feeds in CLI

You can import threat indicator feeds from external sources directly on the Security Gateway.

After you import the feeds for the first time and install policy, the Security Gateway automatically pulls and enforces the indicator file each time the feed file is updated.

The Security Gateway imports the file over HTTP or HTTPS, or by reading from a local file or local directory.

Important - You must import the feed files on each Security Gateway and each Cluster Member separately.

You can import indicator feeds in the CLI in these formats:

- CSV in the Check Point format
- Custom CSV in other formats
- STIX XML (STIX 1.0)

The Feed's Resource

The Feed's resource for all formats can be one of these:

Resource	Description	Syntax Example
URL	HTTP or HTTPS. **Note** - HTTPS resource with a self-signed certificate prompts for a user agreement to update the Trusted CA bundle. You can skip the certificate verification by running this command in the Expert mode on the Security Gateway before you run the "`ioc_feeds`" command: `export EXT_IOC_NO_SSL_VALIDATION=1`	`ioc_feeds add --feed_name remote_feed --transport http --resource "http://10.0.0.1/my_feeds/stix_feed.xml"`
Local File	Local File on the Security Gateway.	`ioc_feeds add --feed_name local_feed --transport local_file --resource "/home/admin/my_feed.csv"`

Resource	Description	Syntax Example
Local Directory	Local Directory on the Security Gateway that contains the applicable files in the correct feed format.	`ioc_feeds add --feed_name local_feed --transport local_directory --resource "/home/admin/my_feed_folder"`

'ioc_feeds' CLI Commands for Managing External Custom Intelligence Feeds

Use these "`ioc_feeds`" commands in the Expert mode on the Security Gateway to import and manage threat indicator files.

Commands

Command	Description	Syntax Example
`ioc_feeds -h`	Shows the built-in help.	
`ioc_feeds push`	Pushes feeds now.	`ioc_feeds push`
`ioc_feeds show`	Shows all existing feeds.	`ioc_feeds show`
`ioc_feeds show --feed_name <Feed>`	Shows details for the specified feed.	`ioc_feeds show --feed_name local_feed`
`ioc_feeds show_interval`	Shows the fetching interval.	`ioc_feeds show_interval`
`ioc_feeds set_interval <sec>`	Configures the interval (in seconds) for fetching all feeds.	`ioc_feeds set_interval 1000`
`ioc_feeds show_scanning_mode`	Shows the statue of the scanning mode.	`ioc_feeds show_scanning_mode`

Command	Description	Syntax Example
`ioc_feeds set_scanning_mode {on|off}`	Enables (`on`) or disables (`off`) the scanning mode.	`ioc_feeds set_scanning_mode off`

Command	Description	Syntax Example

`ioc_feeds add`	Adds a new feed.
	Mandatory parameters:
	- `--feed_name <Feed>` Configures the feed name.
	- `--transport {http | https} --resource <URL>` Specifies a remote feed URL.
	- `--transport local_file --resource <Absolute Path to Local File>` Specifies a local feed file.
	- `--transport local_directory --resource <Absolute Path to Local Directory>` Specifies a local feed directory. Must be inside the `/home/` directory.
	Optional parameters:
	- `--state {true | false}`
		Example 1 - local file feed:
		`ioc_feeds add --feed_name local_feed --transport local_file --resource /home/admin/my_feed.csv`
		Example 2 - remote feed through a proxy:
		`ioc_feeds add --feed_name remote_feed --transport http --resource "http://10.0.0.1/my_feeds/stix_feed.xml" --proxy 192.168.22.33:8080 --state false -feed_action Detect --user_name admin@example.com`
		Example 3 - dry run for a remote feed:
		`ioc_feeds add --feed_name remote_stix_file --transport http --resource "http://www.public_indicators.com/ioc_stix_file.xml" --test true`

Command	Description	Syntax Example
	Configures the feed state - active (`true`, this is the default) or inactive (`false`). ■ `--feed_action {Prevent | Detect | Ask}` Configures the feed action (default - `Prevent`) ■ `--user_name <user>` Specifies the username for the feed source - a prompt for a password appears. ■ `--proxy none` Specifies not to use any proxy when connecting to the feed source. If you do not specify the "`--no_proxy`" or the "`--proxy`" parameter, the tool uses the Security Gateway proxy. ■ `--proxy <proxy server>:<proxy port>`	

Command	Description	Syntax Example
	Overrides the Security Gateway proxy when connecting to the feed source. If you do not specify the "`--no_proxy`" or the "`--proxy`" parameter, the tool uses the Security Gateway proxy. ■ `--proxy_user_name <user>` Specifies the username for the proxy server - a prompt for a password appears. ■ `--test true` Performs a dry run - fetches and parses the specified feed but does not save its configuration.	
`ioc_feeds modify`	Modifies an existing feed. Values of the feed parameters that are not specified, stay as they were before.	`ioc_feeds modify --feed_name local_feed --state true`

Command	Description	Syntax Example
`ioc_feeds delete`	Deletes existing specified feed. Mandatory parameter: - `--feed_name <feed>` Specifies the feed name.	`ioc_feeds delete --feed_name local_feed`

CSV Check Point and STIX Formats

Each record in CSV Check Point format and the STIX format must have these fields (files in other CSV formats do not have to include all these fields (see

Fields

Field	Description	Valid Values	Value Criteria	Optional
UNIQ-NAME	Name of the observable	Free text	Must be unique	No
VALUE	A valid value for the type of the observable	As provided in this table	Value of parameter	No

Field	Description	Valid Values	Value Criteria	Optional
TYPE	Type of the observable	`URL`	Any valid URL Not case sensitive	No
		`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	
		`SHA1`	Any valid SHA1	
		`SHA256`	Any valid SHA256	
		`Mail-subject`	Any non-empty text string	
		`Mail-from`	Can be one of these: ■ A single email address (Example: `abc@domain.com`) ■ An email domain (Examples: `@domain.com`, or `domain.com`)	
		`Mail-to`	Can be one of these: ■ A single email address (Example: `abc@domain.com`) ■ An email domain (Examples: `@domain.com`, or `domain.com`)	

Field	Description	Valid Values	Value Criteria	Optional
		`Mail-cc`	Can be one of these: - A single email address (Example: `abc@domain.com`) - An email domain (Examples: `@domain.com`, or `domain.com`)	
		`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`)	
CONFIDENCE	Degree of confidence the observable presents	- `low` - `medium` - `high` - `critical`	Default - high	Yes
SEVERITY	Degree of threat the observable presents	- `low` - `medium` - `high` - `critical`	Default - high	Yes

Field	Description	Valid Values	Value Criteria	Optional
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, SHA1 and SHA256 observables.	Yes
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 does not load.
- As of this release, STIX 2.0 (JSON file) is not supported.
- Custom Indicators CLI (load_indicators) are not supported.
- The supported STIX elements are:

```
stix:STIX_Package
stix:STIX_Header
stix:Title
stix:Description
stix:Indicators
stix:Indicator
indicator:Title
indicator:Type
indicator:Description
indicator:Observable
cybox:Object
cybox:Properties
FileObj:Hashes
cyboxCommon:Hash
cyboxCommon:Type
cyboxCommon:Simple_Hash_Value
stix:Observables
cybox:Observable
URIObj:Value
URIObject:Value
AddressObject:Address_Value
AddressObj:Address_Value
AddressObj:AddressObjectType
AddressObjet:AddressObjectType
cybox:Title
```

Condition Type Enum and **Condition Application Enum** support **Equals** and **Any**.

<cyboxCommon:Simple_Hash_Value condition="Equals" apply_condition="ANY">

Syntax rules of CSV Indicator files in Check Point format

- 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 in Check Point format

```
#! DESCRIPTION = indi file,,,,,,
"#! REFERENCE = Indicator Bulletin; Feb 20, 2014",,,,,,
# FILE FORMAT:,,,,,,
"# All lines beginning ""#"" are comments",,,,,,
"# All lines beginning ""#!"" are metadata read by the SW",,,,,,
"# UNIQ-NAME,VALUE,TYPE,CONFIDENCE,SEVERITY,PRODUCT,COMMENT",,,,,,
observ1,8d9b6b8912a2ed175b77acd40cbe9a73,MD5,medium,medium,AV,FILENAME:WUC
 Invitation Letter Guests.doc
observ2,76700f862a0c241b8f4b754f76957bda,MD5,high,high,AV,FILENAME:essais~.swf|
NOTE:FWS type Flash file
observ4,5dda6d1446b3cdb0bd4a3f0adb85d030ff59e975,SHA1,low,high,AV,file_name.pdf
observ5,db435a875be456f088f11c579aa52f30bc83cfff272cfad5a3f6f4de74de0654,SHA256,high,high,AV,file_name.doc
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,Dpmain,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,
```

Example of a STIX 1.0 XML Indicator File

```
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:indicator="http://stix.mitre.org/Indicator-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:FileObj="http://cybox.mitre.org/objects#FileObject-2"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:cyboxCommon="http://cybox.mitre.org/common-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
    http://stix.mitre.org/stix-1 ../stix_core.xsd
    http://stix.mitre.org/Indicator-2 ../indicator.xsd
    http://stix.mitre.org/default_vocabularies-1 ../stix_default_vocabularies.xsd
    http://cybox.mitre.org/objects#FileObject-2 ../cybox/objects/File_Object.xsd
    http://cybox.mitre.org/default_vocabularies-2 ../cybox/cybox_default_vocabularies.xsd"
    id="example:STIXPackage-ac823873-4c51-4dd1-936e-a39d40151cc3"
    version="1.0.1">
    <stix:STIX_Header>
        <stix:Title>Example file watchlist</stix:Title>
        <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators -
Watchlist</stix:Package_Intent>
    </stix:STIX_Header>
    <stix:Indicators>
        <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-611935aa-
4db5-4b63-88ac-ac651634f09b">
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">File Hash
Watchlist</indicator:Type>
            <indicator:Description>Indicator that contains malicious file
hashes.</indicator:Description>
            <indicator:Observable id="example:Observable-c9ca84dc-4542-4292-af54-
3c5c914ccbbc">
                <cybox:Object id="example:Object-c670b175-bfa3-48e9-a218-aa7c55f1f884">
                    <cybox:Properties xsi:type="FileObj:FileObjectType">
                        <FileObj:Hashes>
                            <cyboxCommon:Hash>
                                <cyboxCommon:Type xsi:type="cyboxVocabs:HashNameVocab-1.0"
condition="Equals">MD5</cyboxCommon:Type>
                                <cyboxCommon:Simple_Hash_Value condition="Equals" apply_
condition="ANY">0522e955aaee70b102e843f14c13a92c##comma##0522e955aaee70b102e843f14c13a92d##co
mma##0522e955aaee70b102e843f14c13a92e</cyboxCommon:Simple_Hash_Value>
                            </cyboxCommon:Hash>
                        </FileObj:Hashes>
                    </cybox:Properties>
                </cybox:Object>
            </indicator:Observable>
        </stix:Indicator>
    </stix:Indicators>
</stix:STIX_Package>
```

Custom CSV Format

Custom Intelligence Feeds feature supports different kinds of CSV structure files.

Syntax Rules of Custom CSV files

- The supported observables are:

  `Name`, `Value`, `Type`, `Confidence`, `Severity`, `Product`, `Comment`.

- Define the file's format, delimiter, and the comment lines to skip:

Use "`--format`" and specify your observables inside square brackets.

Use "`--comment`" for content to ignore in the original file.

Notes:

- Content specified within the square brackets of "`--format`" is fetched from the original file.
- Content inside the square brackets of "`--comment`" is ignored.

- The `Value` and `Type` observables are mandatory.
- The `Value` observable is specified based on its location in the original file: `#<location_of_item>`.

  For example:

  If the `Value` observable is in the 3rd place in your CSV row, enter:

  ```
  --format [value:#3]
  ```

- For all other observables, you can enter their location in the original file, or specify their value.

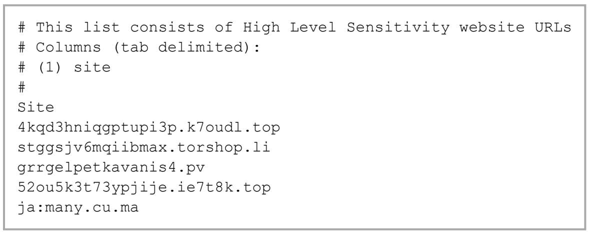
  For example, if you want the value of the `Type` observable to be the domain specified in every CSV row, enter:

  ```
  --format [type:domain]
  ```

- When the feed's resource is a remote source (transport equals HTTP or HTTPS), every time the feed is fetched, it parses based on the format that was specified for this feed.

Examples

Original CSV file is a list of domains



```
# This list consists of High Level Sensitivity website URLs
# Columns (tab delimited):
# (1) site
#
Site
4kqd3hniqgptupi3p.k7oudl.top
stggsjv6mqiibmax.torshop.li
grrgelpetkavanis4.pv
52ou5k3t73ypjije.ie7t8k.top
ja:many.cu.ma
```

If you enter this command, the Security Gateway takes the domain specified in the first place of every row, and ignores anything that starts with *#* and the word *Site*.

```
ioc_feeds add --feed_name domain_list --transport https --
resource "https://isc.sans.edu/feeds/suspiciousdomains_High.txt"
--format [type:domain,value:1] --comment "#, Site"
```

This is the original CSV file

```
# category Descriptive tag name for this entry. For this report,
# the text sshpwauth will appear.
#
# A commented footer section shows an aggregate account of ASNs and
# addresses seen in the current report
#
3 | organization A | 18.30.10.26 | 2018-12-15 08:16:39 | sshpwauth
3 | organization B | 18.30.21.197 | 2018-12-28 17:43:41 | sshpwauth
17 | organization C | 128.46.80.71 | 2019-01-04 17:56:00 | sshpwauth
111| organization D | 128.197.31.119 | 2019-01-10 03:12: 18| sshpwauth
```

If you enter this command, the Security Gateway takes the IP address from the 3rd place in the row, takes the comment from the second place in the row, and ignores all content preceded by #:

```
ioc_feeds add --feed_name ip_list_with_spaces --transport local_
file --resource "/home/admin/ioc/ip_list_with_spaces.txt" --
format [value:#3,comment:#2,type:ip] --comment [#] --delimiter
"|"
```

To learn more about Custom Intelligence Feeds, see sk132193.

Importing External Custom Intelligence Feeds in SmartConsole

Custom Intelligence Feeds lets you fetch feeds from a third-party server directly to the Security Gateway to be enforced by the Anti-Virus and Anti-Bot blades. The Custom Intelligence Feeds feature helps you manage and monitor indicators with minimal operational overhead.

Note - Starting from R81.20, the Check Point Security Gateway can support at least 2 million patterns/observables for these observable types: URL, Domain, IP addresses, and Hashes. The maximum number of supported patterns/observables is limited by the available memory on the Security Gateway. Before the Security Gateway loads more than 2 million patterns/observables, it checks if 50% of the total memory is free.

To import an external IoC feed

Before you start - In SmartConsole, go to the applicable profile > **Indicators** > **Activation** > make sure that **Enable indicator scanning** is selected.

Step	Instructions
1	In the SmartConsole main view, go to **Security Policies** > **Threat Prevention** > **Custom Policy** > **Custom Policy Tools** > **Indicators**. If you are working with Autonomous Threat Prevention, go to **Security Policies** > **Threat Prevention** > **Autonomous Policy** > **Autonomous Policy Tools** > **Indicators**.
2	Click **New** and select **New IoC Feed**. The **New IoC Feed** configuration window opens.
3	In the top field, enter a unique object name.
4	In the **Action** field, select the applicable action: ■ **Prevent** - Threat Prevention Software Blades block the detected observable. ■ **Detect** - Threat Prevention Software Blades create a log, and lets the detected observable go through. ■ **Inactive** - Disables this feed (Security Gateways ignore it).
5	In the **Feed URL** field, enter the full URL that starts with `http://` or `https://`.
6	In the Feed Parsing section, from the **Format** drop-down menu, select the applicable format (see sk132193): ■ **Check Point format/STIX** - Configure the applicable feed parsing setting. ■ **Custom CSV** - Configure the applicable feed parsing settings.
7	Expand the **Advanced** section (click the **^** icon on the right side).

Step	Instructions
8	In the **Authentication** section, enter the applicable username and password, if the external feed requires authentication.
9	In the **Network** section, select **Use gateway proxy for connection**, if the Security Gateway must connect to the external feed through a proxy server.
11	Make sure the Security Gateways can get this feed: 1. Click **Test Feed**. 2. From the **Select gateway** drop-down menu, select the applicable Security Gateway. 3. Click **Test Feed**. 4. Click **Close**. **Note** - The **Select gateway** menu does not show Virtual Switches.
12	Click **OK**. The new indicator appears on the **Indicators** page.
13	Install the Threat Prevention Policy.

Note - The Security Gateways fetch the configured feeds every 30 minutes and enforce them immediately without the need to install a Threat Prevention Policy.
To change the fetching interval:

1. From the left navigation panel, click **Manage & Settings**.
2. In the top middle pane, click **Blades**.
3. In the **Threat Prevention** section, click **Advanced Settings**.
4. From the left tree, click **External Feed**.
5. Configure the applicable interval.
6. Click **OK**.
7. Install the Threat Prevention Policy.

Limitations

- External Indicators of Compromise (IoC) added in SmartConsole are supported only on Security GatewaysR81 and higher.
- IoC feeds are fetched on all connections and are not affected by Threat Prevention Policy.
- Policy installation does not fail if a Security Gateway cannot get a feed.

  In this case, the Security Gateway generates a control log.

Cyber Attack View - Gateway

The **Cyber Attack View - Gateway** view shows cyber-attacks against your network based on attack vectors.

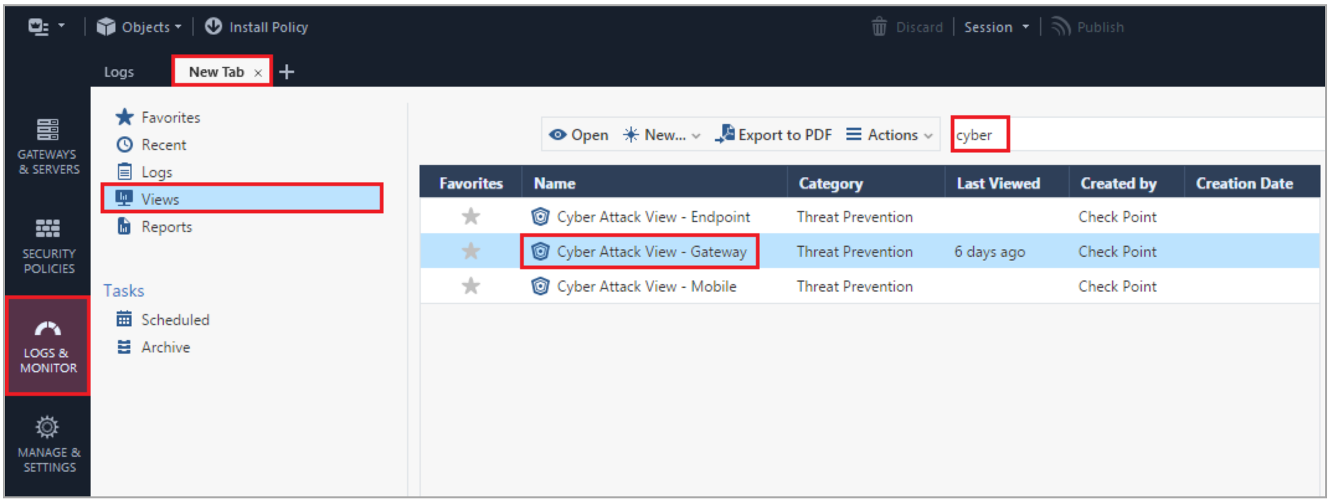
This view lets you pinpoint events that require attention.

Main Screen - SmartConsole

To open this view:

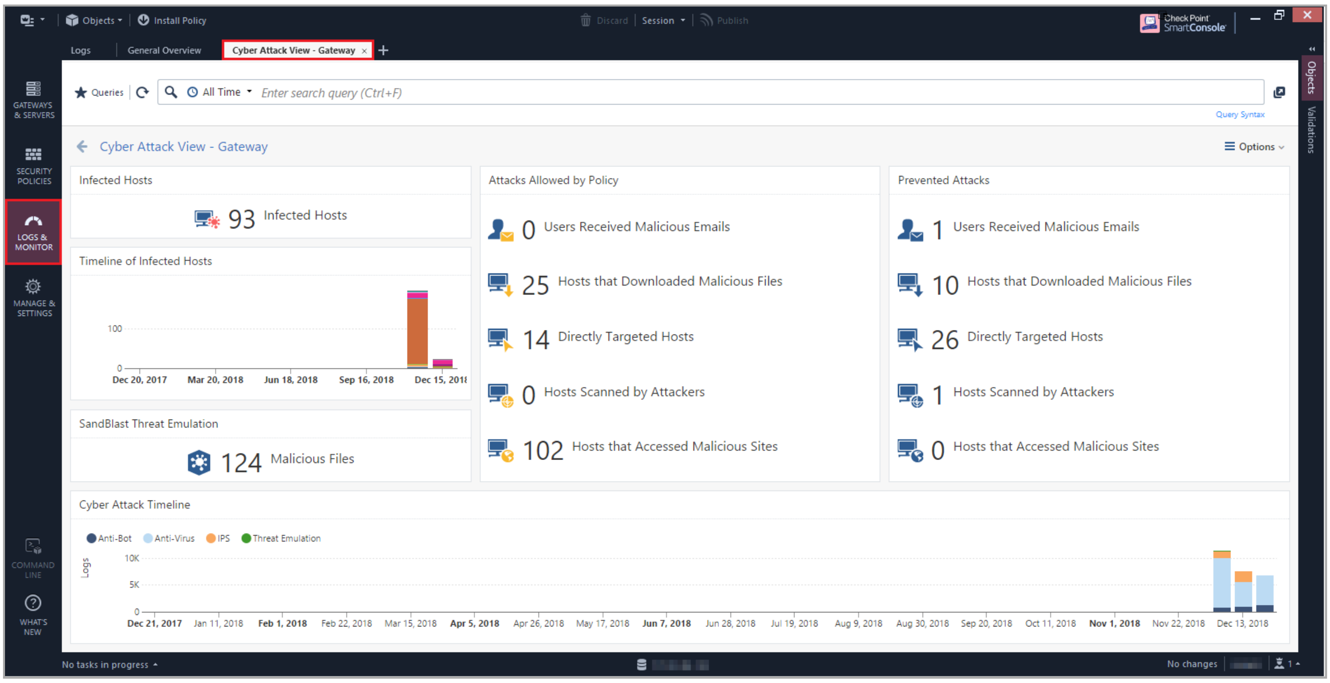
Step	Instructions
1	Connect with SmartConsole to your Security Management Serveror Domain Management Server.
2	From the left navigation panel, click Logs & Monitor.
3	At the top, click the **+** tab. The **New Tab** tab opens.
4	In the left tree, click **Views**.
5	In the top search field, enter the word **cyber**.
6	The list of the views shows the available **Cyber Attack View** views.
7	Double-click the **Cyber Attack View - Gateway** (or select it and click **Open**).

Example: SmartConsole > New Tab > Logs & Monitor:



Favorites	Name	Category	Last Viewed	Created by	Creation Date
★	Cyber Attack View - Endpoint	Threat Prevention		Check Point	
★	Cyber Attack View - Gateway	Threat Prevention	6 days ago	Check Point	
★	Cyber Attack View - Mobile	Threat Prevention		Check Point	

Example: Cyber Attack View - Gateway



Cyber Attack View - Gateway

Infected Hosts

93 Infected Hosts

SandBlast Threat Emulation

124 Malicious Files

Attacks Allowed by Policy

- 0 Users Received Malicious Emails
- 25 Hosts that Downloaded Malicious Files
- 14 Directly Targeted Hosts
- 0 Hosts Scanned by Attackers
- 102 Hosts that Accessed Malicious Sites

Prevented Attacks

- 1 Users Received Malicious Emails
- 10 Hosts that Downloaded Malicious Files
- 26 Directly Targeted Hosts
- 1 Hosts Scanned by Attackers
- 0 Hosts that Accessed Malicious Sites

All the correlated events are tagged with a **Severity** and **Confidence Level** of **Medium** and above (Check Point assigns these tags, and users cannot change them). The queries that run in the background show events with these tags.

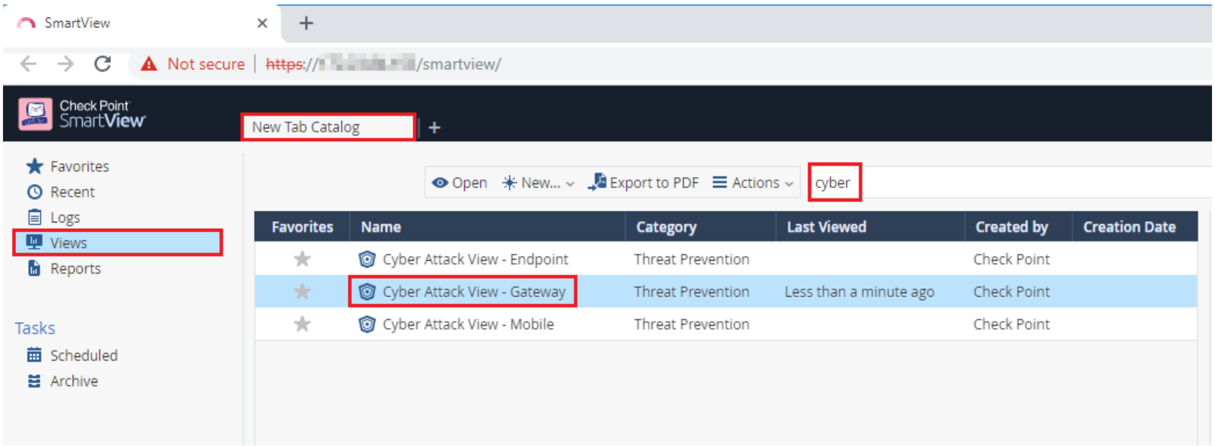
All the other events show in the **Additional Events** section.

Main Screen - SmartView

To open this view:

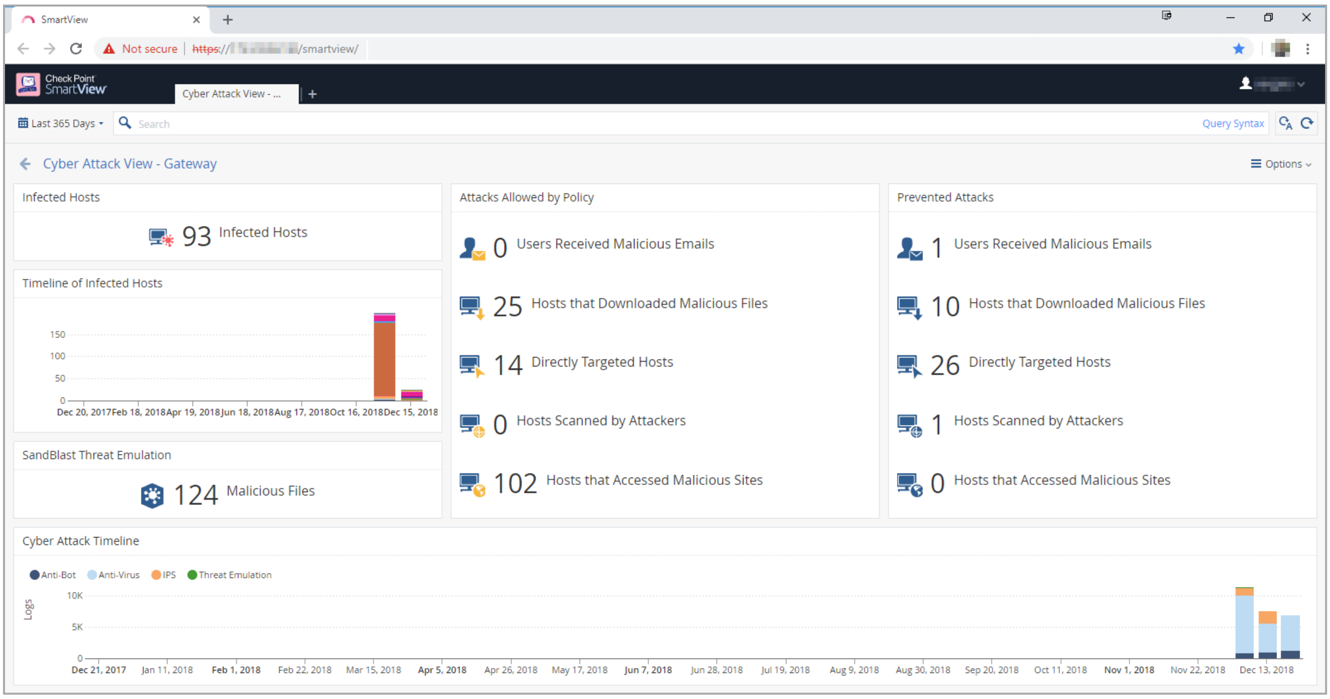
Step	Instructions
1	In your web browser, connect to the SmartView on your Security Management Server or Domain Management Server: `https://<IP Address of Management Server>/smartview`
2	At the top, click the **+** tab. The **New Tab Catalog** tab opens.
3	In the left tree, click **Views**.
4	In the top search field, enter the word **cyber**.
5	A list shows the available **Cyber Attack View** views.
6	Double-click the **Cyber Attack View - Gateway** (or select it and click **Open**).

Example: SmartView > New Tab Catalog > Views



Favorites	Name	Category	Last Viewed	Created by	Creation Date
★	Cyber Attack View - Endpoint	Threat Prevention		Check Point	
★	Cyber Attack View - Gateway	Threat Prevention	Less than a minute ago	Check Point	
★	Cyber Attack View - Mobile	Threat Prevention		Check Point	

Example: Cyber Attack View - Gateway



SmartView

Not secure | https://[redacted]/smartview/

Check Point SmartView | Cyber Attack View - ... | [redacted]

Last 365 Days | Search | Query Syntax

Cyber Attack View - Gateway | Options

Infected Hosts

93 Infected Hosts

Timeline of Infected Hosts

SandBlast Threat Emulation

124 Malicious Files

Attacks Allowed by Policy

0 Users Received Malicious Emails

25 Hosts that Downloaded Malicious Files

14 Directly Targeted Hosts

0 Hosts Scanned by Attackers

102 Hosts that Accessed Malicious Sites

Prevented Attacks

1 Users Received Malicious Emails

10 Hosts that Downloaded Malicious Files

26 Directly Targeted Hosts

1 Hosts Scanned by Attackers

0 Hosts that Accessed Malicious Sites

Cyber Attack Timeline

All the correlated events are tagged with a **Severity** and **Confidence Level** of **Medium** and above (Check Point assigns these tags, and users cannot change them). The queries that run in the background show events with these tags.

All the other events show in the **Additional Events** section.

Default Query

The view runs this query and presents the data in different widgets:

```
Pre-defined Filter > Log Type Filter
Product Family > Equals > Threat
Severity > Equals > Medium, High, Critical
Confidence Level > Equals > Medium, Medium-High, High
```

Some widgets add their own filters to the default query.

Default widgets

These are the default widgets in this view:

Widget	Type	Description
Infected Hosts	Infographic	Shows the number of hosts in the network infected with malware over the selected report period.
Timeline of Infected Hosts	Timeline	Shows the dates and the number of logs for hosts in the network infected with malware over the selected report period.
Attacks Allowed by Policy	Infographic	Shows the number of attacks in different attack vectors that the current Security Policy allowed over the selected report period.
Prevented Attacks	Infographic	Shows the number of attacks in different attack vectors that the current Security Policy prevented over the selected report period.
SandBlast Threat Emulation	Infographic	Shows the number of blocked malicious files over the selected report period.
Cyber Attack Timeline	Timeline	Shows the number of logs from different Software Blade (Anti-Bot, Anti-Virus, IPS, and Threat Emulation) over the selected report period.

Editing the View and Widgets

To edit the view and its widgets, click **Options > Edit** in the top right corner.

On the top toolbar, these buttons become available:

Icon	Button	Description
+ Add Widget	**Add Widget**	Add a new widget to this view. Available widget types are: ▪ **Table** ▪ **Chart** ▪ **Timeline** ▪ **Map** ▪ **Infographic** ▪ **Container** ▪ **Rich Text**
↶ Undo	**Undo**	Undo the last action.
↷ Redo	**Redo**	Repeat the last action.
⊗ Discard	**Discard**	Discard all changes and exit the edit mode.
✓ Done	**Done**	Save all changes and exit the edit mode.

In the top right corner of every widget, these buttons show according to the widget type:

Icon	Button	Description
✕ Remove	**Remove**	Deletes an element (that you added with the **Add Widget** button) from this widget.
+ Add	**Add**	Adds more elements to this widget: ▪ **Chart** ▪ **Timeline** ▪ **Map** ▪ **Infographic** ▪ **Rich Text**

Icon	Button	Description
📊	**Chart Type**	Selects the chart type: ▪ **Columns** ▪ **Bars** ▪ **Pie** ▪ **Area** ▪ **Line**
▼	**Edit Filter**	Edits the query filter.
⚙	**Settings**	Configures the settings for this widget (**Container**) and for the elements of this widget.
		For the widget's **Container**, you can configure: ▪ Title ▪ Description ▪ Layout (Horizontal, Vertical, Grid, Tabs)
		For widget of type **Infographic**, you can configure: ▪ Title ▪ Field Name ▪ Filter ▪ Icon (search or hover the mouse cursor to see the tooltip with an icon's name) ▪ Primary Text (appears on the right of the icon) ▪ Secondary Text (appears in smaller font under the Primary Text) ▪ Icon template (controls the shape and size of the icon and whether to show the counter) ▪ Horizontal Alignment (Left, Center, Right) ▪ Vertical Alignment (Top, Middle, Bottom) ▪ Style (Normal, Small)
		For widget of type **Table**, you can configure: ▪ Title ▪ Description ▪ Table Type (Statistical Table, Logs Table) ▪ Columns (which log fields to analyze and how to present their data)

Icon	Button	Description
		For widget of type **Chart**, you can configure: ■ Title ■ Description ■ Chart Type ■ Values for Y-axis ■ Values for X-axis ■ Sort order ■ Number of values to show ■ Number of samples to show ■ Axis titles ■ Legend
✕	**Remove Widget**	Deletes the widget from the view.

To change the size of a widget:

1. Left-click and hold in the bottom right corner of the widget.
2. Drag the corner to the desired position.
3. Release the mouse button.

To restore the default settings:

In the top right corner, click **Options > Restore Defaults**.

Working with Widgets

Working with widgets of type Infographic

- Double-click anywhere on the headline or the icon.
- Right-click anywhere on the headline or the matching icon and click **Drill Down**.

Working with widgets of type Table:

- Click once on the column header to sort in ascending or descending order.
- Hover the mouse cursor over a value to see a full-text tooltip.
- To open the next drill-down level, you can:
  - Double-click on a row inside the table.
  - Right-click on a row inside the table and click **Drill Down**.
- To filter the applicable logs only for a specific value, right-click on the value inside the table and click **Filter: "<*VALUE*>"**.
- To filter a specific value out of the applicable logs, right-click on the value inside the table and click **Filter Out: "<*VALUE*>"**.

Working with widgets of type Chart:

- Hover the mouse cursor over the chart area to see a full-text tooltip.
- To open the next drill-down level, you can:
  - Double-click on a chart bar inside the graph.
  - Right-click on a chart bar inside the graph and click **Drill Down**.
- To filter the applicable logs only for a specific value, right-click on the value inside the table and click **Filter: "<*VALUE*>"**.
- To filter a specific value out of the applicable logs, right-click on the value inside the table and click **Filter Out: "<*VALUE*>"**.

Working with widgets of type Timeline:

- Hover the mouse cursor over the chart area to see a full-text tooltip.
- To open the next drill-down level, you can:
  - Double-click on a chart bar inside the graph.
  - Right-click on a chart bar inside the graph and click **Drill Down**.

- In the legend, you can:
  - Double-click on a specific category to show only its data on the graph
  - Single-click on a specific category to remove its data from the graph
  - Single-click on the same specific category to show its data again on the graph

  If you disabled two or more specific categories in the legend, then to enable all categories again:
  - Single-click on each disabled category until the legend shows all categories as enabled
  - Double-click a specific category to show only its data on the graph and then single-click on the same specific category

Working with widgets of type Map:

- Hover the mouse cursor over the circled country to see a full-text tooltip.
- To open the next drill-down level, you can:
  - Double-click on a circled country inside the map.
  - Right-click on a circled country inside the map and click **Drill Down**.
- To filter the applicable logs only for a specific value, right-click on the circled country and click **Filter: "<*VALUE*>"**.
- To filter a specific value out of the applicable logs, right-click on the circled country and click **Filter Out: "<*VALUE*>"**.

Infected Hosts

Description

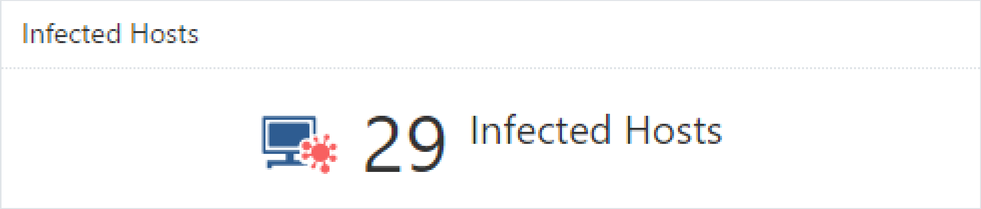
This widget shows the number of hosts in the network infected with malware over the selected report period.

Note - Select the report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

The Security Gateway treats a host as infected when it detects an outbound malicious communication or propagation event (lateral movement) from that host.

Anti-Bot and **IPS** events show this malware communication. The events shown have a **Severity** and **Confidence Level** of **Medium** and above.

Example:



Infected Hosts

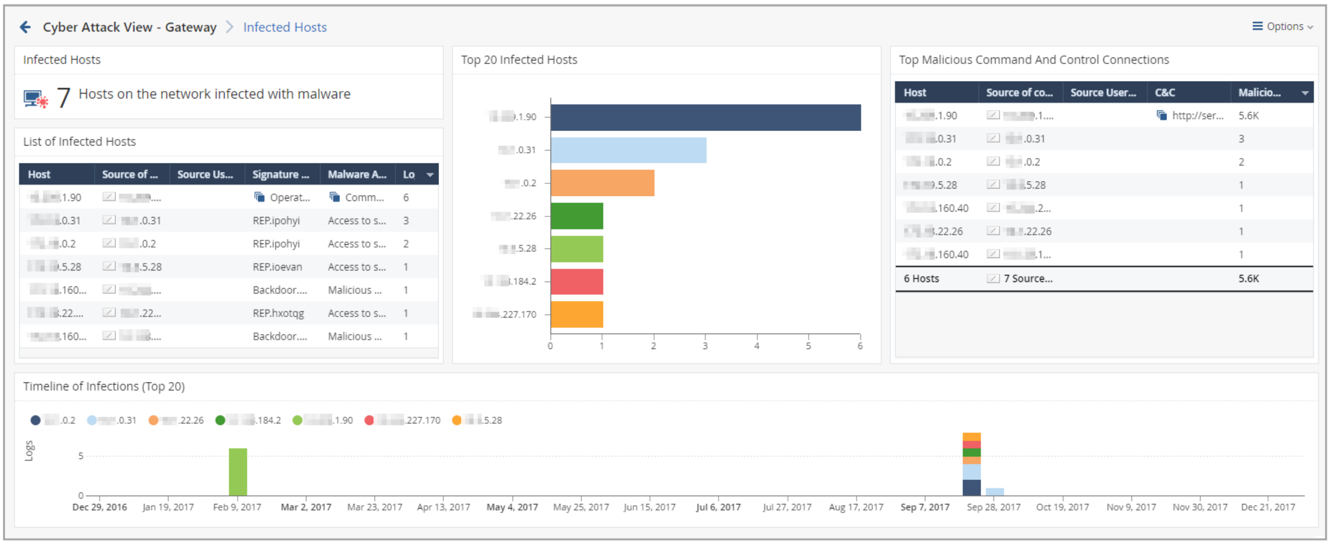
29 Infected Hosts

To open the next drill-down level, double-click a headline or matching icon.

The drill-down view shows summarized data about infected hosts on your internal network.

Drill-Down View

This is an obfuscated example of the drill-down view:



Infected Hosts

7 Hosts on the network infected with malware

List of Infected Hosts

Host	Source of ...	Source Us...	Signature ...	Malware A...	Lo
[redacted].1.90	[redacted]....		Operat...	Comm...	6
[redacted].0.31	[redacted].0.31		REP.ipohyi	Access to s...	3
[redacted].0.2	[redacted].0.2		REP.ipohyi	Access to s...	2
[redacted].5.28	[redacted].5.28		REP.ioevan	Access to s...	1
[redacted].160...	[redacted]....		Backdoor....	Malicious ...	1
[redacted].22....	[redacted].22...		REP.hxotqg	Access to s...	1
[redacted].160...	[redacted]....		Backdoor....	Malicious ...	1

Top Malicious Command And Control Connections

Host	Source of co...	Source User...	C&C	Malicio...
[redacted].1.90	[redacted].1....		http://ser...	5.6K
[redacted].0.31	[redacted].0.31			3
[redacted].0.2	[redacted].0.2			2
[redacted].5.28	[redacted].5.28			1
[redacted].160.40	[redacted].2...			1
[redacted].22.26	[redacted].22.26			1
[redacted].160.40	[redacted].1...			1
6 Hosts	7 Source...			5.6K

To see the applicable logs (the next drill-down level), double-click on a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Infected Hosts	Infographic	Shows the number of hosts on the network infected with malware.
Top 20 Infected Hosts	Chart	Shows top hosts (based on the logs count) that connected to Command and Control (C&C) servers. Shows: - The source IP addresses of the top 20 infected hosts - The number of detected malicious connections Different colors show different infected hosts.
Top Malicious Command And Control Connections	Table	Shows top hosts (based on the connection rates) that connected to Command and Control (C&C) servers. Shows: - Hostnames of the infected hosts - Source IP addresses of the infected hosts - Source usernames - C&C server IP addresses - Number of malicious C&C connections
List of Infected Hosts	Table	Shows the list of infected hosts. Shows: - Hostnames of the infected hosts - Source IP addresses of the infected hosts - Source usernames - Signature names of the detected malware (based on *Check Point ThreatWiki* and *Check Point Research*) - Malware action - Number of logs

Widget	Type	Description
Timeline of Infections (Top 20)	Timeline	Shows the timeline of malicious connections to Command and Control (C&C) servers across all infected hosts. Shows: ■ Source IP addresses of the top 20 infected hosts ■ Number of logs for the top 20 infected hosts ■ Dates and times Different colors show different infected hosts.

Widget Query

In addition to the *"Default Query" on page 438*, the widget runs this query:

```
(blade:Anti-Bot AND severity:(Medium OR High OR Critical) AND
confidence_level:(Medium OR Medium-High OR High) NOT "Mail
analysis") OR (blade:IPS AND "Malware Traffic")
```

Best Practices

1. To see which internal hosts initiate the most malicious connections with Command and Control (C&C) servers:

   - Examine the **Top Malicious Command And Control Connections**.

   - Examine the Threat Prevention logs from the Security Gateway about the internal hosts that initiate the most malicious connections with C&C servers. To do so, double-click the host entry. In the Threat Prevention logs, examine the **Suppressed Logs** column (see *"Log Fields" on page 496*).

2. For every infected host, query for its IP address to see all threat events related to that host.

   This lets you better understand the malicious behavior of the infected host.

   To query an IP address for all related threat events:

   a. Right-click an IP address.

   b. In the context menu, click **Filter: "<*IP Address*>"**

   c. At the top, click **Cyber Attack View - Gateway**.

3. If you configured the Anti-Bot Software Blade based on Check Point recommendations, the Security Gateway generates both **Detect** and **Prevent** logs.

   The Anti-Bot **Detect** logs do not mean that the Security Gateway allowed malicious connections.

   The Anti-Bot can generate the **Detect** logs, if you enabled the DNS trap feature.

   For more information, see:

   - sk74060: Anti-Virus Malware DNS Trap feature
   - sk74120: Why Anti-Bot and Anti-Virus connections may be allowed even in Prevent mode

Timeline of Infected Hosts

Description

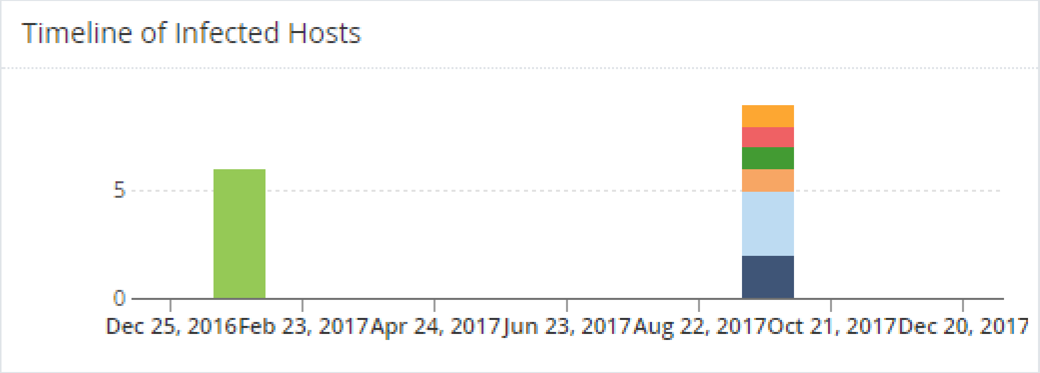
This widget shows the dates and the number of logs for hosts in the network infected with malware over the selected report period.

Note - Select the report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

This information helps you understand the infections trend in your network.

Different colors show different infected hosts.

Example:



To see the applicable logs (the next drill-down level), double-click on a chart bar inside the graph.

Widget Query

In addition to the *"Default Query" on page 438* ,the widget runs this query:

`Customer Filter = NOT "Mail analysis"`
`Blade > Equals > Anti-Bot`

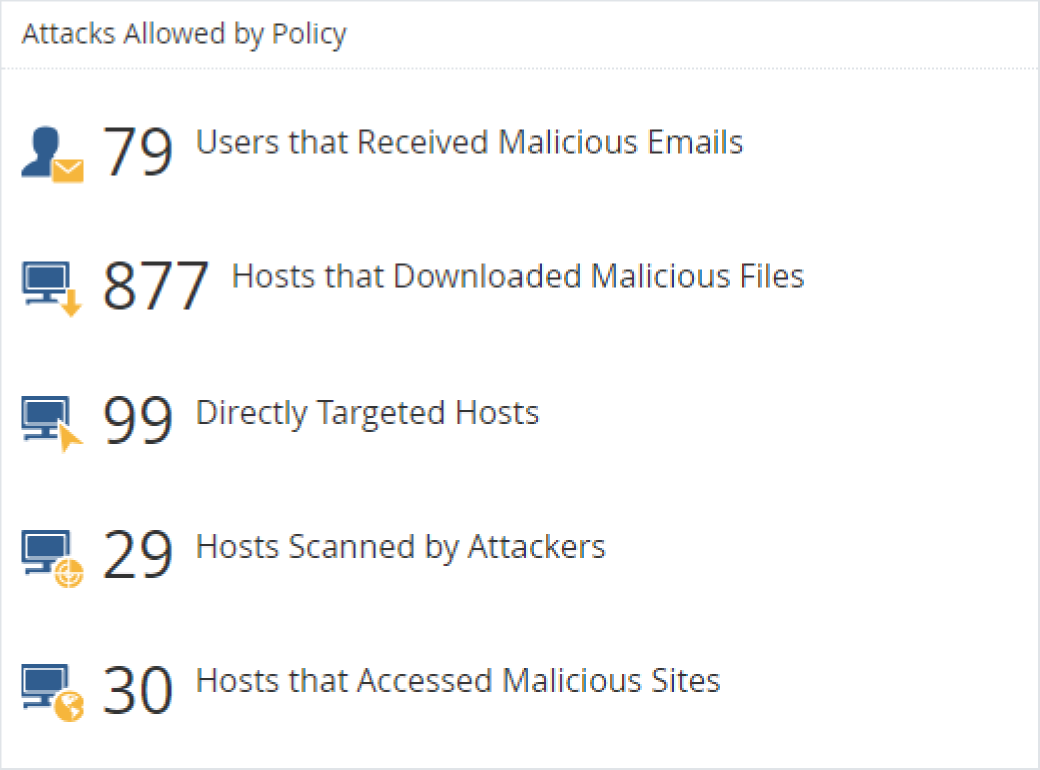
Attacks Allowed By Policy

This widget shows the number of attacks using different attack vectors that the current Security Policy allowed (because it was not configured to prevent them) over the selected report period.

Note - Select the report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

Understand the different vectors and types of attacks to improve your network protection.

Example:



Attacks Allowed by Policy

79 Users that Received Malicious Emails

877 Hosts that Downloaded Malicious Files

99 Directly Targeted Hosts

29 Hosts Scanned by Attackers

30 Hosts that Accessed Malicious Sites

To open the next drill-down level, double-click a headline or matching icon. See the sections below.

Widget Query:

In addition to the *"Default Query" on page 438*, the widget runs this query:

`Action > Equals > Bypass,Detect`
`Action > Equals > Bypass,Detect`

Users that Received Malicious Emails (Attacks Allowed By Policy)

Description

In the main **Cyber Attack View**, in the **Attacks Allowed By Policy** section, double-click **Users that Received Malicious Emails**.

Note - Select the report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

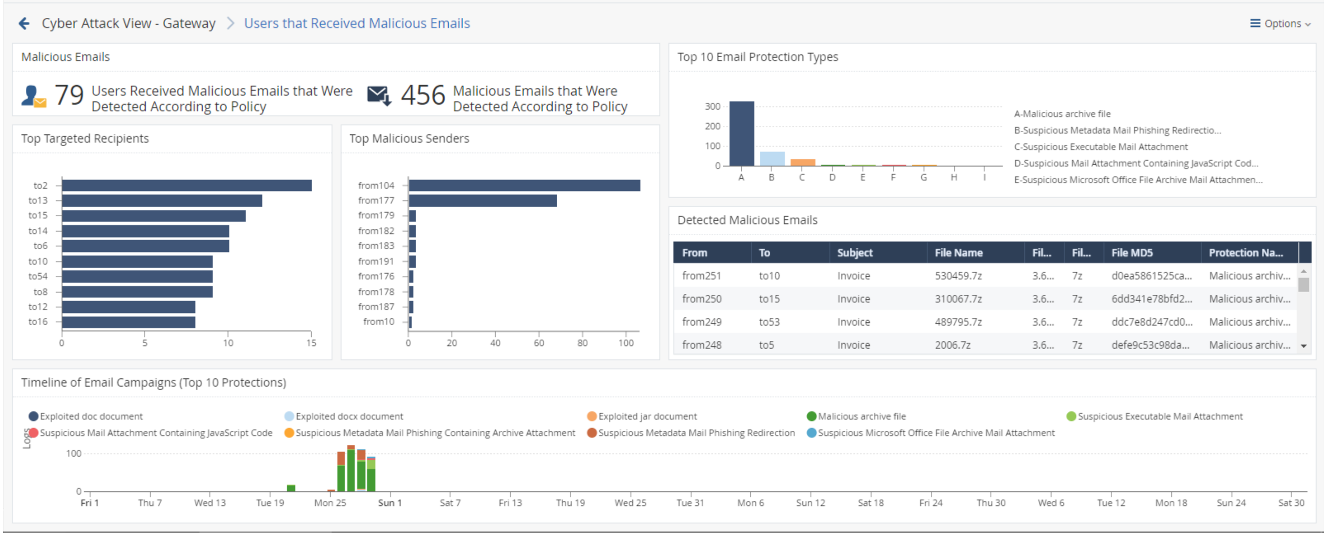
The email vector is the common vector used to deliver a malicious payload.

This drill-down view shows a summary of email attack attempts.

The IPS, Anti-Virus, Threat Emulation and Threat ExtractionSoftware Blades work in parallel to determine if an email is malicious and provide multi-layer protection.

Drill-Down View

This is an obfuscated example of the drill-down view:



Cyber Attack View - Gateway
Users that Received Malicious Emails
Options

Malicious Emails

79 Users Received Malicious Emails that Were Detected According to Policy

456 Malicious Emails that Were Detected According to Policy

Top Targeted Recipients

to2
to13
to15
to14
to6
to10
to54
to8
to12
to16
0
5
10
15

Top Malicious Senders

from104
from177
from179
from182
from183
from191
from176
from178
from187
from10
0
20
40
60
80
100

Top 10 Email Protection Types

300
200
100
0
A
B
C
D
E
F
G
H
I
A-Malicious archive file
B-Suspicious Metadata Mail Phishing Redirectio...
C-Suspicious Executable Mail Attachment
D-Suspicious Mail Attachment Containing JavaScript Cod...
E-Suspicious Microsoft Office File Archive Mail Attachmen...

Detected Malicious Emails

From	To	Subject	File Name	Fil...	Fil...	File MD5	Protection Na...
from251	to10	Invoice	530459.7z	3.6...	7z	d0ea5861525ca...	Malicious archiv...
from250	to15	Invoice	310067.7z	3.6...	7z	6dd341e78bfd2...	Malicious archiv...
from249	to53	Invoice	489795.7z	3.6...	7z	ddc7e8d247cd0...	Malicious archiv...
from248	to5	Invoice	2006.7z	3.6...	7z	defe9c53c98da...	Malicious archiv...

Timeline of Email Campaigns (Top 10 Protections)

Exploited doc document
Exploited docx document
Exploited jar document
Malicious archive file
Suspicious Executable Mail Attachment
Suspicious Mail Attachment Containing JavaScript Code
Suspicious Metadata Mail Phishing Containing Archive Attachment
Suspicious Metadata Mail Phishing Redirection
Suspicious Microsoft Office File Archive Mail Attachment
Logs
100
0
Fri 1
Thu 7
Wed 13
Tue 19
Mon 25
Sun 1
Sat 7
Fri 13
Thu 19
Wed 25
Tue 31
Mon 6
Sun 12
Sat 18
Fri 24
Thu 30
Wed 6
Tue 12
Mon 18
Sun 24
Sat 30

To see the applicable logs (the next drill-down level), double-click a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Malicious Emails	Infographic	Shows the total number of emails with content that the Security Gateway found as malicious.

Widget	Type	Description
Top 10 Email Protection Types	Chart	Shows top Check Point protections that found malicious emails. Shows: ■ The names of the top protections on (from all the Software Blades) that found malicious emails. ■ The number of malicious emails the top protections found. Different colors show different protection types.
Top Targeted Recipients	Chart	Shows the recipients of malicious emails sorted by the number of emails they received. Shows: ■ Users, who received the largest number of malicious emails. ■ The number of malicious emails they received. Different colors show different recipients.
Top Malicious Senders	Chart	Shows the senders of malicious emails sorted by the number of emails they sent. Shows: ■ Users, who sent the largest number of malicious emails. ■ The number of malicious emails they sent. Different colors show different senders.
Detected Malicious Emails	Table	Shows malicious emails. Shows this information about the detected malicious emails: ■ From ■ To ■ Subject ■ File Name ■ File Size ■ File MD5 ■ Protection Name

Widget	Type	Description
Timeline of Email Campaigns (Top 10 Protections)	Timeline	Shows the number of detected malicious emails and their timeline. The timeline is divided into different protection types. Different colors show different campaigns.

Widget Query

In addition to the *"Default Query" on page 438*, the widget runs this query:

```
Calculated Service > Equals > SMTP
```

```
Custom Filter = ((blade:ips AND ("Adobe Reader Violation" OR
"Content Protection Violation" OR "Mail Content Protection
Violation" OR "SMTP Protection Violation" OR "Phishing Enforcement
Protection" OR "Adobe Flash Protection Violation")) OR
(blade:"Threat Emulation") OR (blade:Anti-Virus ) OR
(blade:"Threat Extraction" AND content_risk ("Medium" OR "High" OR
"Critical"))) AND service:("pop3" OR "smtp" OR "imap")
```

Best Practices

Best practices against malicious emails:

- Examine the **Detected Malicious Emails** to see the number of emails with malicious content that the current Security Policydetected, but did not prevent.
- Examine the **Top 10 Email Protection Types** to see the top attack types.

  Pay attention to protections configured to work in **Detect** mode instead of **Prevent** mode. Fine-tune your email policy accordingly.
- In the Threat Prevention logs from the Security Gateway, examine the **Description** field (see *"Log Fields" on page 496*) to see if the Anti-Virus Software Blade work is in the **Background** or **Hold** mode.

  To do so, in the **Detected Malicious Emails**, double-click on one of the counters > open the log > refer to the **Description** field.

  In addition, read sk74120: Why Anti-Bot and Anti-Virus connections may be allowed even in Prevent mode.

Hosts that Downloaded Malicious Files (Attacks Allowed By Policy)

Description

In the main **Cyber Attack View**, in the **Attacks Allowed By Policy** section, double-click **Hosts that Downloaded Malicious Files**.

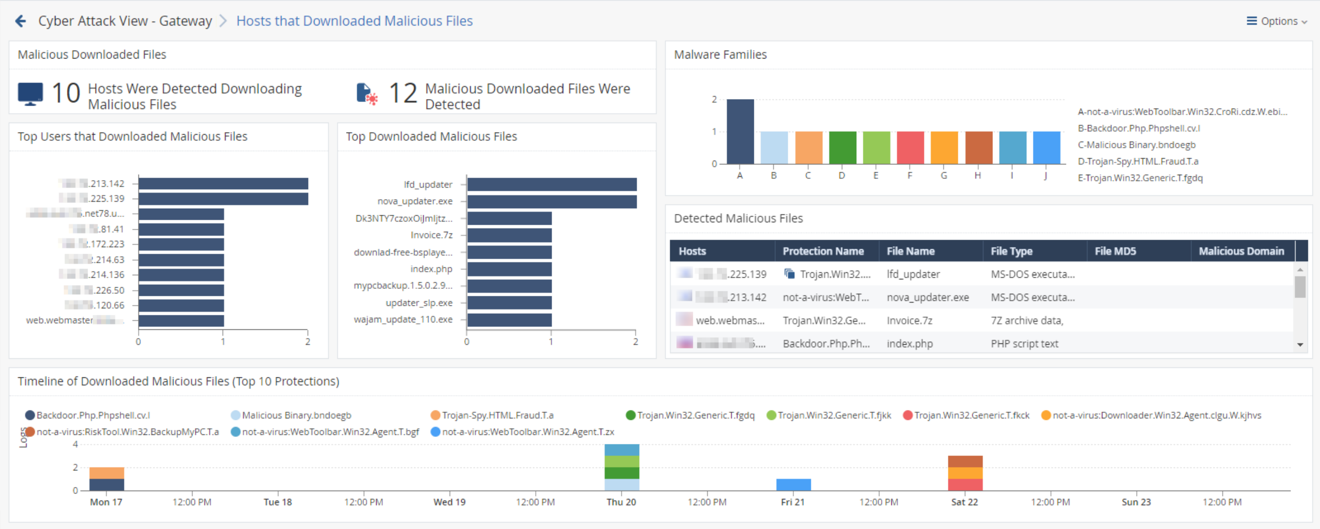
Note - Select the report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

This drill-down view shows a summary of attacks that used malicious files.

This drill-down view shows all the malicious files caught by Check Point Threat Prevention's multi-layer protections.

Drill-Down View

This is an obfuscated example of the drill-down view:



Cyber Attack View - Gateway > Hosts that Downloaded Malicious Files

Malicious Downloaded Files

10 Hosts Were Detected Downloading Malicious Files

12 Malicious Downloaded Files Were Detected

Detected Malicious Files

Hosts	Protection Name	File Name	File Type	File MD5	Malicious Domain
[redacted].225.139	Trojan.Win32....	lfd_updater	MS-DOS executa...		
[redacted].213.142	not-a-virus:WebT...	nova_updater.exe	MS-DOS executa...		
web.webmas...	Trojan.Win32.Ge...	Invoice.7z	7Z archive data,		
[redacted]5....	Backdoor.Php.Ph...	index.php	PHP script text		

Options
Top Users that Downloaded Malicious Files
[redacted].213.142
[redacted].225.139
[redacted].net78.u...
[redacted].81.41
[redacted].172.223
[redacted].214.63
[redacted].214.136
[redacted].226.50
[redacted].120.66
web.webmaster[redacted]
0
1
2
Top Downloaded Malicious Files
lfd_updater
nova_updater.exe
Dk3NTY7czoxOiJmljtz...
Invoice.7z
downlad-free-bsplaye...
index.php
mypcbackup.1.5.0.2.9...
updater_slp.exe
wajam_update_110.exe
0
1
2
Malware Families
2
1
0
A
B
C
D
E
F
G
H
I
J
A-not-a-virus:WebToolbar.Win32.CroRi.cdz.W.ebi...
B-Backdoor.Php.Phpshell.cv.l
C-Malicious Binary.bndoegb
D-Trojan-Spy.HTML.Fraud.T.a
E-Trojan.Win32.Generic.T.fgdq
Timeline of Downloaded Malicious Files (Top 10 Protections)
Backdoor.Php.Phpshell.cv.l
Malicious Binary.bndoegb
Trojan-Spy.HTML.Fraud.T.a
Trojan.Win32.Generic.T.fgdq
Trojan.Win32.Generic.T.fjkk
Trojan.Win32.Generic.T.fkck
not-a-virus:Downloader.Win32.Agent.clgu.W.kjhvs
not-a-virus:RiskTool.Win32.BackupMyPC.T.a
not-a-virus:WebToolbar.Win32.Agent.T.bgf
not-a-virus:WebToolbar.Win32.Agent.T.zx
Logs
4
2
0
Mon 17
12:00 PM
Tue 18
12:00 PM
Wed 19
12:00 PM
Thu 20
12:00 PM
Fri 21
12:00 PM
Sat 22
12:00 PM
Sun 23
12:00 PM

To see the applicable logs (the next drill-down level), double-click on a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Malicious Downloaded Files	Infographic	Shows: ■ The number of hosts that downloaded malicious files. ■ The number of downloaded malicious files.
Malware Families	Chart	Shows the top downloaded malware families (based on *Check Point ThreatWiki* and *Check Point Research*). Different colors show different families.
Top Users that Downloaded Malicious Files	Chart	Shows hosts that downloaded the largest number of malicious files. The chart is sorted by the number of downloaded malicious files.
Top Downloaded Malicious Files	Chart	Shows the number of downloads for the top malicious files. The chart is sorted by the number of appearances of downloaded malicious files.
Detected Malicious Files	Table	Shows the downloaded malicious files. Shows: ■ Hosts that downloaded malicious files ■ The name of the protection that detected the malicious files ■ The name of the malicious file ■ The type of the malicious file ■ The MD5 of the malicious file ■ Malicious Domain
Timeline of Downloaded Malicious Files (Top 10 Protections)	Timeline	Shows the number of logs for downloaded malicious files. Different colors show different files.

Widget Query

In addition to the *"Default Query" on page 438*, the widget runs this query:

```
Custom Filter = ((blade:"threat emulation") OR (blade:"anti-virus"
AND "signature") OR (blade:ips AND (("Adobe Reader Violation" OR
"Content Protection Violation" OR "Instant Messenger" OR "Adobe
Flash Protection Violation"))))
```

Best Practices

Best practices against malicious files:

- In the **Attacks Allowed By Policy** section, click **Hosts that Downloaded Malicious Files**.

  1. In the **Malicious Downloaded Files** widget, double-click the **Hosts Were Detected Downloading Malicious Files** infographic.

  2. Locate events from the IPS Software Blade only.

  3. Examine the IPS protections currently configured in **Detect** mode and decide if you can change them to **Prevent** mode.

     To configure IPS protections in SmartConsole: From the left navigation panel, click **Security Policies** > click the **Threat Prevention** section > at the bottom, click **IPS Protections** > edit the applicable IPS protection > install the Threat Prevention Policy.

- In the Threat Prevention logs from the Security Gateway, examine the **Description** field (see *"Log Fields" on page 496*) to see if the Anti-Virus Software Blade work is in the **Background** or **Hold** mode.

  In addition, read sk74120: Why Anti-Bot and Anti-Virus connections may be allowed even in Prevent mode.

Directly Targeted Hosts (Attacks Allowed By Policy)

Description

In the main **Cyber Attack View**, in the **Attacks Allowed By Policy** section, double-click **Directly Targeted Hosts**.

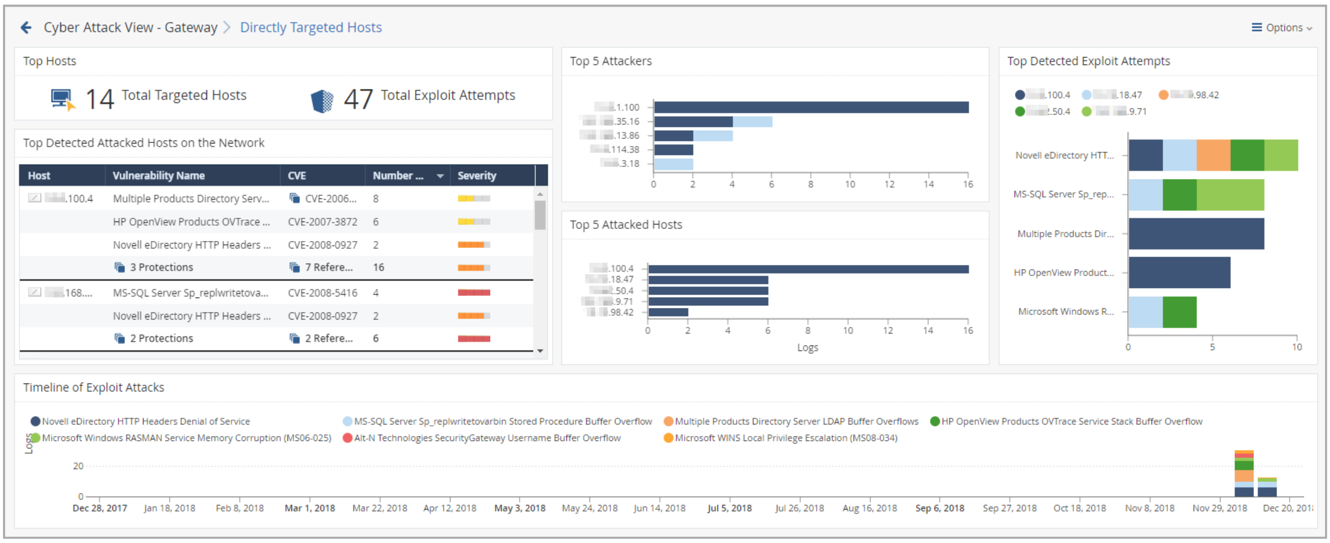
Note - Select the report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

This drill-down view shows a summary of network and hosts exploit attempts.

Host exploit attempts generate the majority of Threat Preventionevents.

Drill-Down View

This is an obfuscated example of the drill-down view:


Cyber Attack View - Gateway > Directly Targeted Hosts
Options
Top Hosts
14 Total Targeted Hosts
47 Total Exploit Attempts
Top Detected Attacked Hosts on the Network
Top 5 Attackers
.1.100
.35.16
.13.86
.114.38
.3.18
0 2 4 6 8 10 12 14 16
Top 5 Attacked Hosts
.100.4
.18.47
.50.4
.9.71
.98.42
0 2 4 6 8 10 12 14 16
Logs
Top Detected Exploit Attempts
.100.4
.18.47
.98.42
.50.4
.9.71
Novell eDirectory HTT...
MS-SQL Server Sp_rep...
Multiple Products Dir...
HP OpenView Product...
Microsoft Windows R...
0 5 10
Timeline of Exploit Attacks
Novell eDirectory HTTP Headers Denial of Service
MS-SQL Server Sp_replwritetovarbin Stored Procedure Buffer Overflow
Multiple Products Directory Server LDAP Buffer Overflows
HP OpenView Products OVTrace Service Stack Buffer Overflow
Microsoft Windows RASMAN Service Memory Corruption (MS06-025)
Alt-N Technologies SecurityGateway Username Buffer Overflow
Microsoft WINS Local Privilege Escalation (MS08-034)
Logs
20
0
Dec 28, 2017
Jan 18, 2018
Feb 8, 2018
Mar 1, 2018
Mar 22, 2018
Apr 12, 2018
May 3, 2018
May 24, 2018
Jun 14, 2018
Jul 5, 2018
Jul 26, 2018
Aug 16, 2018
Sep 6, 2018
Sep 27, 2018
Oct 18, 2018
Nov 8, 2018
Nov 29, 2018
Dec 20, 201

Host	Vulnerability Name	CVE	Number ...	Severity
.100.4	Multiple Products Directory Serv...	CVE-2006...	8	
	HP OpenView Products OVTrace ...	CVE-2007-3872	6	
	Novell eDirectory HTTP Headers ...	CVE-2008-0927	2	
	3 Protections	7 Refere...	16	
.168....	MS-SQL Server Sp_replwritetova...	CVE-2008-5416	4	
	Novell eDirectory HTTP Headers ...	CVE-2008-0927	2	
	2 Protections	2 Refere...	6	

To see the applicable logs (the next drill-down level), double-click on the desired value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Top Hosts	Infographic	Shows: - The total number of attacked internal hosts. - The total number of detected exploit attempts.

Widget	Type	Description
Top 5 Attackers	Chart	Shows the top attackers sorted by the number of their exploit attempts. Shows: ■ The source IP addresses of top attackers. ■ The number of logs for exploit attempts. Different colors show different exploited vulnerabilities. For more information, see the **Top Detected Exploits Attempts** widget.
Top 5 Attacked Hosts	Chart	Shows the top attacked hosts sorted by the number of attempted exploits. Shows: ■ The IP addresses of top attacked internal hosts. ■ The number of logs for attempted exploits.
Top Detected Exploit Attempts	Chart	Shows the top exploit attempts on internal hosts. Shows: ■ The names of the top detected exploits. ■ The number of logs for these exploits. Different colors show different exploited vulnerabilities.
Top Detected Attacked Hosts on the Network	Table	Shows the list of internal hosts and the exploit attempts they encountered. Shows: ■ The IP addresses of your attacked internal hosts. ■ Names of exploited vulnerabilities. ■ CVE ■ Amount of reported events for each attacked internal host. ■ Severity.
Timeline of Exploit Attacks	Timeline	Shows the names of exploited vulnerabilities and their timeline. The timeline is divided into different exploit attempts. Different colors show different exploited vulnerabilities.

Widget Query

In addition to the *"Default Query" on page 438*, the widget runs this query:

```
Custom Filter = blade:IPS NOT ("SMTP" OR "Adobe Reader Violation"
OR "Content Protection Violation" OR "Mail Content Protection
Violation" OR "SMTP Protection Violation" OR "Phishing Enforcement
Protection" OR "Adobe Flash Protection Violation" OR "Adobe Reader
Violation" OR "Content Protection Violation" OR "Instant
Messenger" OR "Adobe Flash Protection Violation" OR "Scanner
Enforcement Violation" OR "Port Scan" OR "Novell NMAP Protocol
Violation" OR "Adobe Flash Protection Violation" OR "Adobe
Shockwave Protection Violation" OR "Web Client Enforcement
Violation" OR "Exploit Kit")
```

Best Practices

Best practices against network and host exploits:

Category	Description
General Best Practices	■ Examine the **Top Detected Exploit Attempts** widget to understand what are the top exploits and vulnerabilities used to attack your network. This lets you determine if your network is under a specific massive attack, or if this is a false positive. This widget also shows the top attacked hosts. This lets you plan a "patch procedure" for your hosts based on the current exploit attempts. ■ To understand if an attacker performed a reconnaissance of a specific host: **a)** In the **Top 5 Attacked Hosts** widget, right-click a chart bar for a host. **b)** In the context menu, click **Filter: "***<IP Address>***"**. **c)** At the top, click **Cyber Attack View - Gateway**. **d)** Pay attention to the **Hosts Scanned by Attackers** counter. ■ Examine the **Timeline of Exploit Attacks** for trends. This lets you understand if your network is under a specific massive attack, or if this is a false positive. ■ Examine the **Top 5 Attackers** widget. Double-click on each IP address to see the applicable logs. In the logs, examine the source countries. Decide if you need to block these countries with a Geo Policy. ■ In the logs examine the **Resource** field (see *"Log Fields" on page 496*), which may contain the malicious request. This is the full path the attacker tried to access on your attacked internal host. ■ You can perform the detected attack by yourself (for example, you can use a local penetration tester). This provides a real test if the ability to exploit your internal host exists.

Category	Description
Best Practices for events that the Security Gateway detected, but did not prevent	■ Schedule SmartView to send an email with data regarding **Directly Targeted Hosts** attacks in your network. This is one of the most important steps to avoid exploits. This important email will expose incomplete or insecure security configurations. ■ Examine the current **IPS** configuration in SmartConsole and change the applicable settings to increase the security. ■ Examine the **Top 5 Attacked Hosts** and **Top Detected Exploit Attempts** widgets to find vulnerable internal hosts. Examine if there is a correlation between the software type and software version of the attacked internal hosts and the exploit attempt. Connect to the attacked internal hosts and determine if the exploit was successful. ■ For the attacked internal hosts, examine: • Time of the detected events. • Time the attacked internal hosts sent their traffic. • Amount of traffic the attacked internal hosts sent. • Geo location of the destination IP addresses, to which the attacked internal hosts sent their traffic. • Protocol and port the attacked internal hosts used to send their traffic. • Reputation of the destination IP addresses and domains, to which the attacked internal hosts sent their traffic. If you enable the Anti-Bot Software Blade on the Security Gateway, the logs can show connections with Command and Control (C&C) servers from your network.

Host Scanned by Attackers (Attacks Allowed By Policy)

Description

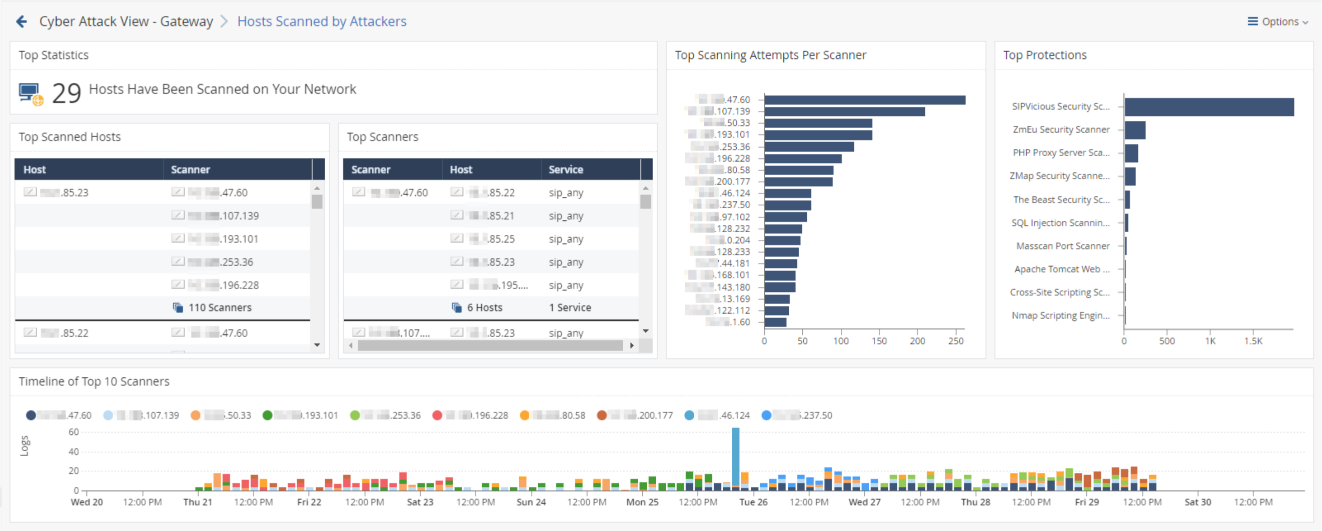
In the main **Cyber Attack View**, in the **Attacks Allowed By Policy** section, click **Host Scanned by Attackers**.

This drill-down view shows the scanned hosts on your internal network.

Network scanners are common. Expect to see many events related to this stage of an attack.

Drill-Down View

This is an obfuscated example of the drill-down view:



Cyber Attack View - Gateway > Hosts Scanned by Attackers

Top Statistics

29 Hosts Have Been Scanned on Your Network

Top Scanned Hosts

Host	Scanner
.85.23	.47.60
	.107.139
	.193.101
	.253.36
	.196.228
	110 Scanners
.85.22	.47.60

Top Scanners

Scanner	Host	Service
.47.60	.85.22	sip_any
	.85.21	sip_any
	.85.25	sip_any
	.85.23	sip_any
	.195....	sip_any
	6 Hosts	1 Service
.107....	.85.23	sip_any

To see the applicable logs (the next drill-down level), double-click on a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Top Statistics	Infographic	Shows the number of internal hosts scanned the most.

Widget	Type	Description
Top Scanning Attempts Per Scanner	Chart	Shows the scanners and the number of their scan attempts. The chart is ordered by the by number of scan attempts. Shows: ▪ The scanner source IP addresses. ▪ The number of scan attempts for each scanner.
Top Protections	Chart	Shows the top protections that reported the scan events. Shows: ▪ The names of protections that reported the largest number of scan events. ▪ The number of detected scan events for each protection.
Top Scanned Hosts	Table	Shows information about the most scanned internal hosts: ▪ Destination (host) IP addresses. ▪ Source (scanner) IP addresses. ▪ The total number of destinations and sources.
Top Scanners	Table	Shows information about the scanners: ▪ Source (scanner) IP address. ▪ Destination (host) IP addresses and total number of scanned destinations. ▪ Check Point services, to which these scan attempts matched (Protocols and Ports).
Timeline of Top 10 Scanners	Timeline	Shows the number of scanned hosts for each detected scanner and their timeline. Different colors show different scanners.

Widget Query

In addition to the *"Default Query" on page 438*, the widget runs this query:

```
Custom Filter = "Scanner Enforcement Violation" OR "Port Scan" OR
"Novell NMAP Protocol Violation"
```

Best Practices

Best practices against network reconnaissance attempts:

1. Find the hosts that are able to connect to external networks **through** the Security Gateway.

   Configure the applicable Access Control rules for hosts that you do not want to connect to external networks.

2. If you use your own vulnerability scanner, you have two options:

   - Add an exception to your policy, so that the Security Gateway does not enforce protections against this scanner.
   - If you still want the Security Gateway to report events generated by your scanner, then run an explicit query that excludes your scanner and shows only the external scanners.

3. Use logs generated by scanning events to determine if new hosts on the network are connecting to the outside world.

Hosts that Accessed Malicious Sites (Attacks Allowed By Policy)

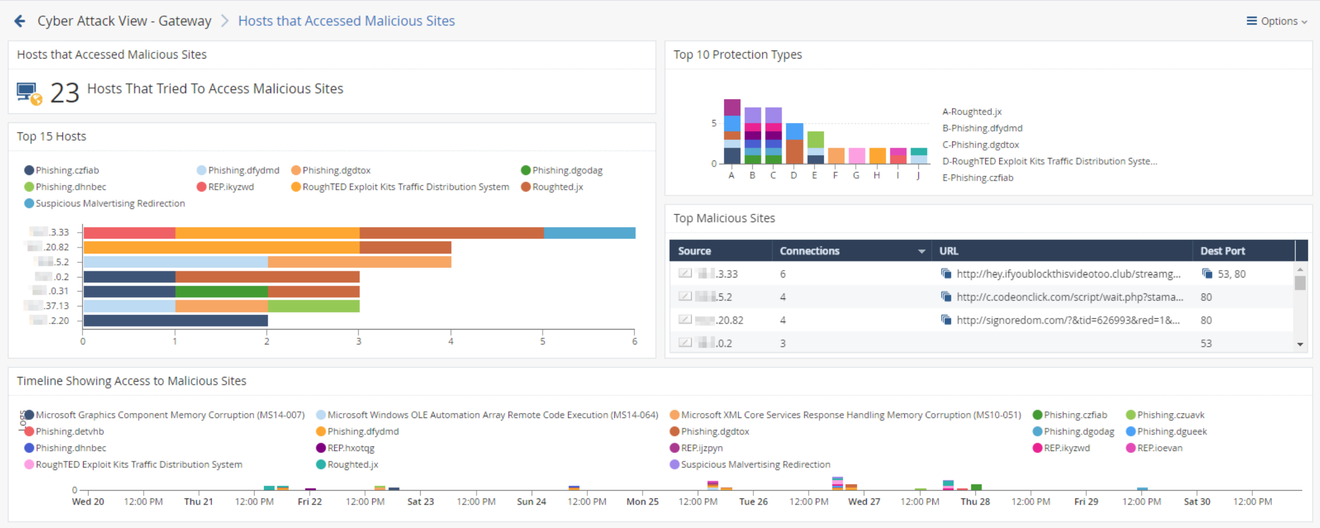
Description

In the main **Cyber Attack View**, in the **Attacks Allowed By Policy** section, double-click **Hosts that Accessed Malicious Sites**.

The drill-down view summarizes access attempts to malicious sites from the internal network.

Drill-Down View

This is an obfuscated example of the drill-down view:



Cyber Attack View - Gateway > Hosts that Accessed Malicious Sites

Hosts that Accessed Malicious Sites

23 Hosts That Tried To Access Malicious Sites

Top Malicious Sites

Source	Connections	URL	Dest Port
[redacted].3.33	6	http://hey.ifyoublockthisvideotoo.club/streamg...	53, 80
[redacted].5.2	4	http://c.codeonclick.com/script/wait.php?stama...	80
[redacted].20.82	4	http://signoredom.com/?&tid=626993&red=1&...	80
[redacted].0.2	3		53

To see the applicable logs (the next drill-down level), double-click on a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Hosts that Accessed Malicious Sites	Infographic	Shows the number of internal hosts that accessed malicious websites.
Top 10 Protection Types	Chart	Shows the number of events reported by web attack protections for the detected malware families (based on *Check Point ThreatWiki* and *Check Point Research*). Different colors show different malware families.

Widget	Type	Description
Top 15 Hosts	Chart	Shows the internal hosts that accessed malicious websites. The chart is ordered by the number of connections from each host. Shows: ■ The source IP addresses of internal hosts that accessed malicious websites. ■ The detected malware families (based on *Check Point ThreatWiki* and *Check Point Research*). ■ The number of logged connections from each host. Different colors show different malware families.
Top Malicious Sites	Table	Shows the information about malicious websites. Shows: ■ The source IP addresses of internal hosts. ■ The number of logged connections from each host. ■ URLs of malicious sites. ■ Destination ports of malicious sites.
Timeline Showing Access to Malicious Sites	Timeline	Shows the detected malware families and their timeline. The timeline is divided into protection types. Different colors show different malware families.

Widget Query

In addition to the *"Default Query" on page 438*, the widget runs this query:

```
Custom Filter = ((blade:IPS AND ("Adobe Flash Protection
Violation" OR "Adobe Shockwave Protection Violation" OR "Web
Client Enforcement Violation" OR "Exploit Kit")) OR (blade:Anti-
Virus AND ("URL Reputation" OR "DNS Reputation")))
```

```
Calculated Service > Not equals > smtp
```

Best Practices

Best practices against malicious sites:

- Examine the Threat Prevention logs to determine how much data (if at all) your internal hosts sent to and received from malicious websites.

  If these logs show extremely low, or zero, amount of data, read sk74120: Why Anti-Bot and Anti-Virus connections may be allowed even in Prevent mode.

- In the Threat Prevention logs from the Security Gateway, examine the **Description** field (see *"Log Fields" on page 496*) to see if the Anti-Virus Software Blade work is in the **Background** or **Hold** mode.

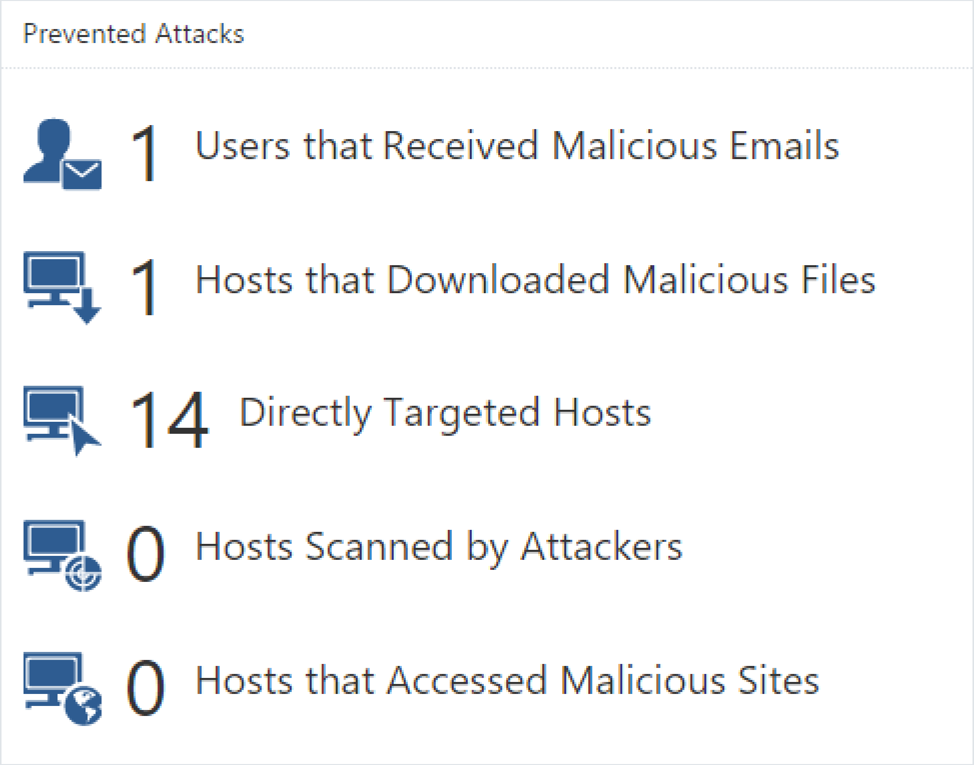
  In addition, read sk74120: Why Anti-Bot and Anti-Virus connections may be allowed even in Prevent mode.

Attacks Prevented By Policy

This widget shows the number of attacks using different attack vectors that the Security Policy prevented over the selected report period.

Note - Select the report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

Example:



Prevented Attacks

1 Users that Received Malicious Emails

1 Hosts that Downloaded Malicious Files

14 Directly Targeted Hosts

0 Hosts Scanned by Attackers

0 Hosts that Accessed Malicious Sites

To open the next drill-down level, double-click a headline or matching icon. See the sections below.

Widget Query:

In addition to the *"Default Query" on page 438*, the widget runs this query:

```
Action > Equals > Drop,Reject,Block,Prevent,Redirect
```

Users that Received Malicious Emails (Prevented Attacks)

Description

In the main **Cyber Attack View**, in the **Prevented Attacks** section, double-click **Users that Received Malicious Emails**.

> **Note** - Select the report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

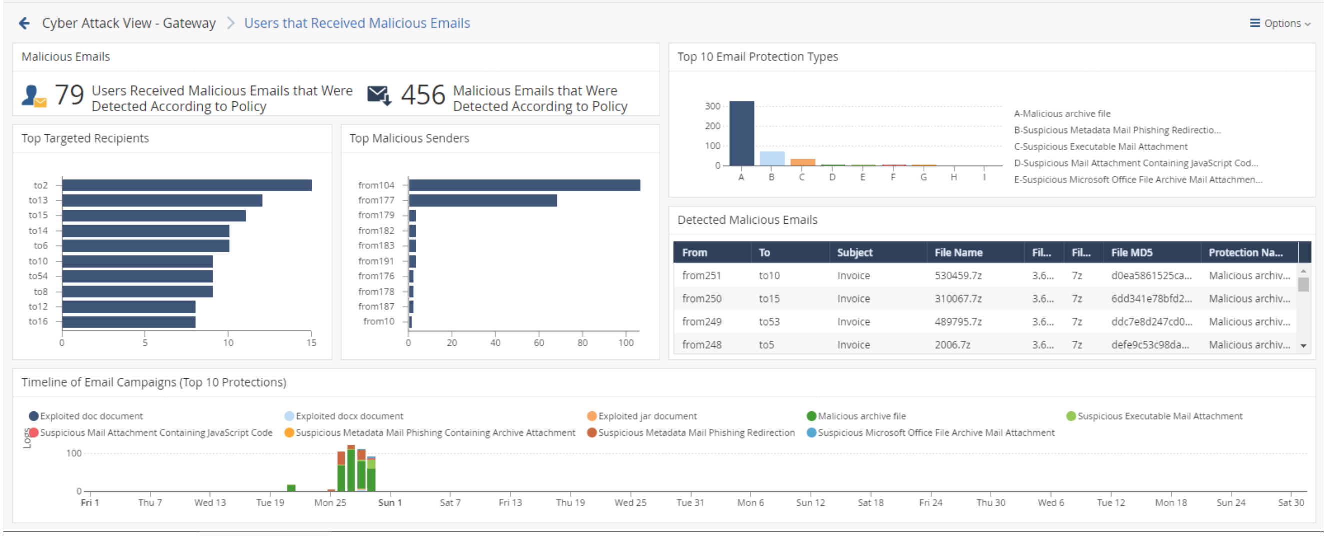
The email vector is the common vector used to deliver a malicious payload.

This drill-down view shows a summary of email attack attempts.

The IPS, Anti-Virus, Threat Emulation and Threat ExtractionSoftware Blades work in parallel to determine if an email is malicious and provide multi-layer protection.

Drill-Down View

This is an obfuscated example of the drill-down view:



Malicious Emails

79 Users Received Malicious Emails that Were Detected According to Policy

456 Malicious Emails that Were Detected According to Policy

Detected Malicious Emails

From	To	Subject	File Name	Fil...	Fil...	File MD5	Protection Na...
from251	to10	Invoice	530459.7z	3.6...	7z	d0ea5861525ca...	Malicious archiv...
from250	to15	Invoice	310067.7z	3.6...	7z	6dd341e78bfd2...	Malicious archiv...
from249	to53	Invoice	489795.7z	3.6...	7z	ddc7e8d247cd0...	Malicious archiv...
from248	to5	Invoice	2006.7z	3.6...	7z	defe9c53c98da...	Malicious archiv...

Cyber Attack View - Gateway
Users that Received Malicious Emails
Options
Top Targeted Recipients
to2
to13
to15
to14
to6
to10
to54
to8
to12
to16
0
5
10
15
Top Malicious Senders
from104
from177
from179
from182
from183
from191
from176
from178
from187
from10
0
20
40
60
80
100
Top 10 Email Protection Types
300
200
100
0
A
B
C
D
E
F
G
H
I
A-Malicious archive file
B-Suspicious Metadata Mail Phishing Redirectio...
C-Suspicious Executable Mail Attachment
D-Suspicious Mail Attachment Containing JavaScript Cod...
E-Suspicious Microsoft Office File Archive Mail Attachmen...
Timeline of Email Campaigns (Top 10 Protections)
Exploited doc document
Exploited docx document
Exploited jar document
Malicious archive file
Suspicious Executable Mail Attachment
Suspicious Mail Attachment Containing JavaScript Code
Suspicious Metadata Mail Phishing Containing Archive Attachment
Suspicious Metadata Mail Phishing Redirection
Suspicious Microsoft Office File Archive Mail Attachment
Logs
100
0
Fri 1
Thu 7
Wed 13
Tue 19
Mon 25
Sun 1
Sat 7
Fri 13
Thu 19
Wed 25
Tue 31
Mon 6
Sun 12
Sat 18
Fri 24
Thu 30
Wed 6
Tue 12
Mon 18
Sun 24
Sat 30

To see the applicable logs (the next drill-down level), double-click a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Malicious Emails	Infographic	Shows the total number of emails with content that the Security Gateway found as malicious.
Top 10 Email Protection Types	Chart	Shows top Check Point protections that found malicious emails. Shows: ■ The names of the top protections on (from all the Software Blades) that found malicious emails. ■ The number of malicious emails the top protections found. Different colors show different protection types.
Top Targeted Recipients	Chart	Shows the recipients of malicious emails sorted by the number of emails they received. Shows: ■ Users, who received the largest number of malicious emails. ■ The number of malicious emails they received. Different colors show different recipients.
Top Malicious Senders	Chart	Shows the senders of malicious emails sorted by the number of emails they sent. Shows: ■ Users, who sent the largest number of malicious emails. ■ The number of malicious emails they sent. Different colors show different senders.

Widget	Type	Description
Detected Malicious Emails	Table	Shows malicious emails. Shows this information about the detected malicious emails: ■ From ■ To ■ Subject ■ File Name ■ File Size ■ File MD5 ■ Protection Name
Timeline of Email Campaigns (Top 10 Protections)	Timeline	Shows the number of detected malicious emails and their timeline. The timeline is divided into different protection types. Different colors show different campaigns.

Widget Query

In addition to the *"Default Query" on page 438*, the widget runs this query:

```
Calculated Service > Equals > SMTP
```

```
Custom Filter = ((blade:ips AND ("Adobe Reader Violation" OR
"Content Protection Violation" OR "Mail Content Protection
Violation" OR "SMTP Protection Violation" OR "Phishing Enforcement
Protection" OR "Adobe Flash Protection Violation")) OR
(blade:"Threat Emulation") OR (blade:Anti-Virus ) OR
(blade:"Threat Extraction" AND content_risk ("Medium" OR "High" OR
"Critical"))) AND service:("pop3" OR "smtp" OR "imap")
```

Best Practices

Best practices against malicious emails:

- Examine the **Timeline of Email Campaigns (Top 10 Protections)** to see email attack trends against your organization.
- To fine-tune your email protection policy, examine the **Top 10 Email Protection Types** to see the top attack types.

  For example, if you see that the top protection that detected malicious emails is **Malicious archive file**, you need to decide if your Security Policy needs to allow archives in emails.

If you need to allow archives in emails, change your policy accordingly to prevent malicious files and not detect them. This includes enabling more Software Blades, if needed (such as Threat Emulationand Threat Extraction).

- Examine the **Top Targeted Recipients** to understand:
  - Why are these internal email addresses exposed outside of your organization?
  - Should these internal email addresses be known outside of your organization from a business perspective?

Hosts that Downloaded Malicious Files (Prevented Attacks)

Description

In the main **Cyber Attack View**, in the **Prevented Attacks** section, double-click **Hosts that Downloaded Malicious Files**.

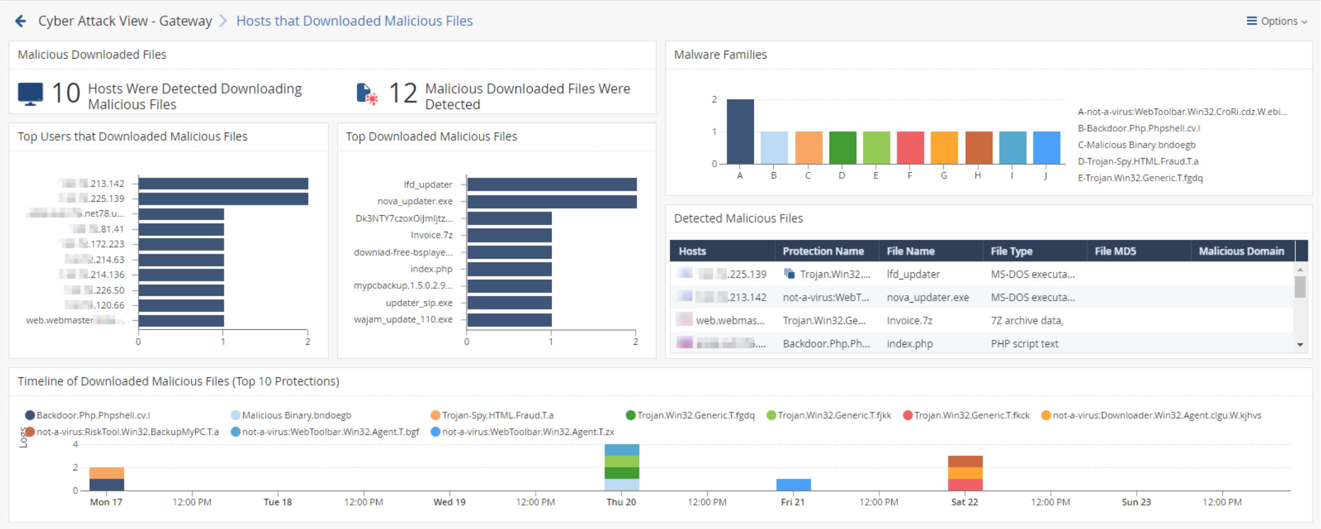
Note - Select the report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

This drill-down view shows a summary of attacks that used malicious files.

This drill-down view shows all the malicious files caught by Check Point Threat Prevention's multi-layer protections.

Drill-Down View

This is an obfuscated example of the drill-down view:



Cyber Attack View - Gateway > Hosts that Downloaded Malicious Files

Malicious Downloaded Files

10 Hosts Were Detected Downloading Malicious Files

12 Malicious Downloaded Files Were Detected

Detected Malicious Files

Hosts	Protection Name	File Name	File Type	File MD5	Malicious Domain
[redacted].225.139	Trojan.Win32....	lfd_updater	MS-DOS executa...		
[redacted].213.142	not-a-virus:WebT...	nova_updater.exe	MS-DOS executa...		
web.webmas...	Trojan.Win32.Ge...	Invoice.7z	7Z archive data,		
[redacted]5....	Backdoor.Php.Ph...	index.php	PHP script text		

Options
Top Users that Downloaded Malicious Files
[redacted].213.142
[redacted].225.139
[redacted].net78.u...
[redacted].81.41
[redacted].172.223
[redacted].214.63
[redacted].214.136
[redacted].226.50
[redacted].120.66
web.webmaster[redacted]
0
1
2
Top Downloaded Malicious Files
lfd_updater
nova_updater.exe
Dk3NTY7czoxOiJmljtz...
Invoice.7z
downlad-free-bsplaye...
index.php
mypcbackup.1.5.0.2.9...
updater_slp.exe
wajam_update_110.exe
0
1
2
Malware Families
2
1
0
A
B
C
D
E
F
G
H
I
J
A-not-a-virus:WebToolbar.Win32.CroRi.cdz.W.ebi...
B-Backdoor.Php.Phpshell.cv.l
C-Malicious Binary.bndoegb
D-Trojan-Spy.HTML.Fraud.T.a
E-Trojan.Win32.Generic.T.fgdq
Timeline of Downloaded Malicious Files (Top 10 Protections)
Backdoor.Php.Phpshell.cv.l
Malicious Binary.bndoegb
Trojan-Spy.HTML.Fraud.T.a
Trojan.Win32.Generic.T.fgdq
Trojan.Win32.Generic.T.fjkk
Trojan.Win32.Generic.T.fkck
not-a-virus:Downloader.Win32.Agent.clgu.W.kjhvs
not-a-virus:RiskTool.Win32.BackupMyPC.T.a
not-a-virus:WebToolbar.Win32.Agent.T.bgf
not-a-virus:WebToolbar.Win32.Agent.T.zx
Logs
4
2
0
Mon 17
12:00 PM
Tue 18
12:00 PM
Wed 19
12:00 PM
Thu 20
12:00 PM
Fri 21
12:00 PM
Sat 22
12:00 PM
Sun 23
12:00 PM

To see the applicable logs (the next drill-down level), double-click on a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Malicious Downloaded Files	Infographic	Shows: ■ The number of hosts that downloaded malicious files. ■ The number of downloaded malicious files.

Widget	Type	Description
Malware Families	Chart	Shows the top downloaded malware families (based on *Check Point ThreatWiki* and *Check Point Research*). Different colors show different families.
Top Users that Downloaded Malicious Files	Chart	Shows hosts that downloaded the largest number of malicious files. The chart is sorted by the number of downloaded malicious files.
Top Downloaded Malicious Files	Chart	Shows the number of downloads for the top malicious files. The chart is sorted by the number of appearances of downloaded malicious files.
Detected Malicious Files	Table	Shows the downloaded malicious files. Shows: ■ Hosts that downloaded malicious files ■ The name of the protection that detected the malicious files ■ The name of the malicious file ■ The type of the malicious file ■ The MD5 of the malicious file ■ Malicious Domain
Timeline of Downloaded Malicious Files (Top 10 Protections)	Timeline	Shows the number of logs for downloaded malicious files. Different colors show different files.

Widget Query

In addition to the *"Default Query" on page 438*, the widget runs this query:

```
Custom Filter = ((blade:"threat emulation") OR (blade:"anti-virus"
AND "signature") OR (blade:ips AND (("Adobe Reader Violation" OR
"Content Protection Violation" OR "Instant Messenger" OR "Adobe
Flash Protection Violation"))))
```

Best Practices

Best practices against malicious files:

- Examine the **Top Downloaded Malicious Files**.

  If you see a specific malicious file downloaded many times, treat it as attack campaign against your network.

- Examine the **Detected Malicious Files** widget.
- Look for the common malicious domains related to the malicious files. In case a domain appears many times:
  1. If this is an unknown website, add this site to your black list (with the URL Filtering blade).
  2. If this is a known website, contact the site owner to alert them about a possible attack on their website.
  3. If this is your website, investigate the issue and contact *Check Point Incident Response Team*.

Directly Targeted Hosts (Prevented Attacks)

Description

In the main **Cyber Attack View**, in the **Prevented Attacks** section, double-click **Directly Targeted Hosts**.

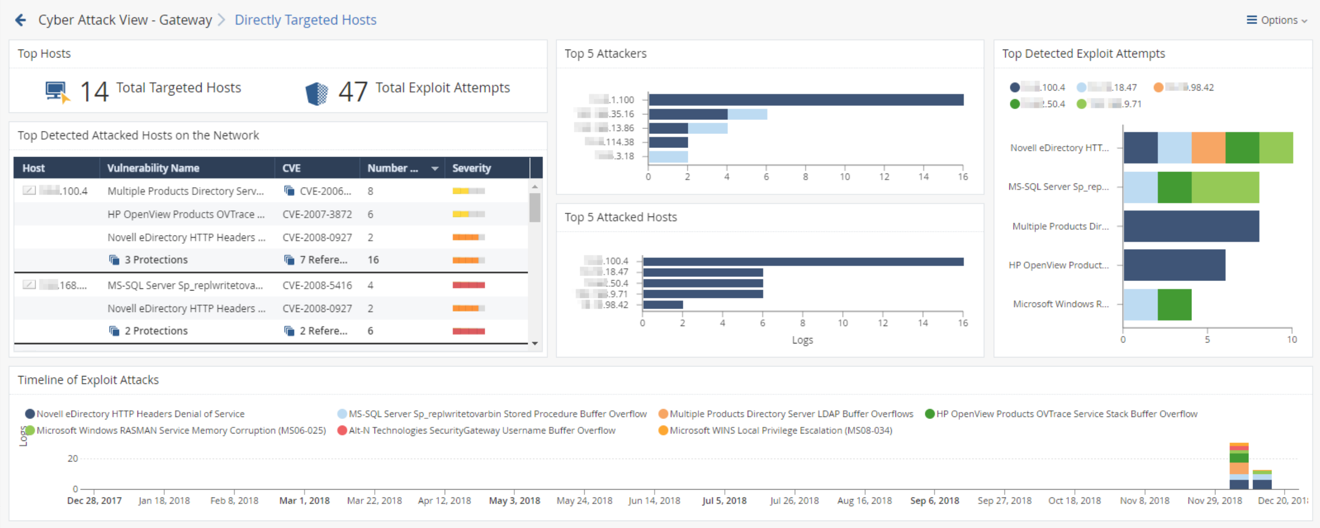
Note - Select the report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

This drill-down view shows a summary of network and hosts exploit attempts.

Host exploit attempts generate the majority of Threat Prevention events.

Drill-Down View

This is an obfuscated example of the drill-down view:



Host	Vulnerability Name	CVE	Number ...	Severity
[redacted].100.4	Multiple Products Directory Serv...	CVE-2006...	8	🟨
	HP OpenView Products OVTrace ...	CVE-2007-3872	6	🟨
	Novell eDirectory HTTP Headers ...	CVE-2008-0927	2	🟧
	3 Protections	7 Refere...	16	🟧
[redacted].168....	MS-SQL Server Sp_replwritetova...	CVE-2008-5416	4	🟥
	Novell eDirectory HTTP Headers ...	CVE-2008-0927	2	🟧
	2 Protections	2 Refere...	6	🟥

To see the applicable logs (the next drill-down level), double-click on the desired value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Top Hosts	Infographic	Shows: ■ The total number of attacked internal hosts. ■ The total number of detected exploit attempts.
Top 5 Attackers	Chart	Shows the top attackers sorted by the number of their exploit attempts. Shows: ■ The source IP addresses of top attackers. ■ The number of logs for exploit attempts. Different colors show different exploited vulnerabilities. For more information, see the **Top Detected Exploits Attempts** widget.
Top 5 Attacked Hosts	Chart	Shows the top attacked hosts sorted by the number of attempted exploits. Shows: ■ The IP addresses of top attacked internal hosts. ■ The number of logs for attempted exploits.
Top Detected Exploit Attempts	Chart	Shows the top exploit attempts on internal hosts. Shows: ■ The names of the top detected exploits. ■ The number of logs for these exploits. Different colors show different exploited vulnerabilities.

Widget	Type	Description
Top Detected Attacked Hosts on the Network	Table	Shows the list of internal hosts and the exploit attempts they encountered. Shows: ■ The IP addresses of your attacked internal hosts. ■ Names of exploited vulnerabilities. ■ CVE ■ Amount of reported events for each attacked internal host. ■ Severity.
Timeline of Exploit Attacks	Timeline	Shows the names of exploited vulnerabilities and their timeline. The timeline is divided into different exploit attempts. Different colors show different exploited vulnerabilities.

Widget Query

In addition to the *"Default Query" on page 438*, the widget runs this query:

```
Custom Filter = blade:IPS NOT ("SMTP" OR "Adobe Reader Violation"
OR "Content Protection Violation" OR "Mail Content Protection
Violation" OR "SMTP Protection Violation" OR "Phishing Enforcement
Protection" OR "Adobe Flash Protection Violation" OR "Adobe Reader
Violation" OR "Content Protection Violation" OR "Instant
Messenger" OR "Adobe Flash Protection Violation" OR "Scanner
Enforcement Violation" OR "Port Scan" OR "Novell NMAP Protocol
Violation" OR "Adobe Flash Protection Violation" OR "Adobe
Shockwave Protection Violation" OR "Web Client Enforcement
Violation" OR "Exploit Kit")
```

Best Practices

Best practices against network and host exploits:

Category	Description
General Best Practices	■ Examine the **Top Detected Exploit Attempts** widget to understand what are the top exploits and vulnerabilities used to attack your network. This lets you determine if your network is under a specific massive attack, or if this is a false positive. This widget also shows the top attacked hosts. This lets you plan a "patch procedure" for your hosts based on the current exploit attempts. ■ To understand if an attacker performed a reconnaissance of a specific host: **a)** In the **Top 5 Attacked Hosts** widget, right-click a chart bar for a host. **b)** In the context menu, click **Filter: "***<IP Address>***"**. **c)** At the top, click **Cyber Attack View - Gateway**. **d)** Pay attention to the **Hosts Scanned by Attackers** counter. ■ Examine the **Timeline of Exploit Attacks** for trends. This lets you understand if your network is under a specific massive attack, or if this is a false positive. ■ Examine the **Top 5 Attackers** widget. Double-click on each IP address to see the applicable logs. In the logs, examine the source countries. Decide if you need to block these countries with a Geo Policy. ■ In the logs examine the **Resource** field (see *"Log Fields" on page 496*), which may contain the malicious request. This is the full path the attacker tried to access on your attacked internal host. ■ You can perform the detected attack by yourself (for example, you can use a local penetration tester). This provides a real test if the ability to exploit your internal host exists.
Best Practices for events that the Security Gateway prevented	■ Examine the **Top Detected Exploit Attempts** to determine if the Security Gateway prevented an attack campaign against you network. ■ Examine (once a month) what are the top exploit attempts against your network. The Check Point Security CheckUp report uses the same queries and shows a full list of attacks and assets in your organization.

Host Scanned by Attackers (Prevented Attacks)

Description

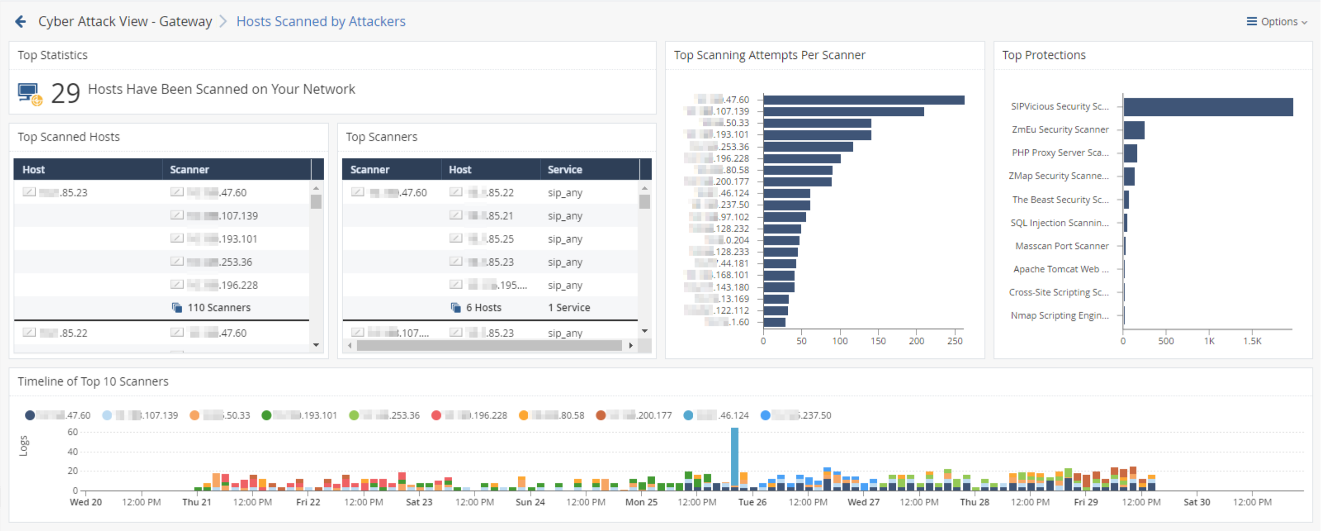
In the main **Cyber Attack View**, in the **Prevented Attacks** section, click **Host Scanned by Attackers**.

This drill-down view shows the scanned hosts on your internal network.

Network scanners are common. Expect to see many events related to this stage of an attack.

Drill-Down View

This is an obfuscated example of the drill-down view:



Cyber Attack View - Gateway > Hosts Scanned by Attackers

Top Statistics

29 Hosts Have Been Scanned on Your Network

Top Scanned Hosts

Host	Scanner
.85.23	.47.60
	.107.139
	.193.101
	.253.36
	.196.228
	110 Scanners
.85.22	.47.60

Top Scanners

Scanner	Host	Service
.47.60	.85.22	sip_any
	.85.21	sip_any
	.85.25	sip_any
	.85.23	sip_any
	.195....	sip_any
	6 Hosts	1 Service
.107....	.85.23	sip_any

To see the applicable logs (the next drill-down level), double-click on a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Top Statistics	Infographic	Shows the number of internal hosts scanned the most.

Widget	Type	Description
Top Scanning Attempts Per Scanner	Chart	Shows the scanners and the number of their scan attempts. The chart is ordered by the by number of scan attempts. Shows: ▪ The scanner source IP addresses. ▪ The number of scan attempts for each scanner.
Top Protections	Chart	Shows the top protections that reported the scan events. Shows: ▪ The names of protections that reported the largest number of scan events. ▪ The number of detected scan events for each protection.
Top Scanned Hosts	Table	Shows information about the most scanned internal hosts: ▪ Destination (host) IP addresses. ▪ Source (scanner) IP addresses. ▪ The total number of destinations and sources.
Top Scanners	Table	Shows information about the scanners: ▪ Source (scanner) IP address. ▪ Destination (host) IP addresses and total number of scanned destinations. ▪ Check Point services, to which these scan attempts matched (Protocols and Ports).
Timeline of Top 10 Scanners	Timeline	Shows the number of scanned hosts for each detected scanner and their timeline. Different colors show different scanners.

Widget Query

In addition to the *"Default Query" on page 438*, the widget runs this query:

```
Custom Filter = "Scanner Enforcement Violation" OR "Port Scan" OR
"Novell NMAP Protocol Violation"
```

Best Practices

Best practices against network reconnaissance attempts:

1. Find the hosts that are able to connect to external networks **through** the Security Gateway.

   Configure the applicable Access Control rules for hosts that you do not want to connect to external networks.

2. If you use your own vulnerability scanner, you have two options:

   - Add an exception to your policy, so that the Security Gateway does not enforce protections against this scanner.
   - If you still want the Security Gateway to report events generated by your scanner, then run an explicit query that excludes your scanner and shows only the external scanners.

3. Use logs generated by scanning events to determine if new hosts on the network are connecting to the outside world.

Hosts that Accessed Malicious Sites (Prevented Attacks)

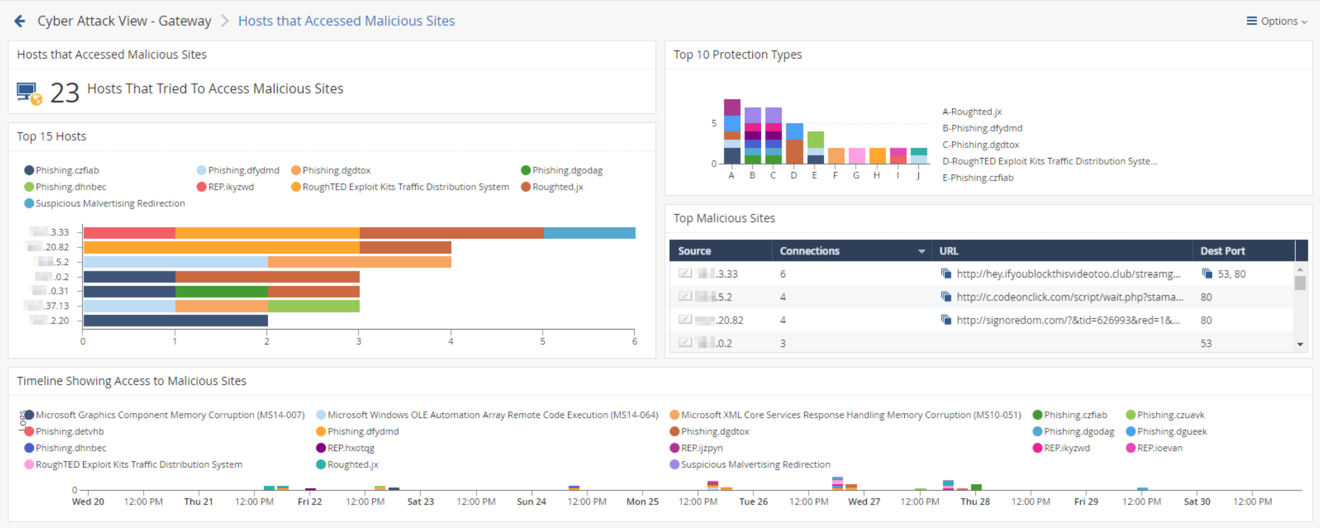
Description

In the main **Cyber Attack View**, in the **Prevented Attacks** section, double-click **Hosts that Accessed Malicious Sites**.

The drill-down view summarizes access attempts to malicious sites from the internal network.

Drill-Down View

This is an obfuscated example of the drill-down view:



Cyber Attack View - Gateway > Hosts that Accessed Malicious Sites

Hosts that Accessed Malicious Sites

23 Hosts That Tried To Access Malicious Sites

Top 15 Hosts

Top 10 Protection Types

Top Malicious Sites

Source	Connections	URL	Dest Port
.3.33	6	http://hey.ifyoublockthisvideotoo.club/streamg...	53, 80
.5.2	4	http://c.codeonclick.com/script/wait.php?stama...	80
.20.82	4	http://signoredom.com/?&tid=626993&red=1&...	80
.0.2	3		53

Timeline Showing Access to Malicious Sites

To see the applicable logs (the next drill-down level), double-click on a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Hosts that Accessed Malicious Sites	Infographic	Shows the number of internal hosts that accessed malicious websites.
Top 10 Protection Types	Chart	Shows the number of events reported by web attack protections for the detected malware families (based on *Check Point ThreatWiki* and *Check Point Research*). Different colors show different malware families.

Widget	Type	Description
Top 15 Hosts	Chart	Shows the internal hosts that accessed malicious websites. The chart is ordered by the number of connections from each host. Shows: - The source IP addresses of internal hosts that accessed malicious websites. - The detected malware families (based on *Check Point ThreatWiki* and *Check Point Research*). - The number of logged connections from each host. Different colors show different malware families.
Top Malicious Sites	Table	Shows the information about malicious websites. Shows: - The source IP addresses of internal hosts. - The number of logged connections from each host. - URLs of malicious sites. - Destination ports of malicious sites.
Timeline Showing Access to Malicious Sites	Timeline	Shows the detected malware families and their timeline. The timeline is divided into protection types. Different colors show different malware families.

Widget Query

In addition to the *"Default Query" on page 438*, the widget runs this query:

```
Custom Filter = ((blade:IPS AND ("Adobe Flash Protection
Violation" OR "Adobe Shockwave Protection Violation" OR "Web
Client Enforcement Violation" OR "Exploit Kit")) OR (blade:Anti-
Virus AND ("URL Reputation" OR "DNS Reputation")))
```

```
Calculated Service > Not equals > smtp
```

Best Practices

Best practices against malicious sites:

- Examine the **Top 15 Hosts** to determine if these hosts are at risk and if you need to clean and reconfigure them.
- Examine the **Top 10 Protection Types** to understand if the websites your internal hosts accessed are compromised.

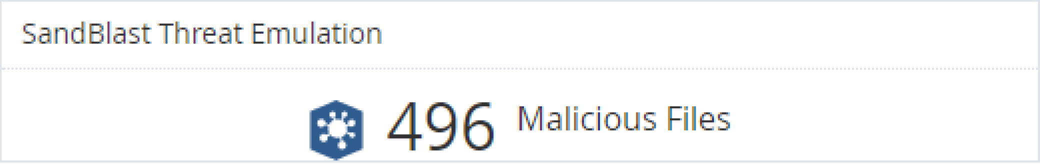
SandBlast Threat Emulation

Description

This widget shows the number of prevented malicious files over the selected report period.

Note - Select the report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

Example:



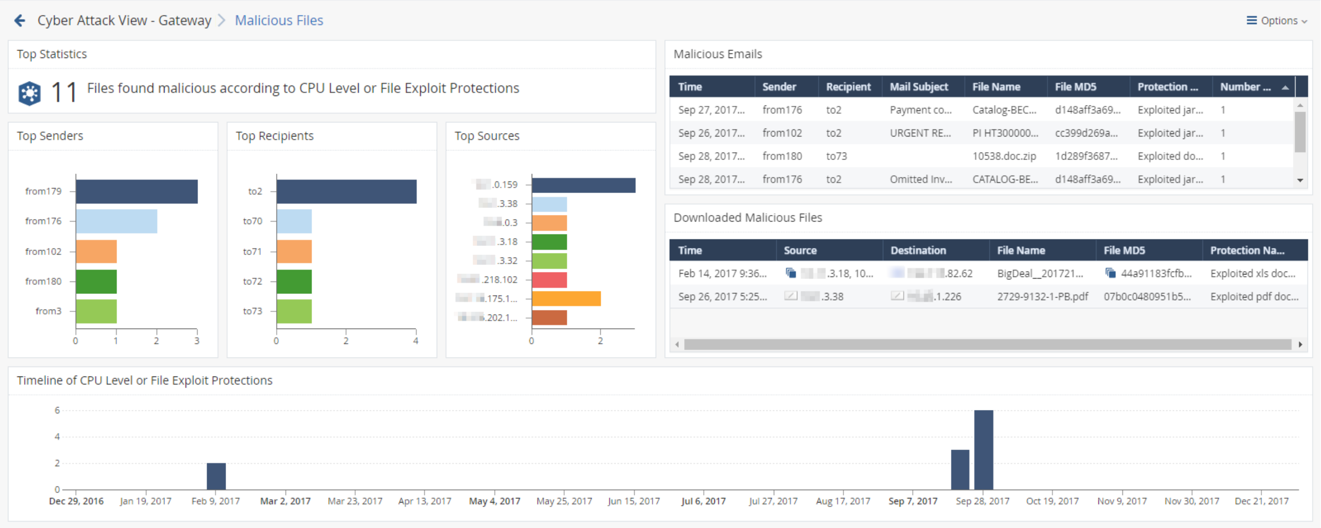
SandBlast Threat Emulation

496 Malicious Files

To open the next drill-down level, double-click a headline or matching icon.

Drill-Down View

This is an obfuscated example of the drill-down view:



Top Statistics

11 Files found malicious according to CPU Level or File Exploit Protections

Malicious Emails

Time	Sender	Recipient	Mail Subject	File Name	File MD5	Protection ...	Number ...
Sep 27, 2017...	from176	to2	Payment co...	Catalog-BEC...	d148aff3a69...	Exploited jar...	1
Sep 26, 2017...	from102	to2	URGENT RE...	PI HT300000...	cc399d269a...	Exploited jar...	1
Sep 28, 2017...	from180	to73		10538.doc.zip	1d289f3687...	Exploited do...	1
Sep 28, 2017...	from176	to2	Omitted Inv...	CATALOG-BE...	d148aff3a69...	Exploited jar...	1

Downloaded Malicious Files

Time	Source	Destination	File Name	File MD5	Protection Na...
Feb 14, 2017 9:36...	[redacted].3.18, 10...	[redacted].82.62	BigDeal__201721...	44a91183fcfb...	Exploited xls doc...
Sep 26, 2017 5:25...	[redacted].3.38	[redacted].1.226	2729-9132-1-PB.pdf	07b0c0480951b5...	Exploited pdf doc...

To see the applicable logs (the next drill-down level), double-click a value.

Available Widgets

Widgets available in the drill-down view:

Widget	Type	Description
Top Statistics	Infographic	Shows the number of files that were found malicious according to CPU Level or File Exploit protections.

Widget	Type	Description
Malicious Emails	Table	Shows the malicious emails. Shows: - Date and Time - Sender email - Recipient email - Email subject - Name of attached file - MD5 of attached file - Protection Name - Number of logged emails
Top Senders	Chart	Shows the senders of the malicious emails. The chart is sorted by the number of logs. Shows: - Who sent the largest number of malicious emails. - The number of the malicious emails these users sent.
Top Recipients	Chart	Shows the recipients of the malicious emails. The chart is sorted by the number of logs. Shows: - Who received the largest number of malicious emails. - The number of the malicious emails these users received.
Top Sources	Chart	Shows the source hosts of the malicious emails. The chart is sorted by the sources that sent the largest number of malicious emails. Shows: - Hosts that sent the largest number of malicious emails. - The number of the malicious emails these hosts sent.

Widget	Type	Description
Downloaded Malicious Files	Table	Shows the information about the detected malicious emails: - From - To - Subject - File Name - File Size - File MD5 - Protection Name
Timeline of CPU Level and File Exploit Protections	Timeline	Shows number of protection logs and their timeline.

Widget Query

In addition to the *"Default Query" on page 438*, the widget runs this query:

```
Custom Filter = "*CPU-Level Detection Event*" OR Exploited
Blade > Equals > Threat Emulation
Product Family > Equals > Threat
```

Cyber Attack Timeline

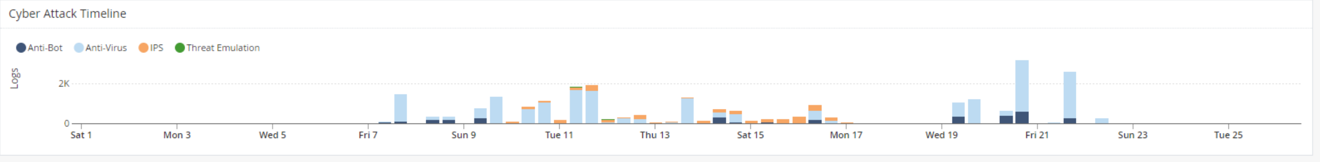
Description

This widget shows the number of logs from different Software Blade (Anti-Bot, Anti-Virus, IPS, and Threat Emulation) over the selected report period.

Note - Select the report period in the top left corner of this view. For example, **Last 7 Days**, **This Month**, and so on.

This information helps you determine if a massive attack has occurred.

Example:



To open the next drill-down level, double-click on a chart bar.

Widget Query

The widget runs the *"Default Query" on page 438*.

MITRE ATT&CK

MITRE ATT&CK is a knowledge base used for the development of threat models and methodologies for the global cybersecurity community.

MITRE ATT&CK lets Check Point customers review the security incidents in their network in a way that exposes the top techniques and tactics used by attackers against their network.

For each malicious file that is found, Threat Emulation (SandBlast technology) adds the techniques and tactics that were used in the attack to the relevant log.

Note - The Threat Emulation blade must be enabled if you want to add MITRE ATT&CK information to the logs.

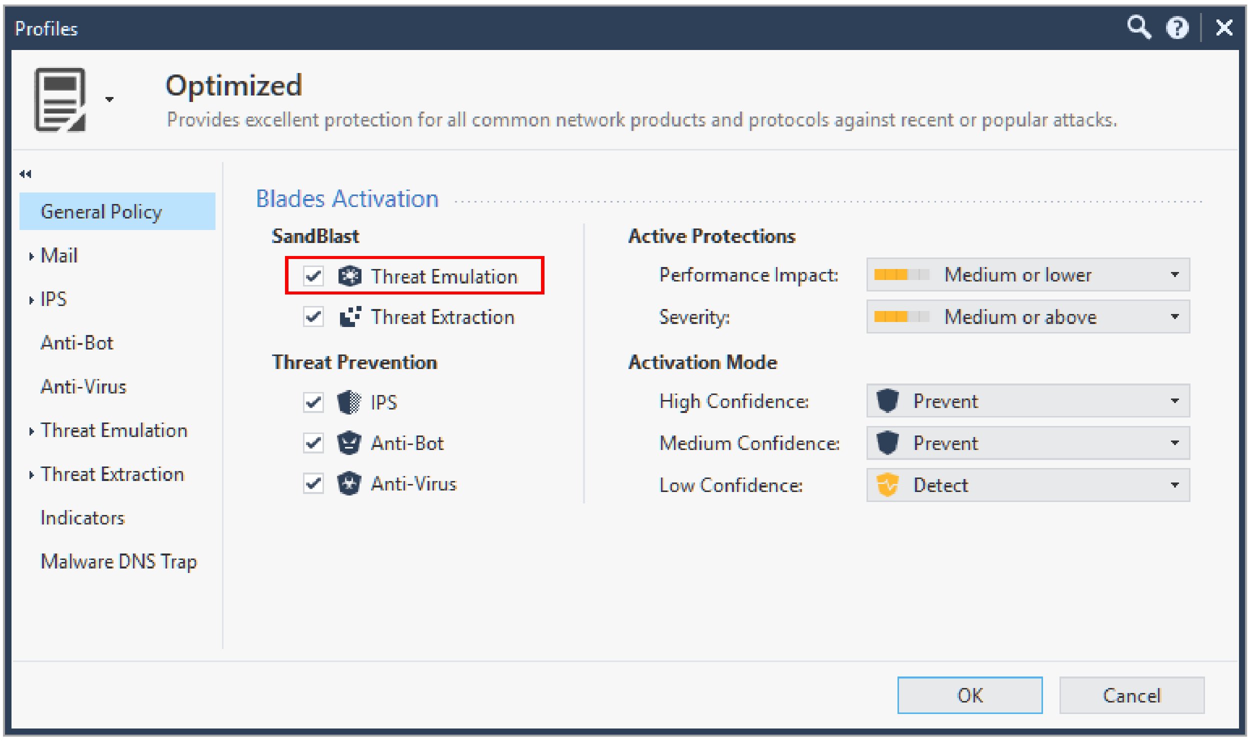
Configuring Threat Emulation Logs with MITRE ATT&CK Data

1. Open SmartConsole.
2. In the **Gateways & Servers** view, enable the **Threat Emulation** blade on the relevant Security Gateway.
3. Select the Security Gateway, click **Actions** > **Open Shell**.
4. Run:

   ```
   tecli advanced engine version
   ```

   The Threat Emulation engine version must be higher than `58.990001056`
5. Open the Threat Prevention profile in use in the Threat Prevention policy (for example

Optimized), and make sure the Threat Emulation blade is activated.



Optimized

Provides excellent protection for all common network products and protocols against recent or popular attacks.

Blades Activation

SandBlast

☑ Threat Emulation

☑ Threat Extraction

Threat Prevention

☑ IPS

☑ Anti-Bot

☑ Anti-Virus

Active Protections

Performance Impact: Medium or lower

Severity: Medium or above

Activation Mode

High Confidence: Prevent

Medium Confidence: Prevent

Low Confidence: Detect

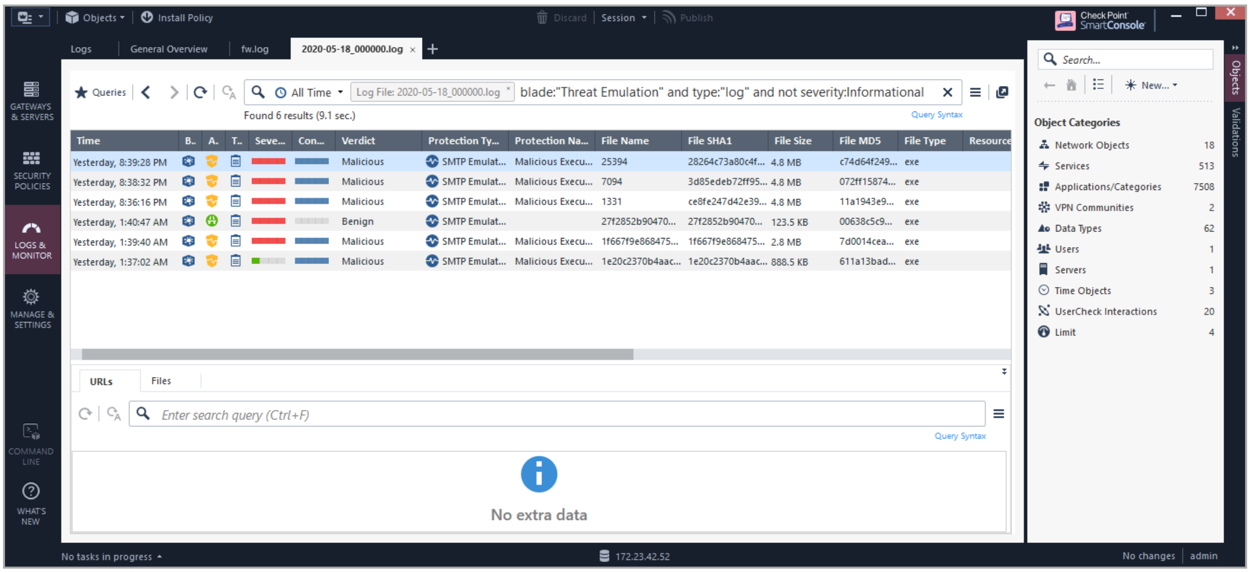
MITRE Logs

To view logs with the added MITRE data:

1. In the **Logs & Monitor** view, open the **Logs** tab.
2. In the search box, enter this query to find malicious files found by Threat Emulation:

```
Blade:"threat Emulation" AND type:"log" AND NOT severity:
"informational"
```

3. Open one of the logs.



Log File: 2020-05-18_000000.log

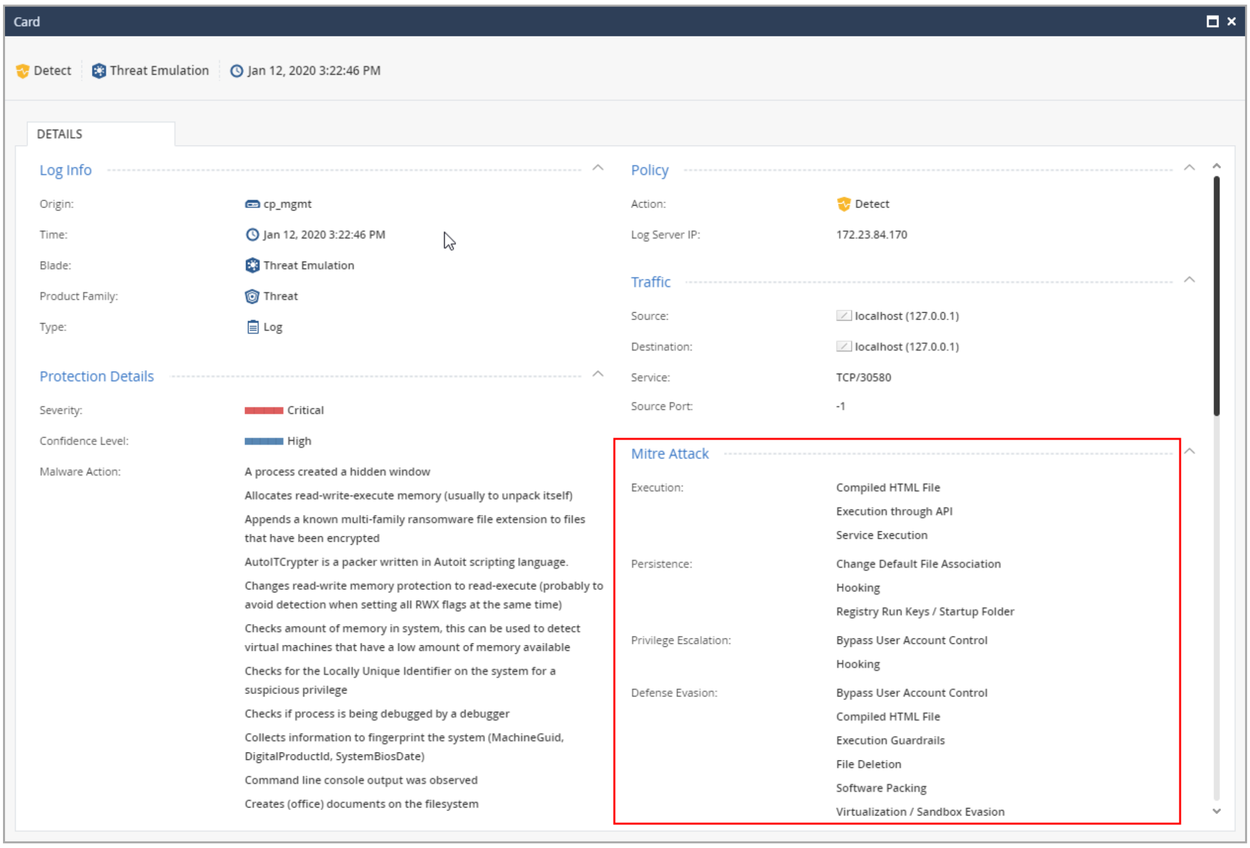
blade:"Threat Emulation" and type:"log" and not severity:Informational

Found 6 results (9.1 sec.)

Time	B..	A.	T..	Seve...	Con...	Verdict	Protection Ty...	Protection Na...	File Name	File SHA1	File Size	File MD5	File Type	Resource
Yesterday, 8:39:28 PM						Malicious	SMTP Emulat...	Malicious Execu...	25394	28264c73a80c4f...	4.8 MB	c74d64f249...	exe	
Yesterday, 8:38:32 PM						Malicious	SMTP Emulat...	Malicious Execu...	7094	3d85edeb72ff95...	4.8 MB	072ff15874...	exe	
Yesterday, 8:36:16 PM						Malicious	SMTP Emulat...	Malicious Execu...	1331	ce8fe247d42e39...	4.8 MB	11a1943e9...	exe	
Yesterday, 1:40:47 AM						Benign	SMTP Emulat...		27f2852b90470...	27f2852b90470...	123.5 KB	00638c5c9...	exe	
Yesterday, 1:39:40 AM						Malicious	SMTP Emulat...	Malicious Execu...	1f667f9e868475...	1f667f9e868475...	2.8 MB	7d0014cea...	exe	
Yesterday, 1:37:02 AM						Malicious	SMTP Emulat...	Malicious Execu...	1e20c2370b4aac...	1e20c2370b4aac...	888.5 KB	611a13bad...	exe	

No extra data

The log shows the MITRE ATT&CK Techniques and Tactics used in the specific attack.



Detect | Threat Emulation | Jan 12, 2020 3:22:46 PM

Log Info

Origin: cp_mgmt
Time: Jan 12, 2020 3:22:46 PM
Blade: Threat Emulation
Product Family: Threat
Type: Log

Protection Details

Severity: Critical
Confidence Level: High
Malware Action: A process created a hidden window
Allocates read-write-execute memory (usually to unpack itself)
Appends a known multi-family ransomware file extension to files that have been encrypted
AutoITCrypter is a packer written in Autoit scripting language.
Changes read-write memory protection to read-execute (probably to avoid detection when setting all RWX flags at the same time)
Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available
Checks for the Locally Unique Identifier on the system for a suspicious privilege
Checks if process is being debugged by a debugger
Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate)
Command line console output was observed
Creates (office) documents on the filesystem

Policy

Action: Detect
Log Server IP: 172.23.84.170

Traffic

Source: localhost (127.0.0.1)
Destination: localhost (127.0.0.1)
Service: TCP/30580
Source Port: -1

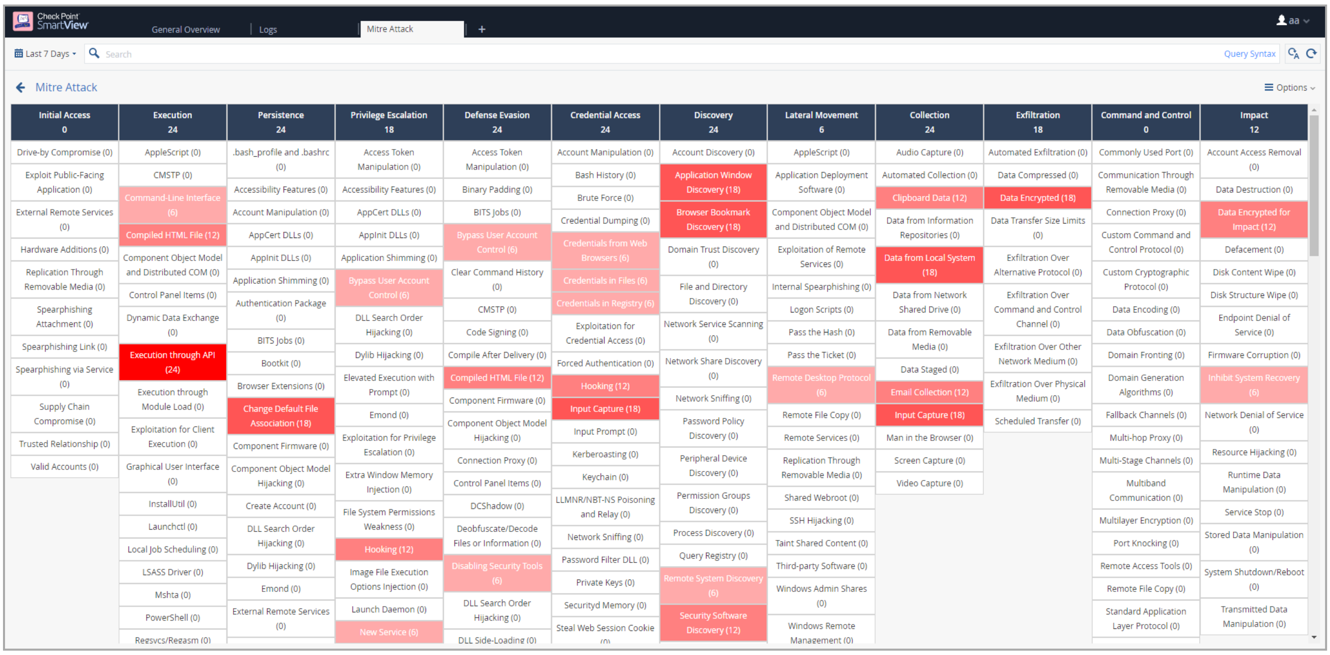
Mitre Attack

Execution: Compiled HTML File
Execution through API
Service Execution
Persistence: Change Default File Association
Hooking
Registry Run Keys / Startup Folder
Privilege Escalation: Bypass User Account Control
Hooking
Defense Evasion: Bypass User Account Control
Compiled HTML File
Execution Guardrails
File Deletion
Software Packing
Virtualization / Sandbox Evasion

The log may show multiple actions such as execution and persistence. For more on each technique as well as mitigation advice, visit the MITRE ATT&CK web site.

MITRE ATT&CK in SmartView

Focusing on malicious files, the **MITRE ATT&CK** view in **Logs & Monitor** gives you a high level overview of the techniques used by attackers against your network.

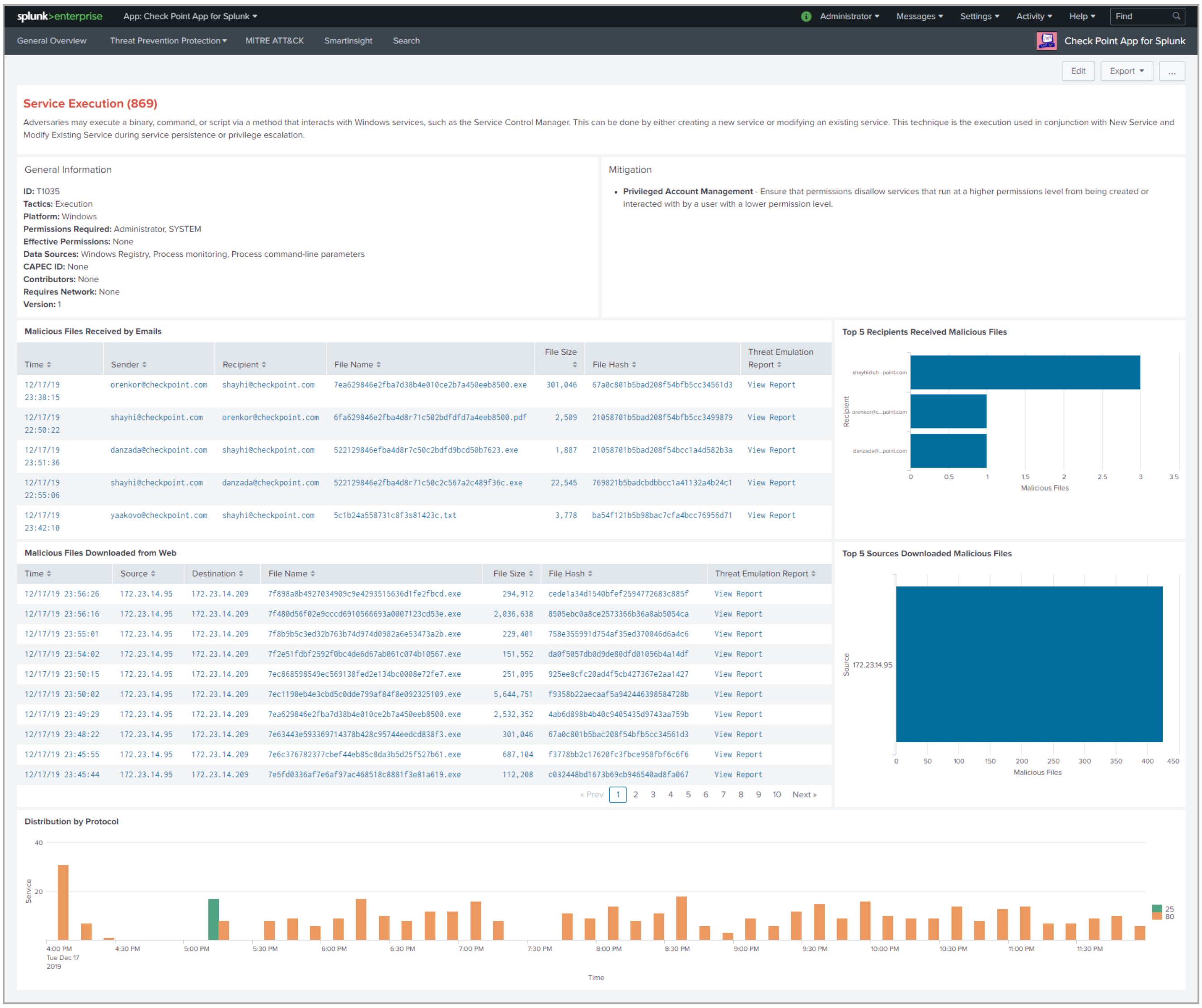


Initial Access 0	Execution 24	Persistence 24	Privilege Escalation 18	Defense Evasion 24	Credential Access 24
Drive-by Compromise (0)	AppleScript (0)	.bash_profile and .bashrc (0)	Access Token Manipulation (0)	Access Token Manipulation (0)	Account Manipulation (0)
Exploit Public-Facing Application (0)	CMSTP (0)	Accessibility Features (0)	Accessibility Features (0)	Binary Padding (0)	Bash History (0)
External Remote Services (0)	Command-Line Interface (6)	Account Manipulation (0)	AppCert DLLs (0)	BITS Jobs (0)	Brute Force (0)
Hardware Additions (0)	Compiled HTML File (12)	AppCert DLLs (0)	AppInit DLLs (0)	Bypass User Account Control (6)	Credential Dumping (0)
Replication Through Removable Media (0)	Component Object Model and Distributed COM (0)	AppInit DLLs (0)	Application Shimming (0)	Clear Command History (0)	Credentials from Web Browsers (6)
Spearphishing Attachment (0)	Control Panel Items (0)	Application Shimming (0)	Bypass User Account Control (6)	CMSTP (0)	Credentials in Files (6)
Spearphishing Link (0)	Dynamic Data Exchange (0)	Authentication Package (0)	DLL Search Order Hijacking (0)	Code Signing (0)	Credentials in Registry (6)
Spearphishing via Service (0)	Execution through API (24)	BITS Jobs (0)	Dylib Hijacking (0)	Compile After Delivery (0)	Exploitation for Credential Access (0)
Supply Chain Compromise (0)	Execution through Module Load (0)	Bootkit (0)	Elevated Execution with Prompt (0)	Compiled HTML File (12)	Forced Authentication (0)
Trusted Relationship (0)	Exploitation for Client Execution (0)	Browser Extensions (0)	Emond (0)	Component Firmware (0)	Hooking (12)
Valid Accounts (0)	Graphical User Interface (0)	Change Default File Association (18)	Exploitation for Privilege Escalation (0)	Component Object Model Hijacking (0)	Input Capture (18)
	InstallUtil (0)	Component Firmware (0)	Extra Window Memory Injection (0)	Connection Proxy (0)	Input Prompt (0)
	Launchctl (0)	Component Object Model Hijacking (0)	File System Permissions Weakness (0)	Control Panel Items (0)	Kerberoasting (0)
	Local Job Scheduling (0)	Create Account (0)	Hooking (12)	DCShadow (0)	Keychain (0)
	LSASS Driver (0)	DLL Search Order Hijacking (0)	Image File Execution Options Injection (0)	Deobfuscate/Decode Files or Information (0)	LLMNR/NBT-NS Poisoning and Relay (0)
	Mshta (0)	Dylib Hijacking (0)	Launch Daemon (0)	Disabling Security Tools (6)	Network Sniffing (0)
	PowerShell (0)	Emond (0)	New Service (6)	DLL Search Order Hijacking (0)	Password Filter DLL (0)
	Regsvcs/Regasm (0)	External Remote Services (0)		DLL Side-Loading (0)	Private Keys (0)
					Securityd Memory (0)
					Steal Web Session Cookie (0)

Discovery 24	Lateral Movement 6	Collection 24	Exfiltration 18	Command and Control 0	Impact 12
Account Discovery (0)	AppleScript (0)	Audio Capture (0)	Automated Exfiltration (0)	Commonly Used Port (0)	Account Access Removal (0)
Application Window Discovery (18)	Application Deployment Software (0)	Automated Collection (0)	Data Compressed (0)	Communication Through Removable Media (0)	Data Destruction (0)
Browser Bookmark Discovery (18)	Component Object Model and Distributed COM (0)	Clipboard Data (12)	Data Encrypted (18)	Connection Proxy (0)	Data Encrypted for Impact (12)
Domain Trust Discovery (0)	Exploitation of Remote Services (0)	Data from Information Repositories (0)	Data Transfer Size Limits (0)	Custom Command and Control Protocol (0)	Defacement (0)
File and Directory Discovery (0)	Internal Spearphishing (0)	Data from Local System (18)	Exfiltration Over Alternative Protocol (0)	Custom Cryptographic Protocol (0)	Disk Content Wipe (0)
Network Service Scanning (0)	Logon Scripts (0)	Data from Network Shared Drive (0)	Exfiltration Over Command and Control Channel (0)	Data Encoding (0)	Disk Structure Wipe (0)
Network Share Discovery (0)	Pass the Hash (0)	Data from Removable Media (0)	Exfiltration Over Other Network Medium (0)	Data Obfuscation (0)	Endpoint Denial of Service (0)
Network Sniffing (0)	Pass the Ticket (0)	Data Staged (0)	Exfiltration Over Physical Medium (0)	Domain Fronting (0)	Firmware Corruption (0)
Password Policy Discovery (0)	Remote Desktop Protocol (6)	Email Collection (12)	Scheduled Transfer (0)	Domain Generation Algorithms (0)	Inhibit System Recovery (6)
Peripheral Device Discovery (0)	Remote File Copy (0)	Input Capture (18)		Fallback Channels (0)	Network Denial of Service (0)
Permission Groups Discovery (0)	Remote Services (0)	Man in the Browser (0)		Multi-hop Proxy (0)	Resource Hijacking (0)
Process Discovery (0)	Replication Through Removable Media (0)	Screen Capture (0)		Multi-Stage Channels (0)	Runtime Data Manipulation (0)
Query Registry (0)	Shared Webroot (0)	Video Capture (0)		Multiband Communication (0)	Service Stop (0)
Remote System Discovery (6)	SSH Hijacking (0)			Multilayer Encryption (0)	Stored Data Manipulation (0)
Security Software Discovery (12)	Taint Shared Content (0)			Port Knocking (0)	System Shutdown/Reboot (0)
	Third-party Software (0)			Remote Access Tools (0)	Transmitted Data Manipulation (0)
	Windows Admin Shares (0)			Remote File Copy (0)	
	Windows Remote Management (0)			Standard Application Layer Protocol (0)	

1. Review the top techniques that were used.
2. Double click on one of them.
3. Use the sub-views identity the target of the attack and the attack vector.

Example:



Service Execution (869)

Adversaries may execute a binary, command, or script via a method that interacts with Windows services, such as the Service Control Manager. This can be done by either creating a new service or modifying an existing service. This technique is the execution used in conjunction with New Service and Modify Existing Service during service persistence or privilege escalation.

General Information

ID: T1035
Tactics: Execution
Platform: Windows
Permissions Required: Administrator, SYSTEM
Effective Permissions: None
Data Sources: Windows Registry, Process monitoring, Process command-line parameters
CAPEC ID: None
Contributors: None
Requires Network: None
Version: 1

Mitigation

- **Privileged Account Management** - Ensure that permissions disallow services that run at a higher permissions level from being created or interacted with by a user with a lower permission level.

Malicious Files Received by Emails

Time	Sender	Recipient	File Name	File Size	File Hash	Threat Emulation Report
12/17/19 23:38:15	orenkor@checkpoint.com	shayhi@checkpoint.com	7ea629846e2fba7d38b4e010ce2b7a450eeb8500.exe	301,046	67a0c801b5bad208f54bfb5cc34561d3	View Report
12/17/19 22:50:22	shayhi@checkpoint.com	orenkor@checkpoint.com	6fa629846e2fba4d8r71c502bdfdfd7a4eeb8500.pdf	2,509	21058701b5bad208f54bfb5cc3499879	View Report
12/17/19 23:51:36	danzada@checkpoint.com	shayhi@checkpoint.com	522129846efba4d8r7c50c2bdfd9bcd50b7623.exe	1,887	21058701b5bad208f54bcc1a4d582b3a	View Report
12/17/19 22:55:06	shayhi@checkpoint.com	danzada@checkpoint.com	522129846e2fba4d8r71c50c2c567a2c489f36c.exe	22,545	769821b5badcbdbbcc1a41132a4b24c1	View Report
12/17/19 23:42:10	yaakovo@checkpoint.com	shayhi@checkpoint.com	5c1b24a558731c8f3s81423c.txt	3,778	ba54f121b5b98bac7cfa4bcc76956d71	View Report

Top 5 Recipients Received Malicious Files

Malicious Files Downloaded from Web

Time	Source	Destination	File Name	File Size	File Hash	Threat Emulation Report
12/17/19 23:56:26	172.23.14.95	172.23.14.209	7f898a8b4927034909c9e4293515636d1fe2fbcd.exe	294,912	cede1a34d1540bfef2594772683c885f	View Report
12/17/19 23:56:16	172.23.14.95	172.23.14.209	7f480d56f02e9cccd6910566693a0007123cd53e.exe	2,036,638	8505ebc0a8ce2573366b36a8ab5054ca	View Report
12/17/19 23:55:01	172.23.14.95	172.23.14.209	7f8b9b5c3ed32b763b74d974d0982a6e53473a2b.exe	229,401	758e355991d754af35ed370046d6a4c6	View Report
12/17/19 23:54:02	172.23.14.95	172.23.14.209	7f2e51fdbf2592f0bc4de6d67ab061c074b10567.exe	151,552	da0f5057db0d9de80dfd01056b4a14df	View Report
12/17/19 23:50:15	172.23.14.95	172.23.14.209	7ec868598549ec569138fed2e134bc0008e72fe7.exe	251,095	925ee8cfc20ad4f5cb427367e2aa1427	View Report
12/17/19 23:50:02	172.23.14.95	172.23.14.209	7ec1190eb4e3cbd5c0dde799af84f8e092325109.exe	5,644,751	f9358b22aecaaf5a942446398584728b	View Report
12/17/19 23:49:29	172.23.14.95	172.23.14.209	7ea629846e2fba7d38b4e010ce2b7a450eeb8500.exe	2,532,352	4ab6d898b4b40c9405435d9743aa759b	View Report
12/17/19 23:48:22	172.23.14.95	172.23.14.209	7e63443e593369714378b428c95744eedcd838f3.exe	301,046	67a0c801b5bac208f54bfb5cc34561d3	View Report
12/17/19 23:45:55	172.23.14.95	172.23.14.209	7e6c376782377cbef44eb85c8da3b5d25f527b61.exe	687,104	f3778bb2c17620fc3fbce958fbf6c6f6	View Report
12/17/19 23:45:44	172.23.14.95	172.23.14.209	7e5fd0336af7e6af97ac468518c8881f3e81a619.exe	112,208	c032448bd1673b69cb946540ad8fa067	View Report

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

Top 5 Sources Downloaded Malicious Files

Distribution by Protocol

Note - The **MITRE ATT&CK** view is only available in R81 and higher.

MITRE ATT&CK Best Practices

Adding MITRE ATT&CK data to your logs lets you:

- **Understand your unique attack landscape**

  Focus on the top techniques used by your attackers. By gaining a high level view of your attackers intent, you can identity attack trends against your network.

  Use MITRE ATT&CK to verify that your Threat Prevention policy is protecting your network against all types of tactics and techniques.

  For additional information about the Check Point coverage of the MITRE ATT&CK, see Enterprise matrix.

- **Take action according to your attacker's intent**

  Review the mitigation options offered by MITRE. These mitigation options are related to the specific type of attack launched against your network.

Log Fields

Field Display Name	Check Point Field Name	Description	Output Example
`Action`	`action`	Response to attack, as defined by policy.	`prevent`
`Action Details`	`action_details`	Description of the detected malicious action.	`Communicating with a Command and control server`
`Analyzed On`	`analyzed_on`	Where the detected resource was analyzed.	`"Check Point Threat Emulation Cloud";`
`App Package`	`app_package`	Unique identifier of the application on the protected mobile device.	`com.facebook.katana`
`Application Name`	`appi_name`	Name of the application downloaded on the protected mobile device.	`Free Music MP3 Player`
`Application Repackaged`	`app_repackaged`	Indicates whether the original application was repackage not by the official developer.	`TRUE`
`Application Signature ID`	`app_sig_id`	Unique SHA identifier of a mobile application.	`b6511332331bc8bc64e8bdb1cd915592b29f4606`

Field Display Name	Check Point Field Name	Description	Output Example
Application Version	app_version	Version of the application downloaded on the protected mobile device.	1.3
Attack Information	attack_info	Description of the vulnerability in case of a host or network vulnerability.	Linux EternalRed Samba Remote Code Execution
Attack Name	attack	Name of the vulnerability category in case of a host or network vulnerability.	Windows SMB Protection Violation
Attack Status	attack_status	In case of a malicious event on an endpoint computer, the status of the attack.	Active
Attacker Phone Number	attacker_ phone_number	In case of a malicious SMS, shows the phone number of the sender of the malicious link inside the SMS.	15712244010
BCC	bcc	The Blind Carbon Copy address of the email.	mail@example.com
Blade	product	Name of the Software Blade.	Anti-Bot

Field Display Name	Check Point Field Name	Description	Output Example
BSSID	bssid	The unique MAC address of the Wi-Fi network related to the Wi-Fi attack against a mobile device.	98:FC:11:B9:24:12
Bytes (sent\received)	Aggregation of: sent_bytes received_bytes	Amount of bytes that was sent and received in the attack.	24 B \ 118 B
CC	cc	The Carbon Copy address of the email.	mail@example.com
Certificate Name	certificate_name	The Common Name that identifies the host name associated with the certificate.	Piso-Nuevo
Client Name	client_name	Client Application or Software Blade that detected the event.	Check Point Endpoint Security Client
Confidence Level	confidence_level	Detection confidence based on Check Point ThreatCloud.	Medium
Content Risk	content_risk	The risk of the extracted content from a document.	4 - high

Field Display Name	Check Point Field Name	Description	Output Example
Dashboard Event ID	dashboard_event_id	Unique ID for the event in the Cloud Dashboard .	1729
Dashboard Origin	dashboard_orig	Name of the Cloud Mobile Dashboard.	SBM Cloud management
Dashboard Time	dashboard_time	Cloud Mobile Dashboard time when the log was created.	7th july 2018 22:27
Description	description	Additional information about detected attack, *or* the error related to the connection.	Check Point Online Web Service failure. See sk74040 for more information.
Destination	dst	Attack destination IP address.	192.168.22.2
Determined By	te_verdict_determined_by	Emulators that determined the file is malicious.	Win7 64b,Office 2010,Adobe 11: local cache. Win7,Office 2013,Adobe 11: local cache.
Developer Certificate Name	developer_certificate_name	Name of the developer's certificate that was used to sign the mobile application.	iPhone Developer (6MZTQJDTZ)

Field Display Name	Check Point Field Name	Description	Output Example
Developer Certificate Sha	developer_certificate_sha	Certificate SHA of the developer's certificate that was used to sign the mobile application.	Sha1
Device ID	device_identification	Unique ID of the mobile device.	2739
Direction	interfacedir	Connection direction.	'inbound'; 'outbound'
Email Recipients Number	email_recipients_num	The number of recipients, who received the same email.	6
Email Subject	email_subject	The subject of the email that was inspected by Check Point.	invoice #43662
Extension Version	extension_version	Build version of the SandBlast Agent browser extension.	SandBlast Extension 990.45.6
Extracted File Hash	extracted_file_hash	In case of an archive file, the list of hashes of archived files.	8e3951897bf8371e6010e3254b99e86d
Extracted File Names	extracted_file_names	In case of an archive file, the list of archived file names.	malicious.js
Extracted File Types	extracted_file_types	In case of an archive file, the archived file types.	js

Field Display Name	Check Point Field Name	Description	Output Example
`Extracted File Verdict`	`extracted_file_verdict`	In case of an archive file, the verdict for internal files.	`malicious`
`File Direction`	`file_direction`	In case of a malicious file that was found by Anti-Virus, the direction of the connection: ■ Incoming - for download ■ Outgoing - for upload	`Incoming`
`File MD5`	`file_md5`	MD5 hash of the detected file.	`8e3951897bf8371e6010e3254b99e86d`
`File Name`	`file_name`	Name of the detected file.	`malicious.exe`
`File SHA1`	`file_sha1`	SHA1 hash of the detected file.	`4d48c297e2cd81b1ee786a71fc1a3def178619aa`
`File SHA256`	`file_sha256`	SHA256 hash of the detected file.	`110d6ae802d229a8105f3185525b5ce2cf9e151f2462bf407db6e832ccac56fa`
`File Size`	`file_size`	Size (in bytes) of the detected file.	`8.4KB`

Field Display Name	Check Point Field Name	Description	Output Example
File Type+A23	file_type	Extension of the detected file.	wsf
First Detection	first_detection	Time of the first detection of the infection.	1th january 2018
Geographic Location	calc_geo_location	In case of a malicious activity on the mobile device, the location of the mobile device (in the format: Longitude, Latitude).	32.0686513, 34.7945463
Hardware Model	hardware_model	Mobile device hardware model.	Samsung A900
Host Time	host_time	Local time on the endpoint computer.	7th july 2018 22:27
Host Type	host_type	Type of the source endpoint computer.	Desktop
Impacted Files	impacted_files	In case of an infection on an endpoint computer, the list of files that the malware impacted.	privatedoc.txt; image.png
Industry Reference	industry_reference	Link to the related MITRE vulnerability documentation.	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0148

Field Display Name	Check Point Field Name	Description	Output Example
Installed Blades	installed_products	List of installed Endpoint Software Blade.	Anti-Ransomware, Anti-Exploit, Anti-Bot
Interface	interfaceName	The name of the Security Gateway, through which a connection traverses.	eth1
Jailbreak Information	jailbreak_message	Indicates whether the integrity of the mobile device OS is violated: ■ True - The OS is Jailbroken or Rooted. ■ False - The OS is intact.	TRUE
Last Detection	last_detection	Time of the last detection of the infection.	2th january 2018
Malware Action	malware_action	Description of the detected malware activity.	'DNS query for a site known to be malicious';
Malware Family	malware_family	Name of the malware related to the malicious IOC.	Locky
MDM ID	mdm_id	Mobile Device ID on the MDM system.	4718

Field Display Name	Check Point Field Name	Description	Output Example
Network Certificate	network_ certificate	Public key of the certificate that was used for SSL interception.	example.com
Not Vulnerable OS	emulated_on	Emulators that did not found the file malicious.	Win7 64b,Office 2010,Adobe 11
Origin	orig	Name of the first Security Gateway that reported this event.	My_GW
OS Name	os_name	Name of the OS installed on the source endpoint computer.	Windows 7 Professional N Edition
OS Version	os_version	Build version of the OS installed on the source endpoint computer.	6.1-7601-SP1.0-SMP
Packet Capture	packet_ capture	Link to the PCAP traffic capture file with the recorded malicious connection.	
Parent Process MD5	parent_ process_md5	MD5 hash of the parent process of the process that triggered the attack.	d41d8cd98 f00b204e9 800998ecf 8427e

Field Display Name	Check Point Field Name	Description	Output Example
Parent Process Name	parent_process_name	Name of the parent process of the process that triggered the attack.	cmd.exe
Parent Process Username	parent_process_username	Owner username of the parent process of the process that triggered the attack.	johndoe
Performance Impact	performance_impact	IPS Signature performance impact on the Security Gateway.	Medium
Phone Number	phone_number	The phone number of the mobile device.	15712244010
Policy	policy_date	Date of the last policy fetch.	1th january 2018
Policy Management	policy_mgmt	Name of the Management Server that manages this Security Gateway.	My_MGMT_server
Policy Name	policy_name	Name of the last policy that this Security Gateway fetched.	My_Perimeter
Process MD5	process_md5	MD5 hash of the process that triggered the attack.	d41d8cd98f00b204e9800998ecf8427e

Field Display Name	Check Point Field Name	Description	Output Example
Process Name	process_name	Name of the process that triggered the attack.	bot.exe
Process Username	process_ username	Owner username of the process that triggered the attack.	johndoe
Product Family	product_ family	Name of the Software Blade family.	Threat
Product Version	client_ version	Build version of SandBlast Agent client installed on the computer.	80.85.7076
Protection Name	protection_ name	Specific name of the attack signature.	'Exploited doc document'
Protection Type	protection_ type	Type of the protection used to detect the attack.	SMTP Emulation
Reason	reason	The reason for detecting or stopping the attack.	Internal error occurred, could not connect to cws.checkpoint.com:80". Check proxy configuration on the gateway."
Recipient	to	Destination email address.	recipient@example.com

Field Display Name	Check Point Field Name	Description	Output Example
Remediated Files	remediated_files	In case of an infection and a successful cleaning of that infection, this is a list of remediated files on the computer.	malicious.exe, dropper.exe
Resource	resource	URL, Domain, or DNS of the malicious request.	www[.]maliciousdomain[.]xyz
Risk	file_risk	Shows the risk rate, in case the Threat Extraction Software Blade found a suspicious content.	4
Scope	scope	Protected scope defined in the rule.	192.168.1.3
Sender	from	Source email address.	sender@example.com
Service	service_name	Protocol and destination port.	http [tcp/80]
Severity	severity	Incident severity level based on Check Point ThreatCloud.	High
Source	src	Attack source IP address.	91.2.22.28

Field Display Name	Check Point Field Name	Description	Output Example
Source IP-phone	src_phone_number	The phone number of the source mobile device.	15712244010
Source Port	s_port	Source port of the connection.	35125
SSID	ssid	The name of the Wi-Fi network, in case a suspicious or malicious event was found in SandBlast Mobile.	Airport_Free_Wifi
Subject	subject	The subject of the email that was inspected by Check Point.	invoice #43662
Suppressed logs	suppressed_logs	Shows the number of malicious connection attempts in a burst. Burst - A series of repeated connection attempts within a very short time period. The attempted connections must all have the same: ■ Source ■ Destination ■ Protocol	72

Field Display Name	Check Point Field Name	Description	Output Example
Suspicious Content	scrubbed_ content	Shows the content that Threat Extraction Software Blade removed.	Embedded Objects:
System App	system_app	Indicates whether the detected app is installed in the device ROM.	False
Threat Extraction Activity	scrub_ activity	Description of the risky active content that the Security Gateway found and cleaned.	Active content was found - DOCX file was converted to PDF
Threat Profile	smartdefense_ profile	Name of the IPS profile, if it is managed separately from other Threat Prevention Software Blade.	Recommended_IPS_ internal
Time	time	The time stamp when the log was created.	7th july 2018 22:27
Total Attachments	total_ attachments	The number of attachments in an email.	3
Triggered By	triggered_by	The name of the mechanism that triggered the Software Blade to enforce a protection.	SandBlast Anti-Ransomware

Field Display Name	Check Point Field Name	Description	Output Example
Trusted Domain	trusted_domain	In case of phishing event, the domain, which the attacker was impersonating.	www.checkpoint.com
Type	type	Log type.	log
Vendor List	vendor_list	The vendor name that provided the verdict for a malicious URL.	Check Point ThreatCloud
Verdict	verdict	Verdict of the malicious activity/File.	Malicious
Vulnerable OS	detected_on	Emulators that found the file malicious.	Win7 Office 2013 Adobe 11 WinXP Office 2003/7 Adobe 9

Command Line Reference

See the *R81.20 CLI Reference Guide*.

Working with Kernel Parameters

See the *R81.20 Quantum Security Gateway Guide* > Chapter "Working with Kernel Parameters".

Kernel Debug

See the *R81.20 Quantum Security Gateway Guide* > Chapter "Kernel Debug on Security Gateway".

Glossary

A

Anti-Bot

Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam

Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus

Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

Application Control

Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

Ask

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

Audit Log

Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

B

Bot

Malicious software that neutralizes Anti-Virus defenses, connects to a Command and Control center for instructions from cyber criminals, and carries out the instructions.

Bridge Mode

Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

Cluster

Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member

Security Gateway that is part of a cluster.

Compliance

Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

Content Awareness

Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. Acronym: CTNT.

CoreXL

Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance

On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

CoreXL SND

Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE

Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself.

D

DAIP Gateway

Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

Data Loss Prevention

Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

Data Type

Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

Detect

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

Distributed Deployment

Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

Dynamic Object

Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

E

Endpoint Policy Management

Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

Expert Mode

The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

G

Gaia

Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish

The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

Gaia Portal

Web interface for the Check Point Gaia operating system.

H

Hotfix

Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

HTTPS Inspection

Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

I

ICA

Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

ICAP Client

The ICAP Client functionality in your Security Gateway or Cluster (in versions R80.40 and higher) enables it to interact with an ICAP Server responses (see RFC 3507), modify their content, and block the matched HTTP connections.

ICAP Server

The ICAP Server functionality in your Security Gateway or Cluster (in versions R80.40 and higher) enables it to interact with an ICAP Client requests, send the files for inspection, and return the verdict.

Identity Awareness

Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

Identity Logging

Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

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.

Internal Network

Computers and resources protected by the Firewall and accessed by authenticated users.

IoC

Indicator of Compromise. Artifact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion. Typical IoCs are virus signatures and IP addresses, MD5 hashes of Malware files, or URLs or domain names of botnet command and control servers. Identified through a process of incident response and computer forensics, intrusion detection systems and anti-virus software can use IoC's to detect future attacks.

IPS

Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN

Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

J

Jumbo Hotfix Accumulator

Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

K

Kerberos

An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

L

Log Server

Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status

Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

M

Mail Transfer Agent

Feature on a Security Gateway that intercepts SMTP traffic and forwards it to the applicable inspection component. Acronym: MTA.

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.

Management Interface

(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

Management Server

Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

Manual NAT Rules

Manual configuration of NAT rules by the administrator of the Check Point Management Server.

Mirror and Decrypt

The Mirror and Decrypt feature on a Security Gateway or Cluster (in versions R80.40 and higher) that performs these actions: (1) Mirror only of all traffic - Clones all traffic (including HTTPS without decryption) that passes through, and sends it out of the designated physical interface. (2) Mirror and Decrypt of HTTPS traffic - Clones all HTTPS traffic that passes through, decrypts it, and sends it in clear-text out of the designated physical interface. Acronym: M&D.

Mobile Access

Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

Multi-Domain Log Server

Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Server

Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

N

Network Object

Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

Network Policy Management

Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

O

Observable

Event or stateful property that can be observed in an operational cyber domain.

Open Server

Physical computer manufactured and distributed by a company, other than Check Point.

P

Prevent

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

Provisioning

Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

Q

QoS

Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

R

Rule

Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

Rule Base

All rules configured in a given Security Policy. Synonym: Rulebase.

S

SecureXL

Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

Security Gateway

Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Management Server

Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

Security Policy

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

SIC

Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

SmartConsole

Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

SmartDashboard

Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

SmartProvisioning

Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

SmartUpdate

Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

Software Blade

Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

Standalone

Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

STIX

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

T

Threat Emulation

Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Emulation Private Cloud Appliance

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

Threat Extraction
Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

ThreatCloud
The cyber intelligence center of all of Check Point products. Dynamically updated based on an innovative global network of threat sensors and invites organizations to share threat data and collaborate in the fight against modern malware.

ThreatCloud Repository
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. See: https://www.checkpoint.com/infinity-vision/threatcloud/

ThreatSpect Engine
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.

U

Updatable Object
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

URL Filtering
Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Directory
Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

UserCheck
Functionality in your Security Gateway or Cluster and endpoint clients that 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.

V

VSX

Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway

Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Z

Zero Phishing

Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.