Important Information

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

Latest Documentation
The latest version of this document is at: http://supportcontent.checkpoint.com/documentation_download?ID=22907

For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

For more about this release, see the R76 home page (http://supportcontent.checkpoint.com/solutions?id=sk91140).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 February 2013</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

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

Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Anti-Bot and Anti-Virus R76 Administration Guide).
Contents

Important Information.................................................................3
Introduction to Anti-Bot and Anti-Virus ........................................7
  The Need for Anti-Bot .............................................................7
  The Need for Anti-Virus ..........................................................7
  The Check Point Anti-Bot and Anti-Virus Solution .......................8
    Identifying Bot Infected Computers .......................................8
    Preventing Bot Damage ......................................................9
    Analyzing Threats ................................................................9
Getting Started with Anti-Bot and Anti-Virus ................................10
  Anti-Bot and Anti-Virus Licensing and Contracts .......................10
  SmartDashboard Toolbar .........................................................10
  Enabling the Anti-Bot and Anti-Virus Software Blades ...............11
    Check Point Information ......................................................11
  Creating an Anti-Bot and Anti-Virus Policy ................................12
    Creating Rules ................................................................12
    Installing the Policy ............................................................14
Managing Anti-Bot and Anti-Virus ................................................15
  The Anti-Bot and Anti-Virus Overview Pane ..............................15
    My Organization ................................................................15
    Messages and Action Items .................................................15
    Statistics ............................................................................15
    Malware Activity ...............................................................16
    RSS Feeds .........................................................................16
  The ThreatCloud Repository ....................................................16
    Using the Threat Wiki ...........................................................17
    Updating the Malware Database ............................................17
  Gateways Pane ......................................................................18
  Protections Browser ................................................................18
    Searching Protections .........................................................19
    Sorting Protections .............................................................19
  Profiles Pane ..........................................................................19
    Creating Profiles ...............................................................20
    Copying Profiles ................................................................22
    Deleting Profiles ................................................................22
  The Policy Rule Base ...............................................................23
    Predefined Rule ................................................................23
    Exception Rules ................................................................23
    Parts of the Rules ................................................................24
  Exception Groups Pane ............................................................26
    Creating Exception Groups ..................................................27
    Adding Exceptions to Exception Groups .................................27
    Adding Exception Groups to the Rule Base ............................27
    Creating Exceptions from Logs or Events ...............................27
Advanced Settings for Anti-Bot and Anti-Virus ...............................28
  Engine Settings .....................................................................28
  Managing Traditional Anti-Virus ..............................................29
    Enabling Traditional Anti-Virus ............................................29
    Database Updates ................................................................30
    Understanding Traditional Anti-Virus Scanning Options ..........30
    Configuring Traditional Anti-Virus .........................................35
    Logging and Monitoring .......................................................38
    UTM-1 Edge Traditional Anti-Virus ........................................38
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Inspection on Non-Standard Ports</td>
<td>38</td>
</tr>
<tr>
<td>HTTPS Inspection</td>
<td>39</td>
</tr>
<tr>
<td>How it Operates</td>
<td>39</td>
</tr>
<tr>
<td>Configuring Outbound HTTPS Inspection</td>
<td>40</td>
</tr>
<tr>
<td>Configuring Inbound HTTPS Inspection</td>
<td>42</td>
</tr>
<tr>
<td>The HTTPS Inspection Policy</td>
<td>43</td>
</tr>
<tr>
<td>Gateways Pane</td>
<td>47</td>
</tr>
<tr>
<td>Adding Trusted CAs for Outbound HTTPS Inspection</td>
<td>47</td>
</tr>
<tr>
<td>HTTPS Validation</td>
<td>48</td>
</tr>
<tr>
<td>HTTP/HTTPS Proxy</td>
<td>50</td>
</tr>
<tr>
<td>Security Gateway Portals</td>
<td>51</td>
</tr>
<tr>
<td>HTTPS Inspection in SmartView Tracker</td>
<td>52</td>
</tr>
<tr>
<td>HTTPS Inspection in SmartEvent</td>
<td>53</td>
</tr>
<tr>
<td>Anti-Bot and Anti-Virus in SmartView Tracker</td>
<td>55</td>
</tr>
<tr>
<td>Log Sessions</td>
<td>55</td>
</tr>
<tr>
<td>Anti-Bot and Anti-Virus Logs</td>
<td>56</td>
</tr>
<tr>
<td>Viewing Logs</td>
<td>56</td>
</tr>
<tr>
<td>Updating the Anti-Bot and Anti-Virus Rule Base</td>
<td>56</td>
</tr>
<tr>
<td>Accessing the Threat Wiki</td>
<td>56</td>
</tr>
<tr>
<td>Viewing Packet Capture Data</td>
<td>57</td>
</tr>
<tr>
<td>Using Predefined Queries</td>
<td>57</td>
</tr>
<tr>
<td>Anti-Bot and Anti-Virus in SmartEvent</td>
<td>58</td>
</tr>
<tr>
<td>Event Analysis in SmartEvent or SmartEvent Intro</td>
<td>58</td>
</tr>
<tr>
<td>Viewing Information in SmartEvent</td>
<td>58</td>
</tr>
<tr>
<td>Updating the Anti-Bot and Anti-Virus Rule Base</td>
<td>59</td>
</tr>
<tr>
<td>Accessing the Threat Wiki</td>
<td>59</td>
</tr>
<tr>
<td>Anti-Bot and Anti-Virus Reports</td>
<td>60</td>
</tr>
<tr>
<td>Viewing Information in SmartEvent Intro</td>
<td>60</td>
</tr>
<tr>
<td>The SmartEvent Intro Overview Page</td>
<td>60</td>
</tr>
<tr>
<td>Anti-Bot and Anti-Virus Event Queries</td>
<td>61</td>
</tr>
<tr>
<td>Anti-Spam and Mail</td>
<td>62</td>
</tr>
<tr>
<td>Introduction to Anti-Spam and Mail Security</td>
<td>62</td>
</tr>
<tr>
<td>Mail Security Overview</td>
<td>63</td>
</tr>
<tr>
<td>Anti-Spam</td>
<td>63</td>
</tr>
<tr>
<td>Adaptive Continuous Download</td>
<td>64</td>
</tr>
<tr>
<td>Configuring Anti-Spam</td>
<td>64</td>
</tr>
<tr>
<td>Configuring a Content Anti-Spam Policy</td>
<td>64</td>
</tr>
<tr>
<td>Configuring an IP Reputation Policy</td>
<td>65</td>
</tr>
<tr>
<td>Configuring a Block List</td>
<td>65</td>
</tr>
<tr>
<td>Configuring Anti-Spam SMTP</td>
<td>66</td>
</tr>
<tr>
<td>Configuring Anti-Spam POP3</td>
<td>66</td>
</tr>
<tr>
<td>Configuring Network Exceptions</td>
<td>66</td>
</tr>
<tr>
<td>Configuring an Allow List</td>
<td>66</td>
</tr>
<tr>
<td>Selecting a Customized Server</td>
<td>66</td>
</tr>
<tr>
<td>Anti-Spam on UTM-1 Edge Devices</td>
<td>67</td>
</tr>
<tr>
<td>Bridge Mode and Anti-Spam</td>
<td>67</td>
</tr>
<tr>
<td>Configuring Anti-Virus Protection for Mail</td>
<td>67</td>
</tr>
<tr>
<td>Configuring Mail Anti-Virus</td>
<td>67</td>
</tr>
<tr>
<td>Configuring Zero Hour Malware Protection</td>
<td>68</td>
</tr>
<tr>
<td>Configuring SMTP and POP3</td>
<td>68</td>
</tr>
<tr>
<td>Configuring File Types</td>
<td>69</td>
</tr>
<tr>
<td>Configuring Settings</td>
<td>69</td>
</tr>
<tr>
<td>Configuring a Disclaimer</td>
<td>69</td>
</tr>
<tr>
<td>Anti-Spam Logging and Monitoring</td>
<td>69</td>
</tr>
<tr>
<td>Reporting False Positives to Check Point</td>
<td>70</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction to Anti-Bot and Anti-Virus

In This Chapter

- The Need for Anti-Bot
- The Need for Anti-Virus
- The Check Point Anti-Bot and Anti-Virus Solution

The Need for Anti-Bot

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

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

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

Both of these trends are driven by bot attacks.

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

When a bot infects a computer, it:

- Takes control over the computer and neutralizes its Anti-Virus defenses. Bots are difficult to detect since they hide within your computer and change the way they appear to Anti-Virus software.

- Connects to a Command and Control (C&C) center for instructions from cyber criminals. The cyber criminals, or bot herders, can remotely control it and instruct it to execute illegal activities without your knowledge. These activities include:
  - Data theft (personal, financial, intellectual property, organizational)
  - Sending SPAM
  - Attacking resources (Denial of Service Attacks)
  - Bandwidth consumption that affects productivity

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

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

The Need for Anti-Virus

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

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

To challenge today's malware landscape, Check Point's comprehensive threat prevention solution offers a multi-layered, pre- and post-infection defense approach and a consolidated platform that enables enterprise security to deal with modern malware:

- **Anti-Virus** - Pre-infection blocking of viruses and file transfers.
- **Anti-Bot** - Post-infection bot detection, prevention, and threat visibility.

The Anti-Bot and Anti-Virus Software Blades use a separate policy installation to minimize risk and operational impact. They are integrated with other Software Blades on the same gateway to detect and stop these threats.

**The Anti-Bot Software Blade:**

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

**The Anti-Virus Software Blade:**

- Identifies malware in the organization using the ThreatSpect engine and ThreatCloud repository:
  - Prevents malware infections from incoming malicious files types (Word, Excel, PowerPoint, PDF, etc.) in real-time. Incoming files are classified on the gateway and the result is then sent to the ThreatCloud repository for comparison against known malicious files, with almost no impact on performance.
  - Prevents malware download from the internet by preventing access to sites that are known to be connected to malware. Accessed URLs are checked by the gateway's 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.

**Identifying Bot Infected Computers**

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

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

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

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

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

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

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

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

The layers of the ThreatSpect engine:

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

Preventing Bot Damage

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

Analyzing Threats

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

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

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

The Threat Wiki shows extensive malware information. It includes malware type, description, and all available details such as executables run and used protocols.
Chapter 2

Getting Started with Anti-Bot and Anti-Virus

In This Chapter

Anti-Bot and Anti-Virus Licensing and Contracts 10
SmartDashboard Toolbar 10
Enabling the Anti-Bot and Anti-Virus Software Blades 11
Creating an Anti-Bot and Anti-Virus Policy 11

Anti-Bot and Anti-Virus Licensing and Contracts

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

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

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

- The Messages and Actions section of the Overview pane of the Anti-Bot and Anti-Virus tab.
- The Check Point User Center, when you log in to your account.

SmartDashboard Toolbar

You can use the SmartDashboard toolbar to do these actions:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Open the SmartDashboard menu. When instructed to select menu options, click this button to show the menu.</td>
</tr>
<tr>
<td></td>
<td>For example, if you are instructed to select Manage &gt; Users and Administrators, click this button to open the Manage menu and then select the Users and Administrators option.</td>
</tr>
<tr>
<td></td>
<td>Save current policy and all system objects.</td>
</tr>
<tr>
<td></td>
<td>Open a policy package, which is a collection of policies saved together with the same name.</td>
</tr>
<tr>
<td></td>
<td>Refresh policy from the Security Management Server.</td>
</tr>
<tr>
<td></td>
<td>Open the Database Revision Control window.</td>
</tr>
<tr>
<td></td>
<td>Change global properties.</td>
</tr>
</tbody>
</table>
Enabling the Anti-Bot and Anti-Virus Software Blades

Enable one or more of these Software Blades on a Security Gateway: Anti-Bot and Anti-Virus.

To enable the Software Blades:

1. In SmartDashboard, right-click the gateway object and select Edit. The Gateway Properties window opens.
2. In Network Security tab, select Anti-Bot, Anti-Virus, or both of them. The Anti-Bot and Anti-Virus First Time Activation window opens.
3. Select one of the activation mode options:
   - According to policy - Enable the Anti-Bot and Anti-Virus Software Blades and use the profile settings in the Anti-Bot and Anti-Virus policy.
   - Detect only - Packets are allowed, but the traffic is logged according to the settings in the Rule Base.
4. Click OK and then install the policy.

Check Point Information

To help improve Check Point Anti-Bot and Anti-Virus products, the Security Gateway automatically sends anonymous information about feature usage, infection details, and product customizations to Check Point. The Security Gateway does not collect, process, or send any personal data.

Participating in Check Point information collection is a unique opportunity for Check Point customers to be a part of a strategic community of advanced security research. Your participation in this network allows you to contribute data to Check Point for security research. This research aims to improve coverage, quality, and accuracy of security services and obtain valuable information for organizations.

Data Check Point Collects

When you enable information collection, the Check Point Security Gateway collects and securely submits event IDs, URLs, and external IPs to the Check Point Lab regarding potential security risks.

For example:

```
<entry engineType="3" sigID="-1" attackName="CheckPoint - Testing Bot" sourceIP="7a1ec646fe17e2cd" destinationIP="d8c8f142" destinationPort="80" host="www.checkpoint.com" path="/za/images/threatwiki/pages/TestAntiBotBlade.html" numOfAttacks="20" />
```

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

You can disable information collection by clearing the Check Point Information checkbox in the Security Gateway object > Anti-Bot and Anti-Virus node window.
Creating an Anti-Bot and Anti-Virus Policy

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

- The Overview pane gives an overview of your policy and traffic.
- The Policy pane contains your Rule Base, which is the primary component of your Anti-Bot and Anti-Virus policy. Click the Add Rule buttons to get started.
- Look through the Threat Wiki to learn about malware and bots.

Creating Rules

Here are examples of how to create different types of rules.

Blocking Bots and Viruses

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

To block bots and viruses in your organization:
1. In the Gateway properties page, select the Anti-Bot Software Blade and configure the activation setting to According to the Anti-Bot and Anti-Virus policy.
2. Select the Anti-Virus Security Gateway.
3. In the Anti-Bot and Anti-Virus tab of SmartDashboard, open the Policy pane.
4. Click one of the Add Rule toolbar buttons to add the rule in the position that you choose in the Rule Base. The first rule matched is applied.
5. Make a rule that includes these components:
   - Name - Give the rule a name such as Block Bot and Virus Activity.
   - Protected Scope - The list of network objects you want to protect. In this example, the Any network object is used.
   - Action - The Profile that contains the protection settings you want ("Profiles Pane" on page 19). The default profile is Recommended_Profile.
   - Track - The type of log you want to get when detecting malware on this scope. In this example, keep Log and also select Packet Capture to capture the packets of malicious activity. In SmartView Tracker, you will then be able to view the actual packets.
   - Install On - Keep it as All or choose specified gateways to install the rule on.

Monitoring Bot Activity

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

To monitor all bot activity:
1. In the Anti-Bot and Anti-Virus tab of SmartDashboard, open the Policy pane.
2. Click one of the Add Rule toolbar buttons to add the rule in the position that you choose in the Rule Base. The first rule matched is applied.
3. Make a rule that includes these components:
   - Name - Give the rule a name such as Monitor Bot Activity.
   - Protected Scope - Keep Any so the rule applies to all traffic in the organization.
- **Action** - Right-click in the Action cell and select **New Profile**. Create a profile where all confidence level settings are configured to **Detect**.

- Select the **Performance Impact** - In this example, **Medium or lower**. This profile will detect all protections that can be identified as an attack of some sort with low, medium or high confidence and have a medium or lower performance impact.

- Set this profile as the **Action** for the rule.

- **Track** - Keep Log.

- **Install On** - Keep it as **All** or choose specified gateways to install the rule on.

**Disabling a Protection on a Specified Server**

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

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

1. In the **Anti-Bot and Anti-Virus** tab of SmartDashboard, open the **Policy** pane.
2. Click the rule that contains the scope of **Server_1**.
3. Click the **Add Exception** toolbar button to add the exception under the rule. The first exception matched is applied.
4. Make a rule exception that includes these components:
   - **Name** - Give the exception a name such as **Exclude**.
   - **Scope** - Change it to **Server_1** so that it applies to all detections on the server.
**Protection** - Click the plus sign in the cell to open the Protections viewer. Select the protection to exclude and click **OK**.

![Protection Viewer](image)

**Action** - Keep it as **Detect**.

**Track** - Keep it as **Log**.

**Install On** - Keep it as All or choose specified gateways to install the rule on.

<table>
<thead>
<tr>
<th>Name</th>
<th>Protected Scope</th>
<th>Protection</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Bot Activity</td>
<td>Any</td>
<td>- n/a</td>
<td>Recommended_Profile</td>
<td>Log</td>
</tr>
<tr>
<td>Exclude</td>
<td>Server_1</td>
<td>Backdoor.Win32.Agent.AH</td>
<td>Detect</td>
<td>Log</td>
</tr>
</tbody>
</table>

**Installing the Policy**

The Anti-Bot and Anti-Virus Software Blades have a dedicated policy. The Anti-Bot and Anti-Virus policy installation is separate from the general policy installation of the other Software Blades.

This lets you update the Anti-Bot and Anti-Virus policy Rule Base as necessary according to newly discovered threats to receive immediate coverage. It also minimizes operational impact.

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

1. From the **Anti-Bot and Anti-Virus** tab > **Policy** pane, click **Install Policy**.
2. Select the relevant options:
   - **Install Anti-Bot & Anti-Virus Policy on all gateways** - Installs the policy on all gateways enabled with Anti-Bot and Anti-Virus.
   - **Install Anti-Bot & Anti-Virus Policy on selected gateways** - Select the relevant gateways.
   - **Install on each selected gateway independently** - Enables you to install the policy on selected gateways. If you choose to install the policy on selected gateways, at the same time you can install on all gateway cluster members. This indicates that the installation process will verify that all cluster members can enforce the policy being installed.
   - **Install on all selected gateways, if it fails do not install on gateways of the same version** - Enables you to install the policy on selected gateways or on all gateways.
3. Click **OK**.
Chapter 3

Managing Anti-Bot and Anti-Virus

In This Chapter

- The Anti-Bot and Anti-Virus Overview Pane
- The ThreatCloud Repository
- Gateways Pane
- Protections Browser
- Profiles Pane
- The Policy Rule Base
- Exception Groups Pane
- Advanced Settings for Anti-Bot and Anti-Virus
- Managing Traditional Anti-Virus
- HTTP Inspection on Non-Standard Ports
- HTTPS Inspection

The Anti-Bot and Anti-Virus Overview Pane

In the Anti-Bot and Anti-Virus Overview pane, you can quickly see the gateways in your organization that are enforcing Anti-Bot and Anti-Virus and malware details. Use the windows for the most urgent or commonly-used management actions.

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

My Organization

The My Organization window shows a summary of which Security Gateways enforce Anti-Bot and Anti-Virus. It also has a link to the Gateways pane and a direct link to add a new gateway.

Messages and Action Items

The Messages and Action Items window includes:

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

Statistics

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

- Virus or bot incidents - Viruses or bots detected by the system.
Managing Anti-Bot and Anti-Virus

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

The timeline wheels are grouped according to:
- Selected time interval - hour, day, week or month
- Severity - color-coded according to critical, high, medium and low

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

This window also has links to open SmartView Tracker to see Anti-Bot and Anti-Virus logs and SmartEvent to see traffic graphs and analysis.

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

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

**Malware Activity**

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

- **Attack Map** - Pinpoints regions in the world that are attacking your organization and the corresponding number of incidents. This information comes from aggregated data on suspicious URLs and IPs.
- **Attacker IPs/URLs** - Shows details for the pinpointed regions in the Attack Map. These details include the specified URLs or IP addresses, the number of attempts and the severity.
- **Suspicious Email** - Shows the number of outgoing emails scanned from when the Anti-Bot and Anti-Virus blades were activated.

**RSS Feeds**

Shows RSS feeds with malware related information. When you click a link, it opens the Check Point Threat Wiki.

**The ThreatCloud Repository**

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

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

- A local database, the Malware database that contains commonly used signatures, URLs, and their related reputations. You can configure automatic or scheduled updates for this database ("Updating the Malware Database" on page 17).
- A local cache that gives answers to 99% of URL reputation requests. When the cache does not have an answer, it queries the ThreatCloud repository.
  - For Anti-Virus - the signature is sent for file classification.
  - For Anti-Bot - the host name is sent for reputation classification.

Access the ThreatCloud repository from:

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

**Using the Threat Wiki**

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

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

You can access the Threat Wiki from:

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

**Updating the Malware Database**

The Malware database automatically updates regularly to make sure that you have the most current data and newly added signatures and URL reputations in your Anti-Bot and Anti-Virus policy.

The Malware database only updates if you have a valid Anti-Bot and/or Anti-Virus contract.

By default, updates run on the Security Gateway every two hours. You can change the update schedule or choose to manually update the Security Gateway. The updates are stored in a few files on each Security Gateway.

**Connecting to the Internet for Updates**

The Security Gateway connects to the internet to get the Malware database updates. To make sure that it can get the updates successfully:

- Make sure that there is a DNS server configured.
- Make sure a proxy is configured for each gateway, if necessary.

To configure a proxy:

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

**Scheduling Updates**

You can change the default automatic scheduling.

To change the update schedule:

1. On the **Advanced > Updates** pane, under **Schedule Updates**, click **Configure**. The Scheduled Event Properties window opens.
2. In the General page, set the Time of Event. Use one of these options:
   - Select Every, and then adjust the setting to run the update after an interval of time.
   - Select At to set days of the week or month and a time of day for updates to occur.
     - Enter an hour in the format that is shown.
     - Click the Days node to open the Days page. Select the days when the update will occur. If you select Days of week or Days of month, more options open for you to select.
3. Click OK.

If you have Security Gateways in different time zones, they will not be synchronized when one updates and the other did not yet update.

**Gateways Pane**

The Gateways pane lists the gateways with Anti-Bot and/or Anti-Virus enabled. The Gateways pane contains these options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Add a gateway or create a new gateway.</td>
</tr>
<tr>
<td>Edit</td>
<td>Modify an existing gateway.</td>
</tr>
<tr>
<td>Remove</td>
<td>Remove the Anti-Bot and Anti-Virus blades from the selected gateway.</td>
</tr>
<tr>
<td>Search</td>
<td>Search for a gateway.</td>
</tr>
</tbody>
</table>

For each gateway, you see the gateway name and IP address in the list. You also see these columns:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-Bot</td>
<td>If Anti-Bot is enabled.</td>
</tr>
<tr>
<td>Anti-Virus</td>
<td>If Anti-Virus is enabled.</td>
</tr>
<tr>
<td>Update Status</td>
<td>If the Malware database is up to date on the gateway or if an update is necessary.</td>
</tr>
<tr>
<td>Engine Mode</td>
<td>If the activation mode is configured by a policy or is set to detect only.</td>
</tr>
<tr>
<td>Comments</td>
<td>All relevant comments.</td>
</tr>
</tbody>
</table>

**Protections Browser**

The Protections browser shows the Anti-Bot and Anti-Virus protection types and a summary of important information and usage indicators.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection</td>
<td>Shows the name of the protection type. A description of the protection type is shown in the bottom section of the pane. The Malicious Activity and Unusual Activity protections contain lists of protections. Click the plus sign to see them.</td>
</tr>
<tr>
<td>Blade</td>
<td>Shows if the protection type belongs to the Anti-Bot or Anti-Virus Software Blade.</td>
</tr>
<tr>
<td>Engine</td>
<td>Shows the layer of the ThreatSpect engine that handles the protection type.</td>
</tr>
<tr>
<td>Known Today</td>
<td>Shows the number of known protections.</td>
</tr>
</tbody>
</table>
### Column Description

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance Impact</td>
<td>Shows how much the group of protections affects the gateway’s performance. If possible, shows an exact figure.</td>
</tr>
<tr>
<td>&lt;Profile Name&gt;</td>
<td>Shows the activation setting of the protection type for each defined profile. The values shown here are calculated based on the settings of the confidence levels in the profile and the specified protections that match that confidence level. You can right-click the activation setting and select a different setting if required. This overrides the setting in the original profile.</td>
</tr>
</tbody>
</table>

### Searching Protections

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

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

### Sorting Protections

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

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

### Profiles Pane

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

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

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

A **profile** is a set of configurations based on:
- **Activation settings** (prevent, detect, or inactive) for each **confidence level** of protections that the ThreatSpect engine analyzes
- Anti-Bot Settings
- Anti-Virus Settings
- 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.
Activation Settings

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

- **Detect** - The protection action that allows identified virus or bot traffic to pass through the gateway. It logs the traffic, or tracks it, according to configured settings in the Rule Base.

- **Inactive** - The protection action that deactivates a protection.

Confidence Level

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

Performance Impact

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

There are three options:

- High or lower
- Medium or lower
- Low

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

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

Creating Profiles

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

To create a profile:
1. In the Anti-Bot and Anti-Virus tab, select **Profiles**.
2. Click **New**.
3. From the **New Profile** window, configure:
   - **General Properties**
   - **Anti-Bot Settings**
   - **Anti-Virus Settings**
   - **Malware DNS Trap**
4. Click **OK**.

General Properties

Set the general properties of the profile:

- **Name** - Mandatory, cannot contain spaces or symbols.
- **Color** - Optional color for SmartDashboard object mapping.
- **Comment** - Optional free text.
- **High Confidence, Medium Confidence, and Low Confidence** - The default action that protections will take when enabled.
- **Prevent** - Protections will block traffic matching the protection type's definitions.
- **Detect** - Protections will allow and track traffic matching the protection type's definitions.
- **Inactive** - Protections are deactivated.
- **Performance Impact** - Set the gateway performance impact level at which to activate protections.

### Anti-Bot Settings

Set the Anti-Bot parameters:

- **Inspect outgoing mails only** - The Suspicious Mail Outbreaks layer of the ThreatSpect engine inspects only outgoing emails.
- **Inspect incoming and outgoing mails** - The Suspicious Mail Outbreaks layer of the ThreatSpect engine inspects incoming and outgoing emails.

**Note** - The Suspicious Mail Outbreaks layer requires an Anti-Spam License.

- **Inspect first X (KB) of email messages** - Set the number of KB that the ThreatSpect engine should inspect for threatening bot activity.

### Anti-Virus Settings

Set the Anti-Virus parameters:

- Select a **Protected Scope** option:
  - **Inspect incoming files only**
  - **Inspect incoming and outgoing files**
- Select the relevant **Protocol** options:
  - HTTP
  - Mail
  - HTTPS
- If you select Mail, click **Configure** to set options:
  - **Maximum MIME nesting is X levels** - Set the maximum number of levels that will be scanned in a MIME email with nested contents. This controls how deeply into the nesting the ThreatSpect engine will scan.
  - **When nesting level is exceeded block/allow file** - If the nesting in an email is more than the configured level, you can configure to block or allow the file.
- Select a **File Types** option:
  - **Process file types known to contain malware**.
  - **Process all file types**.
  - **Process specific file type families** - Click **Configure** to block or inspect specified file types and click **OK**.
- To enable **Archive Scanning**:
  a) Select **Enable Archiving scanning (impacts performance)** - The engine unpacks archives and applies proactive heuristics.
  b) Click **Configure**.
  c) Set the amount in seconds to **Stop processing archive after X seconds**. The default is 30 seconds.
  d) Set to block or allow the file **When maximum time is exceeded**. The default is block.
  e) Click **OK**.
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 set this address to be the IP address of the Security Gateway’s external interface or another IP address. You can also add internal DNS servers to better identify the origin of malicious DNS requests.

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

At the Security Gateway level, you can configure to use the settings defined for the profiles or a specified IP address that is used by all profiles used on the specific gateway.

To set the Malware DNS Trap parameters for the profile:

- **Resolve requests to** - Select to use a Malware DNS Trap to identify compromised clients attempting to access known malicious domains and select which IP address to use:
  - IP of external interface in Security Gateway
  - IP - Enter another valid IP address

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

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

To set the Malware DNS Trap parameters per gateway:

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

Copying Profiles

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

To copy a profile:

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

Deleting Profiles

You can easily delete a profile (except for the **Recommended_Profile** profile). But do this carefully, as it can affect gateways, other profiles or SmartDashboard objects.

To delete a profile:

1. In the Anti-Bot and Anti-Virus tab, select **Profiles**.
2. Select the profile you want to delete and click **Delete**.

   This message is shown: **Are you sure you want to delete 1 object(s)?**
3. Click **Yes**.
   If the profile contains references to/from other objects, another message is shown:
   `<profile_name>` is used by another object and cannot be deleted.

4. Click **Where Used**.
   The Object References window opens.
   For each object that references the profile, there is a value in the **Is Removable?** column. If the value is **Yes**, you can safely delete the profile. If not, find the relationship before you decide to delete this profile.

## The Policy Rule Base

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

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

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

For examples of how to create different types of rules, see Creating Rules (on page 12).

### Predefined Rule

When you enable Anti-Bot and Anti-Virus, a predefined rule is added to the Rule Base. The rule defines that all traffic for all network objects, regardless of who opened the connection, (the protected scope (on page 25) value equals any) is inspected for all protections according to the recommended profile ("Profiles Pane" on page 19). By default, logs are generated and the rule is installed on all Anti-Bot and Anti-Virus enabled gateways.

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

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

You can see logs related to Anti-Bot and Anti-Virus traffic in SmartView Tracker and SmartEvent. Use the data there to better understand the use of Anti-Virus and Anti-Bot in your environment and create an effective Rule Base. From SmartEvent, you have an option to directly update the Rule Base.

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

### Exception Rules

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

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

You can use exception groups to group exceptions that you want to use in more than one rule. See the Exceptions Groups Pane.
You can expand or collapse the rule exceptions by clicking on the minus or plus sign next to the rule number in the No. column.

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

To add an exception to a rule:
1. In the Policy pane, select the rule to which you want to add an exception.
2. Click Add Exception.
3. Select the Above, Below, or Bottom option according to where you want to place the exception.
4. Enter values for the columns. Including these:
   - Protected Scope - Change it to reflect the relevant objects.
   - Protection - Click the plus sign in the cell to open the Protections viewer. Select the protection(s) and click OK.
5. Click Install Policy to install the dedicated Anti-Bot and Anti-Virus policy ("Installing the Policy" on page 14).

Copying an Exception to an Exception Group

You can copy an exception you have created to be a part of an existing exception group or multiple groups. If necessary, you can create a new group with this option.

To copy an exception to an exception group:
1. In the Policy pane, select the exception rule in the Rule Base.
2. Select Actions > Copy to Group.
   The Select Exception Group window opens.
3. Select the group or groups from the list or click New Group to create a new group.
4. Click OK.

Converting Exceptions into an Exception Group

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

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

Parts of the Rules

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

Number (No.)

The sequence of rules is important because the first rule that matches traffic according to a protected scope (on page 25) and profile is applied.
For example, if rules 1 and 2 share the same protected scope and a profile in rule 1 is set to detect protections with a medium confidence level and the profile in rule 2 is set to prevent protections with a medium confidence level, then protections with a medium confidence level will be detected based on rule 1.

Name
Give the rule a descriptive name. The name can include spaces.
Double-click in the Name column of the rule to add or change a name and click OK.

Protected Scope
The Anti-Bot and Anti-Virus Rule Base uses a scope parameter. Any object you configure in the Protected Scope column is inspected for viruses and/or bots, regardless of whether the object opened the connection or not. This is different from the Firewall Rule Base where the Source object defines who opened the connection.

For example, let's say you configure the protected scope of a rule with a user object named Dan Brown. In Anti-Virus, all files sent to Dan Brown will be inspected, even if he did not open the connection. In Anti-Bot, the Security Gateway will analyze Dan Brown's computer to find if is infected with a bot, even if he did not open the connection.

The predefined rule defines the protection scope as any object in the organization (includes all incoming and outgoing traffic) for all protections according to the recommended profile.

Protection
The Protection column shows the Anti-Bot and Anti-Virus protections that you choose to include.

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

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

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

Action
Action refers to how traffic is inspected.

- For rules, this is defined by the profile. The profile contains the configuration options for different confidence levels and performance impact ("Profiles Pane" on page 19).
- For rule exceptions and exception groups, the action can be set to Prevent or Detect.

To select a profile for a rule:
1. Click in the Action column.
2. Select an existing profile from the list, create a new profile, or edit the existing profile.
Track
Choose if the traffic is logged in SmartView Tracker or if it triggers other notifications. Click in the **Track** column and the options open. The options include:

- **Alert** - Logs the event and executes a command, such as show a popup window, send an email alert, or run a user-defined script as defined in **Policy > Global Properties > Log and Alert > Alerts**.
- **Log** - Records event details in SmartView Tracker. This option is useful for getting general information on network traffic.
- **None** - Does not record the event.
- **Packet capture** - Allows the packets relevant to the connection to be captured for analysis at a later time. The packet capture can be viewed from the event in SmartView Tracker ("Viewing Packet Capture Data" on page 57). This can be configured only for rules (not rule exceptions). To configure packet capture, select any tracking action other than **None** and then select **Packet capture**.

Install On
Choose which gateways the rule will be installed on. The default is All (all gateways that have Anti-Bot and Anti-Virus enabled). Put your mouse in the column and a plus sign shows. Click the plus sign to open the list of available gateways and select.

Exception Groups Pane

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

The pane shows a list of exception groups that have been created, what rules are using them, and any comments associated to the defined group. The Exceptions Groups pane contains these options:

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

**Global Exceptions**

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

**Exception Groups in the Rule Base**

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

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

When you create an exception group, you create a container for adding one or more exceptions. After you create the group, add exceptions to them. You can then add the group to rules that require the exception group in the Anti-Bot and Anti-Virus Rule Base.

To create an exception group:
1. In the Anti-Bot and Anti-Virus tab, select Exception Groups.
2. Click New.
3. From the New Exception Group window, enter:
   - Name - Mandatory, cannot contain spaces or symbols.
   - Color - Optional color for SmartDashboard object mapping.
   - Comment - Optional free text.
4. Click OK.

Adding Exceptions to Exception Groups

To use exception groups, you must add exception rules to them. For details on the columns, see Parts of the Rules (on page 24).

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

Adding Exception Groups to the Rule Base

To add an exception group to the Rule Base:
1. In the Policy pane, select the rule to which you want to add an exception group.
2. Click Add Exception > Add Exception Group.
3. Select the Above, Below, or Bottom option according to where you want to place the exception group.
   
   The Add Exception Group to rule X (where X represents the rule number) window opens.
4. Select the group from the list and click OK.
   
   The exception group is added to the Anti-Bot and Anti-Virus policy.
5. Click Install Policy to install the dedicated Anti-Bot and Anti-Virus policy ("Installing the Policy" on page 14).

Creating Exceptions from Logs or Events

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

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

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

5. Click **Install Policy** to install the dedicated Anti-Bot and Anti-Virus policy ("Installing the Policy" on page 14).

---

### Advanced Settings for Anti-Bot and Anti-Virus

This section describes settings that you can configure in the **Anti-Bot and Anti-Virus** tab > **Advanced** pane. These settings apply globally for all gateways enabled with Anti-Bot and Anti-Virus.

#### Engine Settings

On the **Advanced > Engine Settings** pane, configure settings related to engine inspection, the Check Point Online Web Service (ThreatCloud repository), and email addresses and domains that should not be scanned for Anti-Bot.

**Check Point Online Web Service**

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

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

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

**Anti-Bot Settings**

You can create a list of email addresses or domains that will not be inspected by Anti-Bot. Use this for example to exclude inspection of your organization’s internal emails.

- **Add** - Lets you add an email or domain entry.
- **Edit** - Lets you edit an entry in the list.
- **Remove** - Lets you delete an entry in the list.

**Connection Unification**

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

- For connections that are allowed or blocked in the Anti-Bot and Anti-Virus Rule Base, the default session is 10 hours (600 minutes). To change this, click Session Timeout and enter a different value.

**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.

### Managing Traditional Anti-Virus

Traditional Anti-Virus refers to inspection using these detection modes:

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

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

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

**Enabling Traditional Anti-Virus**

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

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

**To configure traditional Anti-Virus:**

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

The following kinds of database updates are available:

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

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

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

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

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

**Understanding Traditional Anti-Virus Scanning Options**

**Definitions**

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

**Scan By File Direction**

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

**Scan By IP Address**

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

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

**Comparing Scan by File Direction and by IPs**

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

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

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

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

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

**Comparing Scan by File Direction and by IPs for POP3 Protocol**

The next figure illustrates that POP3 data files are always sent in the opposite direction of the connection.

**Comparing Scan by File Direction and by IPs for FTP Protocol**

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

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

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

What is a DMZ?

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

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

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

Scan By File Direction Options

The following Scan By File Direction options are available:

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

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

**Understanding Proactive and Stream Mode Detection**

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

- **Proactive detection mode** - a comprehensive, file-based Traditional Anti-Virus solution where traffic for the selected protocols is trapped in the kernel of the Security Gateway and forwarded to the security server for scanning. It detects not only known viruses, but also zero-day attacks, by using advanced proactive techniques.
  
  This mode uses sandboxes and heuristics to detect malicious code throughout the traffic as opposed to passive signature based detection. Scanned data is either allowed or blocked based on the response of the state-of-the-art Traditional Anti-Virus engine.
  
  Proactive detection provides a high level of protection but has an impact on performance. The FTP and POP3 protocols only work in Proactive mode.
  
  This mode is not available for Virtual System gateways.

- **Stream detection mode** - where traffic is scanned for viruses as it passes through the network on streams of data, without storing entire files and without causing an impact on performance. The SMTP and HTTP protocols can be set to work in either mode.
  
  This mode is based on state-of-the-art virus signatures that are frequently updated in order to detect recent Malware outbreaks.

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

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

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

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

**Continuous Download**

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

When scanning large files, if the whole file is scanned before being made available, the user may experience a long delay before the file is delivered. A similar problem may arise when using client applications with short timeout periods (for example, certain FTP clients) to download large files. If the whole file is cached and scanned before being delivered, the client applications may time out while waiting.
To address this problem, Continuous Download starts sending information to the client while Traditional Anti-Virus scanning is still taking place. If a virus is found during the scan, file delivery to the client is terminated.

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

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

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

### File Type Recognition

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

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

The following file types can be configured:

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

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

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

### Configuring Traditional Anti-Virus

For detailed explanations regarding the options described in the procedures in this section, see Understanding Traditional Anti-Virus Scanning Options (on page 30).

### Configuring Mail Traditional Anti-Virus

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

1. In the **Traditional Anti-Virus** tab, click **Traditional Anti-Virus > Security Gateway > Mail Protocols > Mail Traditional Anti-Virus**.
2. Set the slider to **Block**.
3. Select tracking options for either all POP3 and SMTP mail, or just blocked mail. Tracking options include:
   - None (no logging)
   - Log
   - Popup alert
   - Mail alert
   - SNMP trap alert
   - Three custom user-defined scripts
Configuring Zero Hour Malware

By proactively scanning the Internet, the Data Center identifies massive virus outbreaks as soon as they occur. This Zero-Hour solution provides protection during the critical time it takes to discover a new virus outbreak and assign it a signature.

1. In the **Traditional Anti-Virus** tab, click **Traditional Anti-Virus > Security Gateway > Mail Protocols > Zero Hour Malware Protection**.

2. Using the slider, select a Zero hour malware protection level:
   - Off
   - Monitor Only
   - Block

3. Select tracking options for blocked, SMTP and POP3 mail. Tracking options include:
   - None (no logging)
   - Log
   - Popup alert
   - Mail alert
   - SNMP trap alert
   - Three custom user-defined scripts

Configuring SMTP, POP3, FTP and HTTP

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

1. In the **Traditional Anti-Virus** tab, click **Traditional Anti-Virus > Security Gateway > Mail Protocols > SMTP, POP3, FTP or HTTP**.

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

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

4. When scanning by IPs, create rules for the Rule Base to specify the source and destination of the data to be scanned.

5. For SMTP and HTTP, select the **Activate Proactive Detection (impacts performance)** checkbox to enable file-based Traditional Anti-Virus detection. Clear the checkbox to enable stream mode detection. See Understanding Proactive and Stream Mode Detection (on page 34) for further information. FTP and POP3 are set to Proactive Detection mode automatically.

6. If Proactive Detection has been configured, select the **Activate Continuous Download** checkbox to avoid client time-outs when large files are scanned. See Continuous Download (on page 34) for further information.
Configuring File Types

You can set an action to take place when a file of a certain type passes through the gateway. Certain file types can pass through the gateway without being scanned for viruses. For example, picture and video files are normally considered safe. Other formats can be considered safe because they are relatively hard to tamper with. Update the list as necessary.

### File Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>.7z</td>
<td>7z archive data</td>
<td></td>
</tr>
<tr>
<td>.8bf</td>
<td>BBF8S Adobe Photoshop Image</td>
<td></td>
</tr>
<tr>
<td>.ace</td>
<td>ACE compressed archive</td>
<td></td>
</tr>
<tr>
<td>.afx</td>
<td>AFX compressed file data</td>
<td></td>
</tr>
<tr>
<td>.al</td>
<td>Apple QuickTime</td>
<td></td>
</tr>
<tr>
<td>.arc</td>
<td>ARC archive data</td>
<td></td>
</tr>
<tr>
<td>.arj</td>
<td>ARJ archive data</td>
<td></td>
</tr>
<tr>
<td>.bzip</td>
<td>bzip compressed data</td>
<td></td>
</tr>
<tr>
<td>.bz2</td>
<td>bzip2 compressed data</td>
<td></td>
</tr>
<tr>
<td>.class</td>
<td>compiled Java class data</td>
<td></td>
</tr>
<tr>
<td>.di</td>
<td>Default Scan Values for Unknown File Types</td>
<td></td>
</tr>
<tr>
<td>.eps</td>
<td>EPS EPS Binary File</td>
<td></td>
</tr>
<tr>
<td>.gif</td>
<td>GIF image data</td>
<td></td>
</tr>
<tr>
<td>.gzip</td>
<td>gzip compressed data</td>
<td></td>
</tr>
<tr>
<td>.id</td>
<td>Incompressible data</td>
<td></td>
</tr>
</tbody>
</table>

- In the **Anti-Spam** tab, click **Traditional Anti-Virus > Security Gateway > File Types** page and set the actions. See **File Type Recognition** (on page 35) for more information.

In this window, you can also configure Continuous Download options. Continuous Download options are only relevant if scanning is set to Proactive Detection. See **Continuous Download** (on page 34) for more information.

### Configuring Security Gateway Settings

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

#### Scan Failure

The following scan failure options are available:

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

#### File Handling

The following file handling options are available:

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

Note - An email is treated as an archive and is not affected when the file exceeds the limit.
Archive File Handling

The following file handling archiving options are available:

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

Logging and Monitoring

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

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

UTM-1 Edge Traditional Anti-Virus

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

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

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

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

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

To enable and configure Traditional Anti-Virus protection:

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

HTTP Inspection on Non-Standard Ports

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

When selected, the Anti-Bot and Anti-Virus policy inspects all HTTP traffic, even if it is sent using nonstandard ports. This option is selected by default. You can configure this option in the **Anti-Bot and Anti-Virus** tab > **Advanced** pane.
HTTPS Inspection

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

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

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

There are two types of HTTPS inspection:

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

The Security Gateway acts as an intermediary between the client computer and the secure web site. The Security Gateway behaves as the client with the server and as the server with the client using certificates. All data is kept private in HTTPS Inspection logs. This is controlled by administrator permissions. Only administrators with HTTPS Inspection permissions can see all the fields in a log. Without these permissions, some data is hidden.

**How it Operates**

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

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

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

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

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

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

When required, you can update the trusted CA list in the Security Gateway.

Enabling HTTPS Inspection

You must enable HTTPS inspection on each gateway. From Security Gateway > HTTPS Inspection > Step 3 > Select Enable HTTPS Inspection.

The first time you enable HTTPS inspection on one of the 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 gateways managed on the Security Management Server.

Creating an Outbound CA Certificate

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

After you create an outbound CA certificate, you must export it so it can be distributed to clients. If you do not deploy the generated outbound CA certificate on clients, users will receive SSL error messages in their browsers when connecting to HTTPS sites. You can configure a troubleshooting option that logs such connections ("Troubleshooting" on page 50).

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

To create an outbound CA certificate:

1. In SmartDashboard, right-click the gateway object and select Edit. The Gateway Properties window opens.
2. In the navigation tree, select HTTPS Inspection.
3. In the HTTPS Inspection page, click Create.
4. Enter the necessary information:
   - **Issued by (DN)** - Enter the domain name of your organization.
   - **Private key password** - Enter the password that is used to encrypt the private key of the CA certificate.
   - **Retype private key password** - Retype the password.
   - **Valid from** - Select the date range for which the CA certificate is valid.
5. Click OK.
6. Export and deploy the CA certificate ("Exporting and Deploying the Generated CA" on page 41).
Importing an Outbound CA Certificate

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

- **Important** - If you are importing a CA certificate created on another Security Management Server, make sure the initial certificate was exported ("Exporting a Certificate from the Security Management Server" on page 41) from the Security Management Server on which it was created.

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

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

- **Important** - After you import a certificate from another Security Management Server, make sure to export the certificate and deploy it ("Exporting and Deploying the Generated CA" on page 41) on the client machines if it has not already been deployed.

To import a CA certificate:

1. In SmartDashboard, right-click a gateway object, select Edit > HTTPS Inspection > Import
   Or
   From the HTTPS Inspection > Gateways pane of a supported blade, click the arrow next to Create Certificate and select Import certificate from file.
   The Import Outbound Certificate window opens.
2. Browse to the certificate file.
3. Enter the private key password.
4. Click OK.

Exporting a Certificate from the Security Management Server

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

Usage:

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

To export the CA certificate:

- On the Security Management Server, run:
  ```bash
  /$FWDIR/bin/export_https_cert -local -f [certificate file name under FWDIR/tmp]
  ```
  For example:
  ```bash
  /$FWDIR/bin/export_https_cert -local -f mycompany.p12
  ```

Exporting and Deploying the Generated CA

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

When users do standard updates, the generated CA will be in the CA list and they will not receive browser certificate warnings.
To distribute a certificate with a GPO:
1. From the HTTPS Inspection window of the Security Gateway, click Export certificate
Or
From the HTTPS Inspection > Gateways pane in a supported blade, click Export.
2. Save the CA certificate file.
3. Use the Group Policy Management Console ("Deploying Certificates by Using Group Policy" on page 42) to add the certificate to the Trusted Root Certification Authorities certificate store.
4. Push the policy to the client machines in the organization.

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

Deploying Certificates by Using Group Policy
You can use this procedure to deploy a certificate to multiple client machines by using Active Directory Domain Services and a Group Policy object (GPO). A GPO can contain multiple configuration options, and is applied to all computers that are within the scope of the GPO.

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

To deploy a certificate using Group Policy:
1. Open the Group Policy Management Console.
2. Find an existing GPO or create a new GPO to contain the certificate settings. Make sure the GPO is associated with the domain, site, or organization unit whose users you want affected by the policy.
3. Right-click the GPO and select Edit.
   The Group Policy Management Editor opens and shows the current contents of the policy object.
5. Click Action > Import.
6. Do the instructions in the Certificate Import Wizard to find and import the certificate you exported from SmartDashboard.
7. In the navigation pane, click Trusted Root Certification Authorities and repeat steps 5-6 to install a copy of the certificate to that store.

Configuring Inbound HTTPS Inspection
To enable inbound HTTPS traffic inspection, you must do these steps:

- Set the Security Gateway for HTTPS Inspection (if it is not already configured). From Security Gateway > HTTPS Inspection > Step 3 > Select Enable HTTPS Inspection.
- Import server certificates for servers behind the organizational gateways ("Server Certificates" on page 42).
- Generate an HTTPS inspection policy by defining relevant rules in the HTTPS inspection Rule Base ("The HTTPS Inspection Policy" on page 43).
- Make sure to configure the relevant server certificate in the HTTPS inspection Rule Base ("Certificate" on page 46).

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

For inbound HTTPS inspection, do these steps:
- Add the server certificates to the Security Gateway - This creates a server certificate object ("Adding a Server Certificate" on page 43).
- Add the server certificate object to the Certificate column in the HTTPS Inspection Policy to enforce it in rules ("Certificate" on page 46).

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

**Adding a Server Certificate**

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

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

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

**To add a server certificate:**

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

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

**The HTTPS Inspection Policy**

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

The HTTPS Rule Base lets you inspect the traffic on other network blades. The blades that HTTPS can operate on are based on the blade contracts and licenses in your organization and can include:
- Application Control
- URL Filtering
- IPS
- DLP
- Anti-Virus
- Anti-Bot

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

**To access the HTTPS inspection Rule Base:**

- In SmartDashboard, open the Policy page from the specified blade tab:
  - For Application and URL Filtering, Anti-Bot, Anti-Virus, and IPS - Select **Advanced > HTTPS Inspection > Policy**.
  - For DLP - Select **Additional Settings > HTTPS Inspection > Policy**.
Predefined Rule

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Site Category</th>
<th>Action</th>
<th>Track</th>
<th>Blade</th>
<th>Install On</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predefined Rule</td>
<td>Any</td>
<td>Internet</td>
<td>HTTPS</td>
<td>Any</td>
<td>Inspect</td>
<td>None</td>
<td>All</td>
<td>All</td>
<td>Outbound Certificate</td>
</tr>
</tbody>
</table>

Parts of the Rule

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

**Number (No.)**

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

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

**Name**

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

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

**Source**

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

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

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

**Destination**

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

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

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

**Services**

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

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

**Site Category**

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

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

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

Note - You can only use custom objects that specify the domain name or host part of a URL. URLs that contain paths are not supported. For example, you can use an object defined as ww.gmail.com but not www.gmail.com/myaccount.

To add site categories to a rule:

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

- To filter the Available list by categories or custom-defined sites, click the specified button in the toolbar of the viewer. The Available list opens in the left column and then you can add items to the rule.
- To add a category object to the rule, click the checkbox in the Available list.
- To see the details of category without adding it to the rule, click the name of the item in the Available list.
- You can only select a category to add to the rule from the Available list.
- If a category is already in a rule, it will not show in the Category viewer.
- If you know the name of a category, you can search for it. The results will show in the Available list.
- You can add a new host site with the New button.

Adding a New Host Site

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

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

Action

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

- Inspect - The traffic is inspected on the blades set in the Blades column.
- Bypass - The traffic of source and destination traffic in rules that include the bypass action are not decrypted and inspected. You can bypass HTTPS inspection for all Check Point objects. This is recommended for Anti-Bot, Anti-Virus, URL Filtering, and IPS updates. Other HTTPS protections that already operate on traffic will continue to work even when the HTTPS traffic is not decrypted for inspection.
Track
Choose if the traffic is logged in SmartView Tracker or if it triggers other notifications. Click in the column and the options open. The options include:

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

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

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

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

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

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

- **For outbound HTTPS inspection** - choose the Outbound Certificate object (default) that reflects the CA certificate you created/imported and deployed on the client machines in your organization.
- **For inbound HTTP inspection** - choose the server certificate applicable to the rule. Put your mouse in the column and a plus sign shows. Click the plus sign to open the list of available server certificates and select one. When there is a match to a rule, the Security Gateway uses the selected server certificate to communicate with the source client. You can create server certificates from HTTPS Inspection > Server Certificates > Add.
Bypassing HTTPS Inspection to 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 to software updates:
1. In the HTTPS Inspection > Policy pane, select **Bypass HTTPS Inspection of traffic to well known software update services (list is dynamically updated)**. This option is selected by default.
2. Click **list** to see the list of approved domain names.

Gateways Pane

The **Gateways** pane lists the gateways with HTTPS Inspection enabled. Select a gateway and click **Edit** to edit the gateway properties. You can also search, add and remove gateways from here.

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

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

If the Security Management Server managing the selected gateway does not have a generated CA certificate installed on it, you can add it with **Import certificate from file**. There are two options:

- You can import a CA certificate already deployed in your organization.
- You can import a CA certificate from another Security Management Server. Before you can import it, you must first export ("Exporting a Certificate from the Security Management Server" on page 41) it from the Security Management Server on which it was created.

Adding Trusted CAs for Outbound HTTPS Inspection

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

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

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

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

You can change the default setting to block untrusted server certificates ("Server Validation" on page 48).


Automatically Updating the Trusted CA List and Certificate Blacklist

Updates for the trusted CA list and Certificate Blacklist ("Certificate Blacklisting" on page 49) will be published from time to time on the Check Point web site. They are automatically downloaded to the Security Management Server by default. When you are sent a notification that there is an update available, install it and do the procedure. The first notification is shown in a popup balloon once and then in the notification line under HTTPS Inspection > Trusted CAs. You can disable automatic updates if necessary.

To update the Trusted CA list and Certificate Blacklist:
1. In SmartDashboard, select HTTPS Inspection > Trusted CAs.
2. In the Automatic Updates section, click **Install Now**.
You see the certificates that will be added or removed to the lists and the validity date range of the certificates added to the Trusted CA list.

3. Click **Proceed** to confirm the update.
   The certificates will be added or removed respectively from the lists.

4. Install the policy.

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

**Manually Updating a Trusted CA**

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

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

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

**Saving a CA Certificate**

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

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

**HTTPS Validation**

**Server Validation**

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

- **Untrusted server certificate**
  - When selected, traffic from a site with an untrusted server certificate is immediately dropped. The user gets an error page that states that the **browser cannot display the webpage**.
  - When cleared, a self-signed certificate shows on the client machine when there is traffic from an untrusted server. The user is notified that there is a problem with the website’s security certificate, but lets the user to continue to the website (default).
- **Revoked server certificate (validate CRL)**
  - When selected, the Security Gateway validates that each server site certificate is not in the Certificate Revocation List (CRL) (default).

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

    To validate the CRL, the Security Gateway must have access to the internet. For example, if a proxy server is used in the organization's environment, you must configure the proxy for the Security Gateway.

    To configure the proxy:
    a) From the **Firewall** tab, double-click the Security Gateway that requires proxy configuration.
    b) Select **Topology** > Proxy.
    c) Select **Use custom proxy settings for this network object** and **Use proxy server** and enter the proxy IP address.
    d) Optionally, you can use the default proxy settings.
    e) Click **OK**.

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

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

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

- **Automatically retrieve intermediate CA certificates**
  - When selected, intermediate CA certificates issued by trusted root CA certificates that are not part of the certificate chain are automatically retrieved using the information on the certificate (default).

    When cleared, a web server certificate signed by an intermediate CA certificate which is not sent as part of the certificate chain, will be considered untrusted.

**Certificate Blacklisting**

You can create a list of certificates that are blocked. Traffic from servers using the certificates in the blacklist will be dropped. If a certificate in the blacklist is also in the Trusted CAs list, the blacklist setting overrides the Trusted CAs list.

- **Add** - Lets you add a certificate. Enter the certificate's serial number (in hexadecimal format HH:HH) and a comment that describes the certificate.
• **Edit** - Lets you change a certificate in the blacklist.
• **Remove** - lets you delete a certificate in the blacklist.
• **Search** - Lets you search for a certificate in the blacklist.

**Track dropped traffic**
Choose if the dropped traffic is logged in SmartView Tracker or if it triggers other notifications. The options include:

- **None** - Does not record the event.
- **Log** - Records the event's details in SmartView Tracker
- **Alert** - Logs the event and executes a command, such as shows a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in **Policy > Global Properties > Log and Alert > Alert Commands**
- **Mail** - Sends an email to the administrator, or runs the mail alert script defined in **Policy > Global Properties > Log and Alert > Alert Commands**
- **SNMP Trap** - Sends an SNMP alert to the SNMP GUI, or runs the script defined in **Policy > Global Properties > Log and Alert > Alert Commands**
- **User Defined Alert** - Sends one of three possible customized alerts. The alerts are defined by the scripts specified in **Policy > Global Properties > Log and Alert > Alert Commands**

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

- The generated CA was not deployed on clients ("Exporting and Deploying the Generated CA" on page 41).
- The DN in the certificate does not match the actual URL (for example, when you browse to https://www.gmail.com, the DN in the certificate states mail.google.com).
- Applications (such as FireFox and anti-viruses) that use an internal trusted CAs list (other than Windows). Adding the CA certificate to the Windows repository does not solve the problem.

The option in the HTTPS Validation pane:

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

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

Each successful connection creates two different connections:

- One connection between the client in the organization and the proxy.
- One connection between the proxy and the actual destination.
Proxy Modes
Two proxy modes are supported:

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

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

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

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

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

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

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

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

1. From the **General Properties** window of a Security Gateway object, select **HTTP/HTTPS Proxy** from the tree.
2. Select **Use this gateway as a HTTP/HTTPS Proxy**.
3. Select the **Transparent** or **Non Transparent** proxy mode.

   **Note** - If you select **Non Transparent** mode, make sure to configure the clients to work with the proxy.

4. Select to forward HTTP requests from one of these options:
   - **All Internal Interfaces**
   - **Specific Interfaces** - Click the plus sign to add specified interfaces or the minus sign to remove an interface.

5. To enter more ports on which to forward traffic, select **Add**.
6. To include the actual source IP address in the HTTP header, select **Advanced > X-Forward-For header (original client source IP address)**.

   **Note** - The X-Forward-For header must be configured if traffic will be forwarded to Identity Awareness gateways that require this information for user identification.

7. Click **OK**.

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

- Mobile web access portal
- SecurePlatform WebUI
Managing Anti-Bot and Anti-Virus

- Gaia WebUI
- Identity Awareness (captive portal)
- DLP portal
- SSL Network Extender portal
- UserCheck portal
- Endpoint Security portals (CCC)

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

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

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

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

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

**To Configure TLS Protocol Support for HTTPS inspection:**
1. In GuiDBedit, on the Tables tab, select Other > ssl_inspection.
2. In the Objects column, select general_confs_obj.
3. In the Fields column, select the minimum and maximum TLS version values in these fields:
   - ssl_max_ver (default = TLS 1.2)
   - ssl_min_ver (default = SSLv3)

**HTTPS Inspection in SmartView Tracker**

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

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

**To open SmartView Tracker do one of these:**
- From the SmartDashboard toolbar, select Window > SmartView Tracker.
- Press Control + Shift + T.

**HTTPS Inspection Queries**

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

- All - Shows all HTTPS traffic that matched the HTTPS Inspection policy and was configured to be logged.
- HTTPS Validations - Shows traffic with connection problems.
• Action values include rejected or detected. The actions are determined by the SSL validation settings ("HTTPS Validation" on page 48) for HTTPS Inspection.

• HTTPS Validation values include:
  ▪ Untrusted Server Certificate
  ▪ Server Certificate Expired
  ▪ Revoked Certificate or Invalid CRL
  ▪ SSL Protocol Error - For general SSL protocol problems

Blade Queries
When applying HTTPS Inspection to a specified blade:

• There is an HTTPS Inspection predefined query for each of the blades that can operate with HTTPS Inspection. The query shows all traffic of the specified blade that passed through HTTPS inspection.

• The log in the blade’s queries includes an HTTP Inspection field. The field value can be inspect or bypass. If the traffic did not go through HTTPS inspection, the field does not show in the log.

Permissions for HTTPS Logs
An administrator must have HTTPS inspection permissions to see classified data in HTTPS inspected traffic.

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

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

HTTPS Inspection in SmartEvent
Events from HTTPS Inspection are shown in SmartEvent. There are two types of predefined queries for HTTPS Inspection events in SmartEvent:

• HTTPS Inspection queries for HTTPS validations

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

To open SmartEvent do one of these:
• From the SmartDashboard toolbar, select Window > SmartEvent.
• Press Control +Shift +T.
Event Analysis in SmartEvent

SmartEvent supplies advanced analysis tools with filtering, charts, reporting, statistics, and more, of all events that pass through enabled Security Gateways. SmartEvent shows all HTTPS Inspection events. You can filter the HTTPS Inspection information for fast monitoring on HTTPS Inspection traffic.

- Real-time and history graphs of HTTPS Inspection traffic.
- Graphical incident timelines for fast data retrieval.
- Easily configured custom views to quickly view specified queries.
- Incident management workflow.

SmartEvent shows information for all Software Blades in the environment.

Viewing Information in SmartEvent

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

- HTTPS Inspection queries
- Blade queries

HTTPS Inspection Queries

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

Blade Queries

- There is an HTTPS Inspection predefined query for each of the blades that can operate with HTTPS Inspection. The query shows all traffic of the specified blade that passed through HTTPS inspection.
- The Summary tab in the event record in the blade's queries includes an HTTPS Inspection field. The field value can be inspect or bypass. If the traffic did not go through HTTPS inspection, the field does not show in the event record.
Chapter 4

Anti-Bot and Anti-Virus in SmartView Tracker

In This Chapter

Log Sessions 55
Anti-Bot and Anti-Virus Logs 56
Viewing Logs 56
Viewing Packet Capture Data 57
Using Predefined Queries 57

Log Sessions

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

To see the number of connections made during a session, see the Suppressed Logs field of the log in SmartView Tracker.

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

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

More

<table>
<thead>
<tr>
<th>Traffic</th>
<th>4053</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td><a href="http://tbwe.shopathome.com/RequestHandler.ashx">http://tbwe.shopathome.com/RequestHandler.ashx</a></td>
</tr>
<tr>
<td>Resource</td>
<td><a href="http://admob.com">http://admob.com</a></td>
</tr>
<tr>
<td></td>
<td><a href="http://admob.com?language=en">http://admob.com?language=en</a></td>
</tr>
<tr>
<td>Severity</td>
<td>Critical</td>
</tr>
<tr>
<td>Description</td>
<td>Destination URL has bad reputation</td>
</tr>
<tr>
<td>Source OS</td>
<td>Windows</td>
</tr>
<tr>
<td>Proxyed Source IP</td>
<td>158.70.104.64</td>
</tr>
<tr>
<td>Client Type</td>
<td>Other: SelectRebates</td>
</tr>
<tr>
<td>Suppressed Logs</td>
<td>22</td>
</tr>
<tr>
<td>Sent Bytes</td>
<td>1810</td>
</tr>
<tr>
<td>Received Bytes</td>
<td>1624</td>
</tr>
<tr>
<td>Destination Country</td>
<td>[Taiwan]</td>
</tr>
<tr>
<td>Malware Family</td>
<td>FraudLoad</td>
</tr>
<tr>
<td>Malware Activity</td>
<td>Communication with Command &amp; Control</td>
</tr>
<tr>
<td>Information</td>
<td>Source OS version: XP SP1, 2000 SP3 confidence_level: 67</td>
</tr>
</tbody>
</table>
Anti-Bot and Anti-Virus Logs

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

Viewing Logs

To open SmartView Tracker do one of these:

- Click Start > Check Point > SmartView Tracker.
- From the Anti-Bot and Anti-Virus tab > Navigation Tree > Track Logs link.
- From the Anti-Bot and Anti-Virus tab > Overview > Statistics > Logs link.
- From the SmartDashboard toolbar of any SmartConsole application, select Window > SmartView Tracker or press Control + Shift + T.

Updating the Anti-Bot and Anti-Virus Rule Base

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

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

1. Right-click the log entry.
2. Select Go to Rule.
3. Make related changes.
4. Click Install Policy to install the dedicated Anti-Bot and Anti-Virus policy ("Installing the Policy" on page 14).

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

1. Right-click the log entry.
2. Select Add Exception to the Rule.
3. Select an Exception Scope option:
   - Apply Exception to rule number X - If you want the exception to apply only to the related rule.
   - Apply Exception to all rules - If you want the exception to apply to all rules. The exception is added to the Exception Groups > Global Exceptions pane.
4. Click OK.
5. Click Install Policy to install the dedicated Anti-Bot and Anti-Virus policy ("Installing the Policy" on page 14).

Accessing the Threat Wiki

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

To open the Threat Wiki:

- Click the malware protection link in the Protection Name field of a log record.
Viewing Packet Capture Data
If you set a rule with the Packet Capture track option, you can see the captures in SmartView Tracker.

To see packet captures in SmartView Tracker:
1. Locate the log entry with the packet capture.
2. Right-click the entry and select View packet capture.
3. Select Internal Viewer and click OK.
   The packet is shown in the Viewer Output window.
   You can also use a third-party capture application by selecting Choose Program and entering the application in the Program Name field.

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

- **Anti-Bot** - Shows Anti-Bot traffic (prevented and detected connections).
- **Anti-Virus** - Shows Anti-Virus traffic (prevented and detected connections).
- **Blocked Incidents** - Shows all Anti-Bot and Anti-Virus blocked (prevented) traffic.
- **All** - Shows all Anti-Bot and Anti-Virus traffic, including all prevented and detected connections.
Chapter 5

Anti-Bot and Anti-Virus in SmartEvent

In This Chapter

- Event Analysis in SmartEvent or SmartEvent Intro 58
- Viewing Information in SmartEvent 58
- Anti-Bot and Anti-Virus Reports 59
- Viewing Information in SmartEvent Intro 60

Event Analysis in SmartEvent or SmartEvent Intro

SmartEvent and SmartEvent Intro supply advanced analysis tools with filtering, charts, reporting, statistics, and more, of all events that travel through enabled Security Gateways.

You can filter the Anti-Bot and Anti-Virus information for fast monitoring and useful reporting on connection incidents related to them.

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

SmartEvent shows information for all Software Blades in the environment. SmartEvent Intro shows information for one SmartEvent Intro mode. If you select Anti-Bot and Anti-Virus as the SmartEvent Intro Mode, it shows the Anti-Bot and Anti-Virus information.

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

- R76 SmartEvent Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk91140)
- R76 SmartEvent Intro Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk91140)

Viewing Information in SmartEvent

To open SmartEvent do one of these:

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

When SmartEvent opens, go to Events > Predefined > Anti-Bot and Anti-Virus to use the predefined queries for Anti-Bot and Anti-Virus.

- All Events - Shows all Anti-Bot and Anti-Virus events grouped by source, includes all prevented and detected events.
• **By Protection Name** - Shows all Anti-Bot and Anti-Virus events grouped by protection name.
• **By Protection Type** - Shows all Anti-Bot and Anti-Virus events grouped by protection name.
• **By Activity** - Shows all Anti-Bot and Anti-Virus events grouped by malware activity.
• **More > Anti-Bot** - Shows all Anti-Bot events.
• **More > Anti-Virus** - Shows all Anti-Virus events.
• **More > Blocked Incidents** - Shows all Anti-Bot and Anti-Virus blocked incidents.

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

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

**To update a rule in the Anti-Bot and Anti-Virus Rule Base:**
1. Right-click the event or from within event details select the **Anti-Virus** or **Anti-Bot** menu.
2. Select **Go to Rule**.
   - SmartDashboard opens showing the related rule in the Anti-Bot and Anti-Virus Rule Base.
3. Make related changes.
4. Click **Install Policy** to install the dedicated Anti-Bot and Anti-Virus policy ("Installing the Policy" on page 14).

**To update a rule exception in the Anti-Bot and Anti-Virus Rule Base:**
1. Right-click the event or from within the event details, select the **Anti-Virus** or **Anti-Bot** menu.
2. Select **Add Exception to the Rule**.
   - SmartDashboard opens and shows an **Add Exception** window in the Anti-Bot and Anti-Virus Rule Base. These details are shown:
     • **Protection** - The name of the protection. Details are taken from the ThreatCloud repository or, if there is no connectivity, from the log.
     • **Scope** - The scope is taken from the log. If there is no related host object, an object is created automatically after you click OK. Click the plus sign to add additional objects.
     • **Install On** - Shows **All** by default. You can use the plus sign to add gateways.
3. Select an **Exception Scope** option:
   • **Apply Exception to rule number X** - If you want the exception to apply only to the related rule.
   • **Apply Exception to all rules** - If you want the exception to apply to all rules. The exception is added to the **Exception Groups > Global Exceptions** pane.
4. Click **OK**.
   - The exception is added to the Rule Base. The **Action** is set to **Detect** by default. Change if necessary.
5. Click **Install Policy** to install the dedicated Anti-Bot and Anti-Virus policy ("Installing the Policy" on page 14).

### Accessing the Threat Wiki

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

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

Daily, weekly, and monthly reports of the events recorded by SmartEvent are configured and stored on the Reports tab. These reports show a high-level summary of the event patterns occurring on your network.

Upon creation, reports can be automatically emailed to predefined addresses, eliminating the need to open SmartEvent to learn of the system's status. You can also choose to save them as PDFs or view them in a browser.

Viewing Information in SmartEvent Intro

To open SmartEvent Intro:

1. From the SmartDashboard toolbar, select Window > SmartEvent Intro or press Control + Shift + E.
2. Select Anti-Bot and Anti-Virus.

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

The SmartEvent Intro Overview Page

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

The Overview page includes these panes:

- Timeline View
- Anti-Bot & Anti-Virus
- Top Source/Destination Countries of Anti-Bot & Anti-Virus
- Top Malwares by Event Count
- Top Malicious Activities by Event Count
- Status
Anti-Bot and Anti-Virus Event Queries

See detailed event queries in the **Events** tab.

- **All Events** - Shows all Anti-Bot and Anti-Virus events grouped by source, includes all prevented and detected events.
- **By Protection Name** - Shows all Anti-Bot and Anti-Virus events grouped by protection name.
- **By Protection Type** - Shows all Anti-Bot and Anti-Virus events grouped by protection name.
- **By Activity** - Shows all Anti-Bot and Anti-Virus events grouped by malware activity.
- **More > Anti-Bot** - Shows all Anti-Bot events.
- **More > Anti-Virus** - Shows all Anti-Virus events.
- **More > Blocked Incidents** - Shows all Anti-Bot and Anti-Virus blocked incidents.

See the [R76 SmartEvent Intro Administration Guide](http://supportcontent.checkpoint.com/solutions?id=sk91140).
Chapter 6

Anti-Spam and Mail

In This Chapter
- Introduction to Anti-Spam and Mail Security
- Mail Security Overview
- Configuring Anti-Spam
- Configuring Anti-Virus Protection for Mail
- Configuring a Disclaimer
- Anti-Spam Logging and Monitoring
- Reporting False Positives to Check Point
- Anti-Spam Tracking and Reporting Options

Introduction to Anti-Spam and Mail Security

The relentless and unprecedented growth in unwanted email now poses an unexpected security threat to the network. As the amount of resources (disk space, network bandwidth, CPU) devoted to handling unsolicited emails increases from year to year, employees waste more and more time sorting through unsolicited bulk email commonly known as spam. Anti-Spam and Mail provides network administrators with an easy and central way to eliminate most of the spam reaching their networks.

Anti-Spam and Mail Features

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

On the Anti-Spam & Mail tab:

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

Anti-Spam

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

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

Once identified, the network of spam generating machines is blacklisted. If the network changes its behavior, it is removed from the black list.
The following figure illustrates the Anti-Spam workflow:

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

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

**Adaptive Continuous Download**

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

**Configuring Anti-Spam**

**Configuring a Content Anti-Spam Policy**

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

1. Use the slider to select an Anti-Spam policy protection level.
2. Select flagging options.
3. In the **Security Gateway Engine settings** section, set a maximum data size to scan.
4. In the **UTM-1 Edge Engine settings** section, set a confidence level for spam and suspected spam. A spam confidence level is a grade or rating (usually between zero and a hundred) used to decide whether a particular email message should be treated as spam. For example, if the confidence level is set to 70, then all email messages rated at 70 or above will be treated as spam.

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

5. Select **Tracking Options** for **Spam**, **Suspected Spam**, or **Non Spam**. Tracking options include:
   - None (no logging)
   - Log
   - Popup Alert
   - Mail Alert
   - SNMP trap alert
   - Three custom user-defined scripts.

### Configuring an IP Reputation Policy

This window enables IP reputation, an Anti-Spam mechanism that checks the IP address of the message sender (contained in the opening SYN packet) against a dynamic database of suspect IP addresses. If, according to the IP reputation service, the originating network has a reputation for sending spam, then the spam session is blocked at connect time. In this way, the IP reputation feature creates a list of trusted email sources.

1. Use the slider to select an IP Reputation Policy:
   - **Off** - IP Reputation service is disabled
   - **Monitor** - Monitors known and suspected spam but does not block it
   - **Medium Protection** - Blocks known spam and monitors suspected spam
   - **High Protections** - Blocks known and suspected spam

2. Select tracking options for **Spam**, **Suspected Spam**, or **Non spam**. Tracking options include
   - None (no logging)
   - Log
   - Popup Alert
   - Mail Alert
   - SNMP trap alert
   - Three custom user-defined scripts.

### Configuring a Block List

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

1. Use the slider to select a Block Policy:
   - **Off** - Not blocked
   - **Monitor** Only - Not Blocked, but monitors senders by IP address and email address
   - **Block** - Blocks senders by IP address and email address

2. In the **Blocked senders/domains** section, click **Add** and enter the name of a sender or domain to be rejected.

3. In the **Blocked IPs** section, click **Add** and enter an IP address that should be blocked.

4. From the drop-down list in the **Tracking** section, select a tracking option for blocked mail or non-spam.
Configuring Anti-Spam SMTP
SMTP traffic can be scanned according to direction.
1. Select a scanning direction for:
   - Incoming files
   - Outgoing files
   - Internal files through the gateway
2. Select **Activate Continuous download** to avoid client time-outs when large files are scanned.
   See Adaptive Continuous Download ("Continuous Download" on page 34) for further information.

Configuring Anti-Spam POP3
POP3 traffic can be scanned according to direction.
1. Select a scanning direction for:
   - Incoming files
   - Outgoing files
   - Internal files
2. Select **Activate Continuous download** to avoid client time-outs when large files are scanned.
   See Adaptive Continuous Download ("Continuous Download" on page 34) for further information.

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

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

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

Selecting a Customized Server
You can select an alternative data center for Anti-Spam analysis.

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

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

**To configure Anti-Spam on UTM-1 Edge devices:**
1. Open the General Properties window of the UTM-1 Edge gateway.
2. Select the Anti-Spam option.

---

**Bridge Mode and Anti-Spam**

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

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

---

**Configuring Anti-Virus Protection for Mail**

**Configuring Mail Anti-Virus**

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

**To configure a mail Anti-Virus policy:**
1. In the Anti-Spam & Mail tab, click Traditional Anti-Virus > Security Gateway > Mail Protocols > Mail Anti-Virus.
2. Set the slider to Block.
3. Select tracking options for either all POP3 and SMTP mail, or just blocked mail. Tracking options include:
- None (no logging)
- Log
- Popup alert
- Mail alert
- SNMP trap alert
- Three custom user-defined scripts

**Configuring Zero Hour Malware Protection**

By proactively scanning the Internet, the Data Center identifies massive virus outbreaks as soon as they occur. This Zero-Hour solution provides protection during the critical time it takes to discover a new virus outbreak and assign it a signature.

1. In the **Anti-Spam & Mail** tab, click **Traditional Anti-Virus > Security Gateway > Mail Protocols > Zero Hour Malware Protection**.

2. Using the slider, select a Zero hour malware protection level:
   - Off
   - Monitor Only
   - Block

3. Select tracking options for blocked, SMTP and POP3 mail. Tracking options include:
   - None (no logging)
   - Log
   - Popup alert
   - Mail alert
   - SNMP trap alert

4. Three custom user-defined scripts

**Configuring SMTP and POP3**

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

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

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

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

4. When scanning by IPs, create rules for the Rule Base to specify the source and destination of the data to be scanned.

5. For SMTP and HTTP, select the **Activate Proactive Detection (impacts performance)** checkbox to enable file-based Traditional Anti-Virus detection. Clear the checkbox to enable stream mode detection. See Understanding Proactive and Stream Mode Detection (on page 34) for further information. FTP and POP3 are set to Proactive Detection mode automatically.

6. If Proactive Detection has been configured, select the **Activate Continuous Download** checkbox to avoid client time-outs when large files are scanned.

See Continuous Download (on page 34) for further information.
Configuring File Types

You can set an action to take place when a file of a certain type passes through the gateway. Certain file types can pass through the gateway without being scanned for viruses. For example, picture and video files are normally considered safe. Other formats can be considered safe because they are relatively hard to tamper with. Update the list as necessary.

**File Types**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>7z</td>
<td>7z archive data</td>
<td>Scan</td>
</tr>
<tr>
<td>BBPS</td>
<td>BBPS Adobe Photoshop Image</td>
<td>Pass</td>
</tr>
<tr>
<td>ace</td>
<td>ACE compressed archive</td>
<td>Scan</td>
</tr>
<tr>
<td>ARJ</td>
<td>ARJ compressed file data</td>
<td>Scan</td>
</tr>
<tr>
<td>qti</td>
<td>Apple QuickTime</td>
<td>Scan</td>
</tr>
<tr>
<td>arc</td>
<td>ARC archive data</td>
<td>Scan</td>
</tr>
<tr>
<td>arj</td>
<td>ARJ archive data</td>
<td>Scan</td>
</tr>
<tr>
<td>zip</td>
<td>ZIP compressed data</td>
<td>Scan</td>
</tr>
<tr>
<td>rar</td>
<td>RAR compressed data</td>
<td>Scan</td>
</tr>
<tr>
<td>class</td>
<td>compiled Java class data</td>
<td>Scan</td>
</tr>
<tr>
<td>Unknown</td>
<td>Default Scan Value for Unknown File Types</td>
<td>Scan</td>
</tr>
<tr>
<td>eps</td>
<td>EPS EPS Binary File</td>
<td>Scan</td>
</tr>
<tr>
<td>gil</td>
<td>GIF image data</td>
<td>Pass</td>
</tr>
</tbody>
</table>

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

Configuring Settings

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

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

Configuring a Disclaimer

You can create your own custom disclaimer notice.

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

Anti-Spam Logging and Monitoring

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

Anti-Spam status is monitored using SmartView Monitor. The Anti-Spam status appears under the Firewall product. The status contains information such as the Anti-Spam engine version. Anti-Spam status also includes statistics regarding scanned files. See also: Tracking and Reporting Options ("Anti-Spam Tracking and Reporting Options" on page 70).
Reporting False Positives to Check Point

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

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

1. Request the email session ID from the sender.
2. Open SmartView Tracker.
3. On the Log tab > Content-based Anti-Spam section locate the email session ID.
4. Open the Record Details and click Copy.
5. At the Check Point Support Center, open a Service Request and paste in the record details.

For more information on how to create and view Service Requests, refer to sk31615 (http://supportcontent.checkpoint.com/solutions?id=sk31615).

Anti-Spam Tracking and Reporting Options

Anti-Spam tracking and reporting options are available in:

- SmartView Tracker
- SmartView Monitor
- SmartReporter

SmartView Tracker

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

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

```
No.  Date       Time   Origin    Service   Source   Destination
5441 3Sep2007   9:17:26  spam:plot  smtp      checkpoint... spam:plot  1
5442 3Sep2007   9:17:26  spam:plot  smtp      checkpoint... spam:plot  1
5443 3Sep2007   9:17:26  spam:plot  smtp      checkpoint... spam:plot  1
5444 3Sep2007   9:17:26  spam:plot  smtp      checkpoint... smtp:server  1
```

SmartView Monitor

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

SmartReporter

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

- Anti-Virus
- Anti-Spam
Index

A
Accessing the Threat Wiki • 56, 59
Action • 25, 46
Adaptive Continuous Download • 64
Adding a New Host Site • 45
Adding a Server Certificate • 43
Adding Exception Groups to the Rule Base • 27
Adding Exceptions to Exception Groups • 27
Adding Trusted CAs for Outbound HTTPS Inspection • 47
Advanced Settings for Anti-Bot and Anti-Virus • 28
Analyzing Threats • 9
Anti-Bot and Anti-Virus Event Queries • 61
Anti-Bot and Anti-Virus in SmartEvent • 58
Anti-Bot and Anti-Virus in SmartView Tracker • 55
Anti-Bot and Anti-Virus Licensing and Contracts • 10
Anti-Bot and Anti-Virus Logs • 56
Anti-Bot and Anti-Virus Reports • 60
Anti-Bot Settings • 21, 28
Anti-Spam • 63
Anti-Spam and Mail • 62
Anti-Spam Logging and Monitoring • 69
Anti-Spam on UTM-1 Edge Devices • 66
Anti-Spam Tracking and Reporting Options • 70
Anti-Virus Settings • 21
Archive File Handling • 38
Automatically Updating the Trusted CA List and Certificate Blacklist • 47

B
Blade • 46
Blade Queries • 53
Blocking Bots and Viruses • 12
Bridge Mode and Anti-Spam • 67
Bypassing HTTPS Inspection to Software Update Services • 47

C
Certificate • 46
Certificate Blacklisting • 50
Check Point Information • 11
Check Point Online Web Service • 28
Comparing Scan by File Direction and by IPs • 30
Comparing Scan by File Direction and by IPs for FTP Protocol • 32
Comparing Scan by File Direction and by IPs for HTTP Protocol • 33
Comparing Scan by File Direction and by IPs for POP3 Protocol • 32
Comparing Scan by File Direction and by IPs for SMTP Protocol • 31
Configuring a Block List • 65
Configuring a Content Anti-Spam Policy • 64
Configuring a Disclaimer • 69
Configuring an Allow List • 66
Configuring an IP Reputation Policy • 65
Configuring Anti-Spam • 64
Configuring Anti-Spam POP3 • 66
Configuring Anti-Spam SMTP • 66
Configuring Anti-Virus Protection for Mail • 67
Configuring File Types • 37, 69
Configuring Inbound HTTPS Inspection • 42
Configuring Mail Anti-Virus • 67
Configuring Mail Traditional Anti-Virus • 36
Configuring Network Exceptions • 66
Configuring Outbound HTTPS Inspection • 40
Configuring Security Gateway Settings • 37
Configuring Settings • 69
Configuring SMTP and POP3 • 68
Configuring SMTP, POP3, FTP and HTTP • 36
Configuring Traditional Anti-Virus • 36
Configuring Zero Hour Malware • 36
Configuring Zero Hour Malware Protection • 68
Connecting to the Internet for Updates • 17
Connection Unification • 28
Continuous Download • 35
Converting Exceptions into an Exception Group • 24
Copying an Exception to an Exception Group • 24
Copying Profiles • 22
Creating an Anti-Bot and Anti-Virus Policy • 11
Creating an Outbound CA Certificate • 40
Creating Exception Groups • 27
Creating Exceptions from Logs or Events • 27
Creating Profiles • 20
Creating Rules • 12

D
Database Updates • 30
Definitions • 30
Deleting Profiles • 22
Deploying Certificates by Using Group Policy • 42
Destination • 44
Disabling a Protection on a Specified Server • 13

E
Enabling HTTPS Inspection • 40
Enabling the Anti-Bot and Anti-Virus Software Blades • 11
Enabling Traditional Anti-Virus • 29
Engine Settings • 28
Event Analysis in SmartEvent • 53
Event Analysis in SmartEvent or SmartEvent Intro • 58
Exception Groups Pane • 26
Exception Rules • 23
Exporting a Certificate from the Security Management Server • 41
Exporting and Deploying the Generated CA • 42

F
Fail Mode • 29
File Handling • 38
File Type Recognition • 35