Application Control and URL Filtering

R75.40

Administration Guide

13 August 2013
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=13943)
To learn more, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the home page at the Check Point Support Center (http://supportcontent.checkpoint.com/solutions?id=sk67581)

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 August 2013</td>
<td>Removed reference to CPMSI_Tool</td>
</tr>
<tr>
<td></td>
<td>Improved formatting and document layout</td>
</tr>
<tr>
<td>05 June 2012</td>
<td>Updated HTTPS Inspection in SmartView Tracker (on page 44)</td>
</tr>
<tr>
<td>09 May 2012</td>
<td>Updated the export CA certificate command syntax (&quot;Exporting a Certificate from the Security Management Server&quot; on page 34)</td>
</tr>
<tr>
<td>16 April 2012</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 Application Control and URL Filtering R75.40 Administration Guide).
Engine Settings ..................................................................................................46
Fail Mode ............................................................................................................47
Check Point Online Web Service ....................................................................47
Connection Unification .....................................................................................47
Web Browsing ....................................................................................................48
Application Control Backwards Compatibility .............................................48
Application and URL Filtering and Identity Awareness ..................................48
Using Identity Awareness in the Application and URL Filtering Rule Base ....48
Identifying Users Behind a Proxy ....................................................................49
Legacy URL Filtering ......................................................................................50
Terminology ....................................................................................................50
Architecture ....................................................................................................50
Configuring Legacy URL Filtering ..............................................................51

Application Control and URL Filtering in SmartView Tracker ..................52
Log Sessions ....................................................................................................52
Application Control and URL Filtering Logs ................................................52
Viewing Logs ..................................................................................................53
Predefined Queries ........................................................................................53
Permissions for Logs ......................................................................................53

Application Control and URL Filtering in SmartEvent ..............................55
Event Analysis in SmartEvent or SmartEvent Intro ......................................55
Viewing Information in SmartEvent .............................................................55
Viewing Information in SmartEvent Intro ....................................................56
The SmartEvent Intro Overview Page ............................................................56
Application Control and URL Filtering Event Queries ...............................56

Configuring UserCheck ................................................................................58
Configuring the Security Gateway for UserCheck ........................................58
UserCheck CLI ................................................................................................59
Revoking Incidents ........................................................................................60

UserCheck Client ...........................................................................................61
UserCheck Client Overview .............................................................................61
UserCheck Requirements ................................................................................61
Enabling UserCheck Client .............................................................................61
Client and Gateway Communication ............................................................62
Option Comparison ........................................................................................62
File Name Based Server Discovery .............................................................63
Active Directory Based Configuration ..........................................................64
DNS Based Configuration ..............................................................................66
Getting the MSI File .......................................................................................68
Distributing and Connecting Clients .............................................................68
UserCheck with Check Point Password Authentication ...............................69

Helping Users .................................................................................................70

Setting up a Mirror Port ................................................................................71
Technical Requirements ................................................................................71
Configuring a Mirror Port ...............................................................................71
Connecting the Gateway to the Traffic .........................................................72
Configuring the Interface as a Mirror Port ....................................................72
Checking that it Works ....................................................................................72
Removing the Mirror Port .............................................................................72

Index ..............................................................................................................73
Chapter 1

Introduction to Application Control and URL Filtering

In This Chapter

The Need for Application Control 6
The Need for URL Filtering 6
The Check Point Solution for Application Control and URL Filtering 7
Main Features 7
Glossary 8

The Need for Application Control

The wide adoption of social media and Web 2.0 applications changes the way people use the Internet. More than ever, businesses struggle to keep up with security challenges.

The usage of internet applications creates a new set of challenges. For example:

- **Malware threats** - Application use can open networks to threats from malware. Popular applications like Twitter, Facebook, and YouTube can cause users to download viruses unintentionally. File sharing can easily cause malware to be downloaded into your network.

- **Bandwidth hogging** - Applications that use a lot of bandwidth, for example, streaming media, can limit the bandwidth that is available for important business applications.

- **Loss of Productivity** - Employees can spend time on social networking and other applications that can seriously decrease business productivity.

Employers do not know what employees are doing on the internet and how such use affects them.

The Need for URL Filtering

As with Application Control, access to the internet and non-work-related website browsing can open networks to a variety of security threats and have a negative effect on employee productivity.

You can use URL Filtering to:

- Control employee internet access to inappropriate and illicit websites
- Control bandwidth issues
- Decrease legal liability
- Improve organizational security

When URL Filtering is set, employee data is kept private when attempting to determine a site category. Only the host part of the URL is sent to the Check Point Online Web Service. This data is also encrypted.
The Check Point Solution for Application Control and URL Filtering

Check Point Firewall innovation brings the industry's strongest URL Filtering, application and identity control to organizations of all sizes. You can easily create Policies which detect or block thousands of applications and internet sites.

Use the Application Control and URL Filtering blades to:

• **Learn about the applications**  
  Use the Check Point comprehensive AppWiki to understand what applications are used for and what their risk levels are.

• **Create a Granular Policy**  
  Make rules to allow or block applications or internet sites, by individual application, application or URL categories, or risk levels. When you use Identity Awareness, you can easily make rules for individuals or different groups of users. You can also create an HTTPS Policy that enables the Security Gateway to inspect HTTPS traffic to prevent security risks related to the SSL protocol.

• **Learn What Your Employees are Doing**  
  Use SmartView Tracker and SmartEvent to understand the application and site traffic that really occurs in your environment. Then change the Policy to make it even more effective. Only administrators that have been assigned with applicable permissions can see all the fields in a log. Using these permissions makes sure that restricted data is kept private in logs and cannot be seen by all administrators.

• **Keep Your Policies Updated**  
  The Application and URL Filtering Database is updated regularly with applications and site categories to help you keep your Policy current. The Security Gateway connects to the Check Point Online Web Service to identify social networking widgets and website categories for URLs that it does not recognize. Results are stored on a local cache on each Security Gateway. Subsequent uncategorized URLs are first checked against the local cache before querying the Check Point Online Web Service.

• **Custom Applications, Sites, Categories and Groups**  
  You can create applications, websites, categories and groups that are not in the Application and URL Filtering Database for use in the Policy. Use these custom objects to create a Rule Base that meets your organization requirements. You can contact Check Point to create customized application signatures to be imported into the database. These signatures contain a database of internal applications that are not necessarily web-based.

Main Features

• **Granular Application Control** – Identify, allow, or block thousands of applications and internet sites. This provides protection against the increasing threat vectors and malware introduced by internet applications and sites.

• **Largest application library with AppWiki** – Comprehensive application control that uses the industry's largest application library. It scans for and detects more than 4,500 applications and more than 100,000 Web 2.0 widgets and categories.

• **Integrated into Security Gateways** - Activate Application Control and URL Filtering on Security Gateways including UTM-1, Power-1, IP Appliances, and IAS Appliances.

• **Central Management** – Lets you centrally manage security Policies for Application Control and URL Filtering from one user-friendly console for easy administration.

• **SmartEvent Analysis** - Use SmartEvent advanced analysis capabilities to understand your application and site traffic with filtering, charts, reporting, statistics, and more, of all events that pass through enabled Security Gateways.
Glossary

- **Applications** - Applications include:
  - Programs you install on a desktop, for example Microsoft Office.
  - Programs you use through a browser, for example Google chat.
  - Social Network widgets that reside in social networking sites, for example Farmville on Facebook.
- **Site** - A site which can be accessed via a web browser.
- **Primary Category** - Group of applications with a common defining aspect. Each application has one primary category which is the most defining aspect of the application. See the category in the application descriptions and in the logs. When URL Filtering is enabled, categories also define a group of URLs or patterns of URLs.
- **Additional Categories** - Characteristics of the application. In the Application and URL Filtering Database, applications can have multiple categories. For example, Gmail categories include: Supports File Transfer, Sends mail, and Instant Chat. You can include categories in rules in the Rule Base. If a category is in a rule, the rule matches all applications and sites that are marked with that category. For example if you block the "Sends mail" category: Gmail, Yahoo! Mail, and others will be blocked.
- **Bytes** - As used in Application Control, it means the quantity of bytes of traffic. It does not mean the rate of bytes transferred for a specific unit of time.
- **AppWiki** - The searchable Check Point application database that shows a description, risk level, primary and additional categories. In the AppWiki, additional categories are called tags.
- **Matched Category** - The category that was matched by the URL Filtering rulebase.
Chapter 2

Getting Started

In This Chapter

Application Control and URL Filtering Licensing and Contracts 9
Enabling Application Control on a Security Gateway 9
Enabling URL Filtering on a Security Gateway 9
Creating an Application Control and URL Filtering Policy 10

It is easy to get started with Application Control and URL Filtering after you install and configure your R75.40 environment. Application Control can be enabled on R75 or higher gateways and URL Filtering can be enabled on R75.20 or higher gateways.

Application Control and URL Filtering Licensing and Contracts

Make sure that each Security Gateway has a Security Gateway license and an Application Control contract and/or URL Filtering contract. For clusters, make sure you have a contract and license for each cluster member.

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

If you do not have a valid contract for a Security Gateway, the Application Control blade and/or URL Filtering blade is disabled. When contracts are about to expire or have already expired, you will see warnings. Warnings show in:

- The Message and Action Items section of the Overview pane of the Application and URL Filtering tab.
- The Check Point User Center when you log in to your account.

Enabling Application Control on a Security Gateway

Enable the Application Control Software Blade on each Security Gateway.

To enable the Application Control Software Blade on a Security Gateway:

1. In SmartDashboard, right-click the Security Gateway object and select Edit.
   The Gateway Properties window opens.
3. Click OK.
4. Install the Policy.

After you enable Application Control, you can see logs that relate to application traffic in SmartView Tracker and SmartEvent. These logs show how applications are used in your environment and help you create an effective Rule Base.

Enabling URL Filtering on a Security Gateway

Before you enable the URL Filtering Software Blade, make sure a DNS has been configured in the environment. If you have a proxy server in your network, make sure it is defined on the Security Gateway or in the management environment.
To enable the URL Filtering Software Blade on a gateway:
1. In SmartDashboard, right-click the Security Gateway object and select Edit.
   The Gateway Properties window opens.
3. Click OK.
4. Install the Policy.

Creating an Application Control and URL Filtering Policy

Create and manage the Policy for Application Control and URL Filtering in the Application and URL Filtering tab of SmartDashboard. The Policy defines which users can use specified applications and sites from within your organization and what application and site usage is recorded in the logs.

- 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 Application Control and URL Filtering Policy. Click the Add Rule buttons to get started.
- Look through the AppWiki to learn which applications and categories have high risk levels. Find ideas of applications and categories to include in your Policy.

Creating Rules

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

Monitoring Applications

Scenario: I want to monitor all Facebook traffic in my organization. How can I do this?

To monitor all Facebook application traffic:
1. In the Application and URL Filtering tab of SmartDashboard, open the Policy page.
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 Facebook.
   - Source - Keep it as Any so that it applies to all traffic from the organization.
   - Destination - Keep it as Internet so that it applies to all traffic going to the internet or DMZ.
   - Applications/Sites - Click the plus sign to open the Application viewer. Add the Facebook application to the rule:
     - Start to type "face" in the Search field. In the Available list, see the Facebook application.
Click each item to see more details in the description pane.
Click the checkboxes of the items to add to the rule.

- **Action** - Keep it as **Allow**.
- **Track** - Keep it as **Log**
- **Install On** - Keep it as **All** or choose specified Security Gateways to install the rule on.

The rule allows all Facebook traffic but logs it. You can see the log data in SmartView Tracker and SmartEvent to monitor how people use Facebook in your organization.

### Blocking Applications

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

**To block an application or category of applications, such as pornography, in your organization:**

1. In the Application and URL Filtering 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:
   - **Applications/Sites** - Pornography category
   - **Action** - Block, and optionally, a UserCheck **Blocked Message**. The message informs users that their actions are against company policy and can include a link to report if the website is included in an incorrect category.
   - **Track** - Log

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Applications/Sites</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Pornography</td>
<td>Any</td>
<td>Internet</td>
<td>Pornography</td>
<td>Block Block Message</td>
<td>Log</td>
<td>All</td>
</tr>
</tbody>
</table>

The rule blocks traffic to pornographic sites and logs attempts access sites that are in the pornography category. Users who violate the rule receive a customizable UserCheck message that informs them that the application is blocked according to company security policy. The message can include a link to report if the website is included in an incorrect category.

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

### Limiting Application Traffic

**Scenario:** I want to limit my employees’ access to streaming media so that it does not impede business tasks.

If you do not want to block an application or category, there are two ways to set limits for employee access:

- Add a **Limit** object to a rule to limit the bandwidth that is permitted for the rule.
- Add one or more **Time** objects to a rule to make it active only during specified times.

The example rule below:

- Allows access to streaming media during non-peak business hours only.
- Limits the upload and download throughput for streaming media in the company to 1 Gbps.

**To create a rule that allows streaming media with time and bandwidth limits:**

1. In the Application and URL Filtering 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:
   - **Applications/Sites - Media Streams** category.
   - **Action** - Allow, and a **Limit** object that specifies the maximum upload and download throughput.
   - **Time** - Add a **Time** object that specifies the hours or time period in which the rule is active.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Applications/Sites</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit Streaming Media</td>
<td>Any</td>
<td>Internet</td>
<td>Media Streams</td>
<td>Allow</td>
<td>Log</td>
<td>All</td>
<td>Non-peak</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Upload_1Gbps</td>
<td>Up: 1 Gbps</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Using Identity Awareness Features in Rules**

**Scenario:** I want to allow a Remote Access application for a specified group of users and block the same application for other users. I also want to block other Remote Access applications for everyone. How can I do this?

If you enable Identity Awareness on a Security Gateway, you can use it together with Application Control to make rules that apply to an **access role**. Use access role objects to define users, machines, and network locations as one object.

In this example:

- You have already created an Access Role that represents all identified users in the organization. You can use this to allow access to applications only for users who are identified on the Security Gateway.
- You want to allow access to the Radmin Remote Access tool for all identified users.
- You want to block all other Remote Access tools for everyone within your organization. You also want to block any other application that can establish remote connections or remote control.

To do this, add two new rules to the Rule Base:

1. Create a rule and include these components:
   - **Source** - The ** Identified_Users** access role
   - **Destination** - Internet
   - **Action** - Allow
   - **Applications/Sites** - Radmin

2. Create a rule below the rule from step 1. Include these components:
   - **Source** - Any
   - **Destination** - Internet
   - **Applications/Sites** - The category: **Remote Administration Tool**
   - **Action** - Block

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Applications/Sites</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Radmin to Identified Users</td>
<td>Identified_users</td>
<td>Internet</td>
<td>Radmin</td>
<td>Allow</td>
<td>None</td>
<td>All</td>
</tr>
<tr>
<td>Block other Remote Admin</td>
<td>Any</td>
<td>Internet</td>
<td>Remote Administration Tool</td>
<td>Block</td>
<td>Log</td>
<td>All</td>
</tr>
</tbody>
</table>

**Notes on these rules:**

- Because the rule that allows Radmin is above the rule that blocks other Remote Administration tools, it is matched first.
- The Source of the first rule is the Identified Users access role. If you use an access role that represents the Technical Support department, then only users from the technical support department are allowed to use Radmin.
Getting Started

For more about Access Roles and Identity Awareness, see the R75.40 Identity Awareness Administration Guide.

Blocking Sites

Scenario: I want to block sites that are associated with categories that can cause liability issues. Most of these categories exist in the Application and URL Filtering Database but there is also a custom defined site that must be included. How can I do this?

You can do this by creating a custom group and adding all applicable categories and the site to it. If you enable Identity Awareness on a Security Gateway, you can use it together with URL Filtering to make rules that apply to an access role. Use access role objects to define users, machines, and network locations as one object.

In this example:

- You have already created an Access Role that represents all identified users in the organization.
- You want to block sites that can cause liability issues for everyone within your organization.
- You will create a custom group that includes Application and URL Filtering Database categories as well as a previously defined custom site named Smirnoff.

To create a custom group:

1. In the Application and URL Filtering tab of SmartDashboard, open the Applications/Sites pane.
2. Click New > Applications/Sites Group.
3. Give the group a name. For example, Liability_Sites.
4. Add the group members:
   - Filter by Categories (make sure only the Categories button is selected) and select the checkboxes of all the related categories in the Application and URL Filtering Database.
   - Filter by Custom (click the Categories button to clear it and select Custom) and select the custom application.
5. Click OK.
   
   The categories and custom site are shown in the group members list.

6. Click OK.
   
   The group is added to the Applications/Sites list. You can now use it in the Rule Base

In the Rule Base, add a rule similar to this:

- Create a rule and include these components:
  - Source - The Identified_Users access role
• Destination - Internet
• Applications/Sites - Liability_Sites
• Action - Block

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Applications/Sites</th>
<th>Action</th>
<th>Track</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block sites that may cause a liability</td>
<td>Identified_Users</td>
<td>Internet</td>
<td>Liability_Sites</td>
<td>Block</td>
<td>Log</td>
</tr>
</tbody>
</table>

**Blocking URL Categories**

*Scenario: I want to block pornographic sites. How can I do this?*

You can do this by creating a rule that blocks all sites with pornographic material with the *Pornography category*. If you enable Identity Awareness on a Security Gateway, you can use it together with URL Filtering to make rules that apply to an *access role*. Use access role objects to define users, machines, and network locations as one object.

In this example:

- You have already created an Access Role that represents all identified users in the organization.
- You want to block sites related to pornography.

**In the Rule Base, add a rule similar to this:**

- Create a rule and include these components:
  - **Source** - The *Identified_Users* access role
  - **Destination** - Internet
  - **Applications/Sites** - Pornography category
  - **Action** - Block
Chapter 3

Managing Application Control and URL Filtering

In This Chapter

The Policy Rule Base 15
The Application and URL Filtering Database 25
The Application and URL Filtering Overview Pane 28
AppWiki 29
Gateways Pane 29
Applications/Sites Pane 29
Advanced Settings for Application and URL Filtering 31
HTTPS Inspection 32
Engine Settings 46
Application and URL Filtering and Identity Awareness 48
Legacy URL Filtering 50

You configure Application Control and URL Filtering in SmartDashboard. SmartView Tracker shows the logs and SmartEvent shows real-time traffic statistics and analysis. This chapter explains the Application Control and URL Filtering configuration and management that you do in SmartDashboard.

The Policy Rule Base

The Application Control and URL Filtering Policy determines who can access which applications and sites from an organization. The primary component of the Policy is the Rule Base. The rules use the Application and URL Filtering Database, network objects and custom objects (if defined).

If you enable Identity Awareness on your Security Gateways, you can also use Access Role objects as the source in a rule. This lets you easily make rules for individuals or different groups of users. You cannot use a regular network object and an access role together in one field. For example, you can have the source of Rule 4 as an Access Role and the Destination as an Address Range. But you cannot have an Access Role and an Address Range together in the Source field.

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

For examples of how to create different types of rules, see Creating Application Control Rules ("Creating Rules" on page 10).

Default Rule and Monitor Mode

When you enable Application Control, a default rule is added to the Rule Base that allows all traffic from known applications and sites, with the tracking set to Log.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Applications/Sites</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Internet</td>
<td>Any Recognized</td>
<td>Allow</td>
<td>Log</td>
<td>All</td>
</tr>
</tbody>
</table>

The result of this rule is that all application traffic is monitored. Therefore, you can see logs related to application traffic in SmartView Tracker and SmartEvent. Use the data there to better understand the use of applications in your environment and create an effective Rule Base.
If you enabled Identity Awareness on the Security Gateway, you will also see names of identified users in the logs.

If you do not add other rules to the Rule Base, your Application Control Policy stays in monitor mode. This means that you see application traffic in the logs but do not block access to applications.

If you change the default rule, for example:

- You change the tracking to none
- You change the value in Applications/Sites from **Any Recognized** to a specified application,

Then no traffic will be monitored.

You can add more rules that block specified applications or sites or have different tracking settings. But if you do not change the default rule, traffic that is not included in other rules is allowed and monitored.

**Parts of the Rules**

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

<table>
<thead>
<tr>
<th>No.</th>
<th>Hits</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Applications/Sites</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>Allow HR to browse MyHR.com site</td>
<td>ERA</td>
<td>Internet</td>
<td>MyHR.com</td>
<td>Inform</td>
<td>Log</td>
<td>All</td>
<td>Any</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Block sites which may pose a security risk</td>
<td>ERA</td>
<td>Internet</td>
<td>Potential Liability</td>
<td>Block</td>
<td>Log</td>
<td>All</td>
<td>Any</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Block high risk applications</td>
<td>ERA</td>
<td>Internet</td>
<td>High Risk</td>
<td>Block</td>
<td>Log</td>
<td>All</td>
<td>Any</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Block multimedia</td>
<td>ERA</td>
<td>Internet</td>
<td>Anonymous</td>
<td>Block</td>
<td>Log</td>
<td>All</td>
<td>Any</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Allow TeamViewer application for specific user - ticket #88721</td>
<td>ERA</td>
<td>Internet</td>
<td>John Adams, Role</td>
<td>Allow</td>
<td>Log</td>
<td>All</td>
<td>Any</td>
</tr>
</tbody>
</table>

**Number (NO.)**

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

For example, Gmail additional categories include **Sends Mail**, **Transmits Personal or Enterprise Information**, and **Instant Chat**. If rule 3 allows Gmail and rule 4 blocks applications with the **Instant Chat** additional category, Gmail will be allowed based on rule 3.

**Hits**

Hit Count tracks the number of connections that each rule matches. For each rule in the Rule Base, the Hits column shows by default a visual indicator of matching connections together with the number of hits in K (thousands), M (millions), G (billions), or T (trillions). You can configure to show the percentage of the rule's hits from total hits, the indicator level (very high, high, medium, low, or zero) and set a timeframe for the data that is shown. These options are configured from the Firewall Rule Base by right-clicking the Hits column header or the rule number.

See Hit Count (on page 20).

**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.

Applications/Sites

The Applications/Sites column contains the applications and categories for sites and applications that you choose to include. One rule can include multiple items and items of different types. For example, one rule can include 2 applications and 3 categories. The default is that the rule applies to all known applications and sites. The category on which the rule is matched is shown in the SmartView Tracker logs in the Matched Category field.

You can also include widgets and custom defined applications, sites, categories and groups. Custom defined items are set in SmartDashboard by the administrator and are not a part of the Application and URL Filtering Database.

This application includes all HTTP traffic that is not a defined application. Because Web Browsing traffic can generate a lot of logs, the Web browsing application has its own activation setting. You can activate Web Browsing in Advanced > Engine Settings.

To add applications or categories to a rule:

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

- To add an item to the rule, click the checkbox in the Available list.
- To see the details of an item without adding it to the rule, click the name of the Available item.
- You can select an application or category to add to the rule from the Available list.
- To filter the Available list by categories, applications, custom-defined items or widgets, click the buttons in the toolbar of the viewer. The Available list shows the filtered items and then you can add items to the rule.
- To see all applications in a risk level, select the level from the Risk field in the toolbar.
- If you know the name of an application or category, you can search for it. The results show in the Available list.
- To add a new category, application or site, or application or site group, use the New button.
### Action

Action refers to what is done to the traffic. Click in the column to see the options and select an action to add to the rule.

<table>
<thead>
<tr>
<th>Action</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>Allows the traffic</td>
</tr>
<tr>
<td>Inform</td>
<td>Sends a message to the user attempting to access the application</td>
</tr>
<tr>
<td>Ask</td>
<td>Asks the user a question and adds a confirmatory check box, or a reason box.</td>
</tr>
<tr>
<td>Block</td>
<td>Blocks the traffic. If no UserCheck object is defined for this action, no page is displayed.</td>
</tr>
<tr>
<td>Limit</td>
<td>Limits the bandwidth that is permitted for a rule. Add a Limit object (&quot;Limit Objects&quot; on page 20) to configure a maximum throughput for uploads and downloads.</td>
</tr>
<tr>
<td>User Check Frequency</td>
<td>Configure how often the user should see the configured message when the action is ask, inform, or block.</td>
</tr>
<tr>
<td>Edit User Check Message</td>
<td>Opens the User Check message for editing</td>
</tr>
<tr>
<td>Captive Portal</td>
<td>Redirects http traffic to an authentication (captive) portal. Once the authentication credentials are obtained, further connections from this source are inspected without requiring authentication.</td>
</tr>
<tr>
<td>Rule Actions</td>
<td>From the toolbar at the top of the Application Control Policy page, click the icons to create new rules or to delete the selected rules. If you right-click in a column of the Rule Base and select Rule Actions, a menu opens with these options:</td>
</tr>
<tr>
<td>• New Rule</td>
<td>Select to create a new rule Above or Below the rule that is currently selected.</td>
</tr>
<tr>
<td>• Delete Rule</td>
<td>Deletes the selected rule or rules.</td>
</tr>
<tr>
<td>• Disable Rule</td>
<td>The rule stays in the Rule Base but is not active.</td>
</tr>
<tr>
<td>• Select All Rules</td>
<td>Selects all the rules and you can then choose another action to apply to them.</td>
</tr>
<tr>
<td>• View rule logs in SmartView Tracker</td>
<td>Opens SmartView Tracker and shows logs related to the rule.</td>
</tr>
<tr>
<td>• View rule logs in SmartEvent</td>
<td>Opens SmartEvent and shows logs related to the rule.</td>
</tr>
</tbody>
</table>

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

**Note** - The actions Block, Ask, and Inform involve the creation of UserCheck Interaction Objects.

### 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
- **Logs**
Managing Application Control and URL Filtering

- **Log** - Records the event details in SmartView Tracker. This option is useful to get general information on your network traffic. It consolidates logs by session (there is one log for each session). It shows the initial URL browsed and the number of suppressed logs it includes.

- **Extended Log** - Consolidates logs by session, shows the number of suppressed logs and includes data for each URL request in the session time frame. Each of the URLs has an entry in the **URLs** tab of the log in SmartView Tracker. Using this option can have an effect on performance.

- **Complete Log** - Records logs for each URL request made regardless of session. Each URL request has its own log. This option also generates an event in SmartEvent for each URL browsed and is intended only for troubleshooting purposes. Note that this option generates many logs.

  For more about logs, see log sessions (on page 52).

- **Account** - Records the event in SmartView Tracker with byte information.

- **Alert** - Logs the event and runs 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**.

**Install On**

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

**Time**

You can add a **Time** object to a rule to make the rule active only during specified times. If you do not include a Time object in a rule, the rule is always active.

You can include multiple Time objects in a rule in these ways:

- Select each Time object to include it.
- Create a **Time Group** that includes multiple Time objects.

When you have multiple Time objects or a Time Group, each Time object works independently. For example, if a rule has two Time objects:

- One shows that the rule is active on Mondays.
- One shows that the rule is active from 9:00 - 17:00.

The rule is active each day from 9:00 - 17:00 and all day on Mondays. For the rule to be active from 9:00 - 17:00 on Mondays only, make one Time object that contains all of the criteria.

If Time objects were created from a different tab in SmartDashboard, you can also use them in the Application Control and URL Filtering Rule Base. For example, you can create Time objects from the Firewall Rule Base or from **Manage menu > Time**.

**To add Time objects to a rule:**
1. In the **Time** column of a rule, right click and select **Add Objects**.
2. Select from the available objects and click **OK**.

**To create a new Time object from the Application Control and URL Filtering Rule Base:**
1. In the **Time** column of a rule, right click and select **Add Objects**.
2. Click **New** and select Time.
3. In the **General** pane, enter a **Name** without spaces.
4. In the **Time** pane, select one or more options:
Managing Application Control and URL Filtering

- **Time Period** - Select a date and time when the rule starts to be active and expires.
- **Restrict to specific hour ranges** - Select hours of the day when the rule is active.
- **Specify Days** - Select days of the week or month when the rule is active. The default is **Every Day**.

5. Click **OK**.
6. Click **OK** to add the object to the selected rule.

**Note** - The relevant time zone is that of the Security Gateway enforcing the rule. If Security Gateways are in different time zones, they enforce the same time object rules at different times.

**Limit Objects**

Use the **Limit** action in rules to limit the bandwidth that is permitted for a rule in the Application Control and URL Filtering Rule Base. Configure a maximum throughput for uploads and downloads. The Limit action makes sure that employee use of the internet does not impede important business tasks.

You can add one Limit object to a rule. It can include upload and download rates.

- **Download** - From the internet to the organization.
- **Upload** - From the organization to the internet.

When the limit is reached, the gateway begins to drop packets. The Application Control logs show dropped packets.

**To add a Limit object to a rule:**

1. In the Application Control and URL Filtering Rule Base, right-click in the **Action** column and select **Limit**.
2. Select a limit to add from the list shown or select **New Limit** to create a new Limit object.
3. if creating a new Limit object, in the **Limit Properties** window:
   - Enter a **Name** without spaces.
   - Select **Download**, **Upload**, or the two of them.
   - For each selected option, select a number and unit to define the maximum permitted bandwidth for that action.

4. Click **OK**.
   - The Limit is added to the rule.

   **Note** - The Security Gateway implements the Limit action by dropping successive packets which exceed the allowed bandwidth.

**Hit Count**

Hit Count tracks the number of connections that each rule matches. For each rule in the Rule Base, the Hits column shows by default a visual indicator of matching connections together with the number of hits.

You can configure to show the percentage of the rule hits from total hits, the indicator level (very high, high, medium, low, or zero) and set a timeframe for the data that is shown. These options are configured in the Firewall Rule Base and affect the display in other supported Software Blades.

When you enable Hit Count, the Security Management Server collects the data from supported Security Gateways. Hit Count works independently from logging. It is not necessary to set the **Track** option for each rule to **Log**. Hit count works even if the **Track** option is **None**.

With the data you see in the Rule Base Hits column, you can:

- Make the Rule Base more efficient - You can delete rules that have no matching connections. Note that if you see a rule with a zero hit count it only means that in the Security Gateways enabled with Hit Count there were no matching connections. Other Security Gateways can possibly have matching connections.
- Improve Rule Base performance - In the Firewall Rule Base you can move a rule that has a high hit count to a higher position (one of the first rules) in the Rule Base.
- Better understand the behavior of the policy.
Enabling or Disabling Hit Count

By default, Hit Count is globally enabled for all supported Security Gateways (from R75.40). If it is necessary to disable the Hit Count feature for a specified Security Gateway, you can do it from the gateway's properties. The timeframe setting that defines the data collection time range is configured globally.

After you enable or disable Hit Count you must install the Policy for the Security Gateway to start or stop collecting data.

To enable or disable Hit Count globally:
1. From the Policy menu, select Global Properties.
2. Select Hit Count from the tree.
3. Select the options:
   - Enable Hit Count - Select to enable or clear to disable all Security Gateways to monitor the number of connections each rule matches.
   - Keep Hit Count data up to - Select one of the time range options. The default is 6 months. Data is kept in the Security Management Server database for this period and is shown in the Hits column.
4. Click OK.
5. Install the policy.

To enable or disable Hit Count on each Security Gateway:
1. From the Gateway Properties of the Security Gateway, select Hit Count from the tree.
2. Select Enable Hit Count to enable the feature or clear the checkbox to disable it.
3. Click OK.
4. Install the policy.

Configuring the Hit Count Display

These are the options you can configure for how matched connection data is shown in the Hits column:

- **Value** - Shows the number of matched hits for the rule from supported Security Gateways. Connection hits are not accumulated in the total hit count for:
  - Security Gateways that are not supported (versions before R75.40)
  - Security Gateways that have disabled the hit count feature

  The values are shown with these letter abbreviations:
  - K = 1,000
  - M = 1,000,000
  - G = 1,000,000,000
  - T = 1,000,000,000,000

  For example, 259K represents 259 thousand connections and 2M represents 2 million connections.

- **Percentage** - Shows the percentage of the number of matched hits for the rule from the total number of matched connections. The percentage is rounded to a tenth of a percent.

- **Level** - The hit count level is a label for the range of hits according to the table.
  The hit count range = Maximum hit value - Minimum hit value (does not include zero hits)

<table>
<thead>
<tr>
<th>Hit Count Level</th>
<th>Icon</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero</td>
<td>![Zero Icon]</td>
<td>0 hits</td>
</tr>
<tr>
<td>Low</td>
<td>![Low Icon]</td>
<td>Less than 10 percent of the hit count range</td>
</tr>
<tr>
<td>Medium</td>
<td>![Medium Icon]</td>
<td>Between 10 - 70 percent of the hit count range</td>
</tr>
<tr>
<td>High</td>
<td>![High Icon]</td>
<td>Between 70 - 90 percent of the hit count range</td>
</tr>
<tr>
<td>Very High</td>
<td>![Very High Icon]</td>
<td>Above 90 percent of the hit count range</td>
</tr>
</tbody>
</table>
To configure the Hit Count display:
1. Right-click the Hits column header or the rule number in the row.
2. From the menu, select Display.
3. Select one or more options:
   - Percentage
   - Value
   - Level

Configuring the Hit Count Timeframe
The values shown in the Hits column are based on the Timeframe setting. By default, the timeframe is cumulative according to the Keep Hit Count data up to parameter in the Global Settings. For example, if the parameter is configured to 6 months, the available timeframe options are 1 month, 3 months, and 6 months.

You can change the timeframe according to intervals based on the Global Settings parameter.

To configure the hit count timeframe:
1. Right-click the Hits column header or the rule number in the row.
2. From the menu, select Timeframe.
3. Select the timeframe.

Refreshing the Hit Count Data
Hit count data is transferred from the Security Gateways to the Security Management Server once every three hours for each rule. When you refresh the hit count data, you are getting updated data from the data in the Security Management Server database and not directly from the Security Gateways.

After you install a policy, the hit count is updated from each Security Gateway in the policy to the Security Management Server database. This is done once a minute for the first 3 minutes after the policy is installed.

To refresh hit count data in the Firewall Rule Base:
1. Right-click the Hits column header or the rule number in the row.
2. From the menu, select Hit Count > Refresh.

To refresh hit count data in the Application and URL Filtering Rule Base:
- Click Refresh Hits in the policy toolbar.

UserCheck Interaction Objects
UserCheck Interaction Objects add flexibility to Application and URL Filtering by giving the Security Gateway a mechanism to communicate with users. UserCheck objects are used in the Application and URL Filtering Rule Base to:
- Help users with decisions that can be dangerous to the organization's security.
- Share the organization's changing internet policy for web applications and sites with users, in real-time.

If a UserCheck object is set as the action on a policy rule, the user's browser redirects to the SecurePlatform Administration web portal on port 443 or 80. The portal hosts UserCheck notifications.

The UserCheck client adds the option to send notifications for applications that are not in a web browser, such as Skype, iTunes, or browser add-ons (such as radio toolbars). The UserCheck client can also work together with the UserCheck portal to show notifications on the computer itself when:
- The notification cannot be displayed in a browser, or
- The UserCheck engine determines that the notification will not be shown correctly in the browser and the Fallback Action for the UserCheck object is Allow.

For more about configuring UserCheck on the gateway and the UserCheck client, see Configuring UserCheck (on page 58).
Creating UserCheck Interaction Objects

Create a UserCheck Interaction object from the Rule Base or from the UserCheck page of the Application and URL Filtering tab. The procedure below shows how to create the object from the Rule Base.

To create a UserCheck object that includes a message:
1. In the Application & URL Filtering > Policy rule base > Action column, select one of these interaction modes:
   - Inform - Show an informative message users. Users can continue to the application or cancel the request.
   - Ask - Show a message to users that asks them if they want to continue with the request or not.
   - Block - Show a message to users and block the application request.
2. Select New UserCheck or one of the existing UserCheck Interaction objects.
   If you selected New UserCheck, the UserCheck Interaction window opens on the Message page.
3. Enter a name for the UserCheck object and, optionally, a comment.
4. Select a language (English is the default) from the Languages tabs.
5. Click the Add logo box to add a graphic, such as company logo.
   Note - The graphic must have a height and width of 176 x 52 pixels.
6. Click the text box adjacent to the picture and enter title text for the message.
   Note - Right-clicking inside any of the text boxes gives you the option to Switch to HTML mode and enter HTML code directly. Switching to HTML mode closes the formatting toolbar.
7. In the page title, message subject, and message body text boxes, enter the message content. You can:
   a) Use the formatting toolbar to change text color, alignment, add or remove bullets.
   b) Insert field variables for:
      - Application name
      - Category
      - Username
      - Original URL
      - Source IP
      - Incident ID
     Variables are replaced with applicable values when the (Block, Ask, Inform) action occurs and the message shows. The Username can only be displayed if the Identity Awareness blade is enabled.
   c) Use the Insert User Input variable to add a:
      - Confirm checkbox - Users select a checkbox to continue
      - Textual Input - Users can enter an explanation for their activity or other text according to the instructions. Edit the default text in the Textual Input box based on your business needs.
      - Wrong report category - Users can click a link to report that an incorrect category was included in the message. Use this field with the Category variable.
8. Optional: Click Preview in browser to see the results in your default browser.
9. Click OK.
   This creates the UserCheck object and web page notification for the portal.

UserCheck Frequency and Scope

You can set the number of times that users get UserCheck messages for accessing applications that are not permitted by the policy. You can also set if the notifications are based on accessing the rule, application category, or application itself.

To set how often UserCheck notifications show:
1. Select UserCheck Frequency from the Action column of a rule in the policy. The options are:
   - Once a day
   - Once a week
   - Once a month
   - Custom
2. Select a **UserCheck Scope** option from the **Action** column of a rule in the policy. This sets if the notifications are based on accessing the:

- For this rule
- For each category
- For each application

**Example:**

In a rule that contains:

<table>
<thead>
<tr>
<th>Applications/Sites</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Networking category</td>
<td>Inform</td>
</tr>
</tbody>
</table>

If you select **Once a day**, as the **UserCheck Frequency** and **For this rule** for **UserCheck Scope**:

A user who accesses Facebook and then LinkedIn on the same day gets one Inform message.

If you select **Once a day**, as the **UserCheck Frequency** and **For each application** for **UserCheck Scope**:

A user who accesses Facebook and then LinkedIn on the same day gets one Inform message for Facebook and one for LinkedIn.

In new installations, the **UserCheck Scope** default is **For each category**.

In upgrades from a version before R75.40, the **UserCheck Scope** default is **For this Rule**.

**More UserCheck Interaction Options**

For each UserCheck Interaction object you can configure these options from the UserCheck Interaction window:

- **Languages** - Select a default language for the message.
- **Fallback Action** - Select an alternative action (allow or block) for when the UserCheck notification cannot be shown in the browser or application that caused the notification. If UserCheck determines that the notification cannot be shown in the browser or application, the behavior is:
  - If the **Fallback Action** is **Allow** (the default for Inform messages), the user is allowed to access the website or application, and the UserCheck client (if installed) shows the notification.
  - If the **Fallback Action** is **Block**, the gateway tries to show the notification in the application that caused the notification. If it cannot and the UserCheck client is installed, it shows the notification through the client. The website or application is blocked, even if the user does not see the notification.
- **Redirect to External Portal** - Select this to redirect users to an external portal, not on the gateway.
  - **URL** - Enter the URL for the external portal. The specified URL can be an external system that obtains authentication credentials from the user, such as a user name or password. It sends this information to the gateway.
  - **Add UserCheck Incident ID to the URL query** - An incident ID is added to the end of the URL query.
- **Conditions** - Select actions that must occur before users can access the application. Select one or more of these options:
  - **User accepted and selected the confirm checkbox** - This applies if the UserCheck message contains a checkbox (**Insert User Input > Confirm Checkbox**). Users must accept the text shown and select the checkbox before they can access the application.
  - **User filled some textual input** - This applies if the UserCheck message contains a text field (**Insert User Input > Textual Input**). Users must enter text in the text field before they can access the application. For example, you might require that users enter an explanation for use of the application.
UserCheck Page

On the UserCheck page, you can create, edit, and preview UserCheck interaction objects and their messages.

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

These are the default UserCheck messages:

<table>
<thead>
<tr>
<th>Name</th>
<th>Action Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cancel Page</td>
<td>Cancel</td>
<td>Shows after a user gets an Inform or Ask message and clicks Cancel.</td>
</tr>
<tr>
<td>Blocked Message</td>
<td>Block</td>
<td>Shows when a request is blocked.</td>
</tr>
<tr>
<td>Access Notification</td>
<td>Inform</td>
<td>Shows when the action for the rule is inform. It informs users what the company policy is for that site.</td>
</tr>
<tr>
<td>Company Policy</td>
<td>Ask</td>
<td>Shows when the action for the rule is ask. It informs users what the company policy is for that site and they must click OK to continue to the site.</td>
</tr>
</tbody>
</table>

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

You can preview each message page in two views:

- **Regular view** - How it shows in a web browser on a PC or laptop.
- **Mobile Device** - How it shows in a web browser on a mobile device.

The Application and URL Filtering Database

The Check Point Application and URL Filtering Database contains more than 4,500 applications and about 96 million categorized URLs.

For URL Filtering, each Security Gateway also has:

- A local database that contains commonly used URLs and their related categorization.
- A local cache that gives answers to 99% of URL categorization requests. When the cache does not have an answer, only the host name is sent to the Check Point Online Web Service for categorization. This maintains user privacy since no user parameters are sent for the categorization procedure.

Upon rule match in the Rule Base, it is necessary to determine if the URL is an application and its related category. To do this the Security Gateway does these steps:

1. For URL Filtering: Goes to the local cache to see if the data is already there. If the category data is not in the cache, it checks the local database for the URL category.
   For Application Control: Matches locally stored signatures.
2. For Application Control and URL Filtering: If the URL is suspected to be a widget or the category data is not in the cache, the Security Gateway accesses the Check Point Online Web Service.

Each item has a description, a category, additional categories, and a risk level. You can include applications and categories in your Application Control and URL Filtering rules. When you have a valid Application Control and/or URL Filtering contract, the database is updated regularly with new applications, categories and social networking widgets. This lets you easily create and maintain an up to date Policy.

Access the Application and URL Filtering Database from:
• **SmartDashboard** - From the Application Control Rule Base in SmartDashboard, click the plus sign in the Application column, and the Application viewer opens. From there you can add applications and categories directly into the Rule Base.

• **AppWiki** - An easy to use tool to see the Application and URL Filtering Database. Open it from the AppWiki pane in the Application and URL Filtering tab or from the Check Point website (http://appwiki.checkpoint.com/appwiki/applications.htm).

### Security Category Updates

The local cache on each Security Gateway keeps URL categorization responses up to 3 days. In that time frame, it is possible that the initial categorization of a security category is updated on the Check Point Online Web Service. For example, a URL categorized as portal, is updated to phishing after 24 hours.

Changes made to URLs with security categories (such as phishing, malware, botnet, and spam) are updated in a security service list by the Check Point Online Web Service.

The local cache is updated on a regular basis depending on the category involved. For security related categories, such as phishing, there is a special update Policy that allows fast updates to occur.

### Application Categories

In the Application and URL Filtering Database, each application is assigned to one **primary category** based on its most defining aspect. See the category in the description of each application and in the logs.

In the Application and URL Filtering Database, each application can have **additional categories**, which are characteristics of the application. For example, some of the additional categories of Gmail include: Supports File Transfer, Sends mail, and Instant Chat. If an additional category is in a rule, the rule matches all applications that are marked with it.

*Note* - In the AppWiki, additional categories are called tags.

When you use the AppWiki or add applications to the Rule Base, you can filter by additional category or risk level to see all applications with that characteristic. This is a good way to get ideas of types of applications that you might want to block or allow.

If new applications are added to an additional category that is in an Application Control or URL Filtering rule, the rule is updated automatically when the database is updated.

### Application Risk Levels

The Application and URL Filtering Database and AppWiki show a Risk Level for each application. This table explains what each level means and gives examples of applications or types of applications with that level.

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Definition</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 - Critical</td>
<td>Can bypass security or hide identities</td>
<td>Tor, VTunnel</td>
</tr>
<tr>
<td>4 - High</td>
<td>Can cause data leakage or malware infection without user knowledge</td>
<td>Remote Desktop, File Sharing, P2P (uTorrent, Kazaa)</td>
</tr>
<tr>
<td>3 - Medium</td>
<td>Can be misused and cause data leakage or malware infection</td>
<td>Instant messaging, File Storage (Drop box), WebEx, Gmail</td>
</tr>
<tr>
<td>2- Low</td>
<td>Potentially not business related, but low risk</td>
<td>Gaming, Facebook, YouTube, Media</td>
</tr>
<tr>
<td>1- Very Low</td>
<td>Usually business related with no or very low risk</td>
<td>SalesForce, Google Finance</td>
</tr>
</tbody>
</table>

You can filter a search based on the risk level. For example, select risk level 5 to see all applications with that risk level. The risk level is also a tag that shows in the details of each application. This helps you to understand which types of applications to be wary of and which are low risk.
Managing Application Control and URL Filtering

**Using the AppWiki**

The AppWiki is an easy to use tool that lets you search and filter the Application and URL Filtering Database to find out information.

- Learn about applications, including social networking widgets.
- Filter by a category, tag, or risk level.
- Search for a word or application.

Access the AppWiki from the Application and URL Filtering tab or from the Check Point website (http://appwiki.checkpoint.com/appwiki/applications.htm).

**Updating the Application and URL Filtering Database**

The Application and URL Filtering Database automatically updates regularly to make sure that you have the most current data and newly added applications and websites in your Application Control and URL Filtering Policy. The Application and URL Filtering Database only updates if you have a valid Application Control and/or URL Filtering contract. By default, all new Application Control installations have a valid contract for 30 days.

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

**To manually update the management server only:**

On the **Advanced > Updates** pane of the Application and URL Filtering tab, click **Update Management** to update the management only.

**To change the schedule for updates on the management server and Security Gateways:**

1. Before you run the scheduled update, in the **Automatic Application Updates** section of the Updates pane, select both:
   - **Update Application and URL Filtering Database on the Security Management Server**
   - **Update Application and URL Filtering Database on the Security Gateway**
     
     When you update the database on the Security Management Server, you can see relevant database changes in SmartDashboard. If you only update the Security Gateways, you will see in SmartDashboard that the Security Gateway has a new version of the Application and URL Filtering Database.

2. On the **Updates** pane, in the **Scheduled Updates** section, click **Configure** to schedule when the updates will run. By default, a scheduled update runs at two hour intervals.

In Multi-Domain Security Management, update the database for all Domain Management Servers in the Global SmartDashboard and not from Domain Management Servers.

**Connecting to the Internet for Updates**

The gateway or Security Management Server connects to the internet to get the Application and URL Filtering 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 and the Security Management Server, if necessary.

**To configure a proxy:**

1. The **Advanced > Updates** pane shows if the Security Management Server uses a proxy to connect to the internet or not. Click **Configure Proxy** to go to the SmartDashboard page to configure the proxy for the Security Management Server.

2. In SmartDashboard, in the object properties of a gateway or Security Management Server, go to **Topology > Proxy**.

3. In a Multi-Domain Security Management environment, configure a proxy in **Policy > Global Properties > Proxy**.
Scheduling Updates

To change the update schedule from the default scheduled Application and URL Filtering Database updates:

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.
   - Select Every and 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 Days and the Days page opens. 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 update yet.

The Application and URL Filtering Overview Pane

In the Application and URL Filtering Overview pane, you can quickly see the status of computers and incidents. Use the windows for the most urgent or commonly-used management actions.

My Organization

- Shows a summary of which Security Gateways enforce Application Control and URL Filtering. It also has a link to the Gateways pane.
- Shows the total number of rules in the Policy:
  - The number of Allow rules. Click the link to see them.
  - The number of Block rules. Click the link to see them.

Messages and Action Items

- Shows if a new Application and URL Filtering Database update package is available.
- Shows if Security Gateways require renewed licenses or Application Control or URL Filtering contracts.

Detected in My Organization

Shows a graphical summary of the most popular applications in Top Applications, the most popular categories in Top Categories and the most popular sites in Top Sites.

- Select a time interval for graph data.
- Select the criteria for the graph data: Bandwidth or Sessions.
- Start SmartView Tracker button - Link to open the Application Control and URL Filtering logs in SmartView Tracker.
- Start SmartEvent button - Link to open SmartEvent where you can see the traffic statistics and analysis.

Top Users

Shows a graphical summary of the most popular users who use applications the most.

- Select a time interval for graphs data.
- Select the criteria for the graph data: Bandwidth or Sessions.
Managing Application Control and URL Filtering

- Start SmartView Tracker button - Link to open the Application Control and URL Filtering logs in SmartView Tracker.
- Start SmartEvent button - Link to open SmartEvent where you can see the traffic statistics and analysis.

**AppWiki**
- Shows current statistics of the quantities and types of Applications and Social Networking Widgets included in the Application and URL Filtering Database.
- Click the arrows to browse through the types of Social Networking Widgets.
- Click the links to go directly to the AppWiki.

The Security Gateway connects to the internet to get the most current AppWiki.
- Make sure that there is a DNS server configured.
- Make sure a proxy is configured for each gateway and the Security Management Server, if necessary.

**Gateways Pane**
The Gateways pane lists the gateways with Application Control and/or URL Filtering enabled. Select a gateway and click Edit to edit the gateway properties.

For each gateway, you see the gateway name and IP address. You also see these columns:
- **Application Control** - If Application Control is enabled.
- **URL Filtering** - If URL Filtering is enabled.
- **Identity Awareness** - If Identity Awareness is enabled, and if so, a summary of its Identity Awareness status.
- **Update Status** - If the Application and URL Filtering Database is up to date on the gateway or if an update is necessary.
- **Comments** - All relevant comments.

In the Application and URL Filtering Database Updates section, you can also see the status of the Application and URL Filtering Database on the Security Management Server. A message shows if the Management server is up to date or if a new update is available. Click Updates to go to the Updates pane.

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

You can import a customized application binary file that Check Point creates for applications not in the Application and URL Filtering Database. This file contains a database of internal applications that are not necessarily web-based.

For each object in the list, you see the name and type and also:
- **Primary Category** - If the object is an application or website, this column shows the primary category assigned to it.
- **Description** - The comment entered for the custom-defined object.

**Creating Applications or Sites**
You can create a custom application or site to use in the Rule Base. You can enter the URLs manually or use a .csv (comma separated values) file to add many URLs at one time from an external source.
The .csv file syntax is one URL for each line in the text file. When you use the .csv file option, the URLs are imported when you click Finish. If it is necessary to edit the URLs, click the Applications/Site object in the list and click Edit.

**To create an application or site:**
1. In the Applications/Sites pane, click **New > Application/Site**.
   The Application/Site wizard opens.
2. Enter a name for the application/site.
3. Select one of the options:
   - **Applications/Sites URLs** - To manually enter a URL.
   - **Applications/Sites URLs from a file (.csv)** - To upload a .csv file with URLs.
4. Click Next.
5. If you selected **Applications/Sites URLs**:
   a) Enter a URL and click **Add**.
   b) If you used a regular expression in the URL, click **URLs are defined with regular expressions**.
      Note - Select the **URLs are defined as Regular Expression** checkbox only if the application or site URL is entered as a regular expression using the correct syntax.
   c) Click Next and go to step 7.
6. If you selected **Application/Sites URLs from a file (.csv)**:
   a) Browse to the .csv file and upload it.
   b) Click **Next**.
7. Select a **Primary Category** for the application or site.
   Note - You can click New in the list to create a new category.
8. To select **Additional Categories**:
   a) Click **Add**.
   b) Select the necessary checkboxes in the list.
   c) Click **OK**.
9. Click **Next**.
10. Click **Finish**.
    You can use this custom application or site in the Policy.

**Creating Categories**
You can create a custom category to use in the Rule Base if there is no corresponding category.

**Note** - If category data in the Application and URL Filtering Database for a URL is not applicable for your organization, you can override the categorization ("Overriding Categorization" on page 31).

**To create a new category:**
1. In the Applications/Sites pane, click **New > Category**.
   The Category Properties window opens.
2. Enter a name for the category.
3. Set a color for the category icon (optional).
4. Enter a description for the category (optional).
5. Click **OK**.
   You can use this custom category object in the Policy.
Creating Application or Site Groups

You can create a group of applications or sites to use in the Rule Base. The group members can include categories, applications and widgets from the Application and URL Filtering Database and also custom applications, sites and categories.

To create an application or site group:
1. In the Applications/Sites pane, click New > Applications/Sites Group. The Applications/Sites group window opens.
2. Enter a name for the group.
3. Set a color for the group icon (optional).
4. Enter a comment for the group (optional).
5. Click Add. The Application viewer opens.
6. Select the categories, applications, widgets, and custom items to add as members ("Applications/Sites" on page 17) to the group.
7. Click OK. The selected items are shown in the Group members list.
8. Click OK. You can use this group in the Policy.

Exporting and Importing Applications or Sites

You can import Check Point custom applications for Application Control from the Applications/Sites pane. These are signatures that Check Point creates for organizations that have network applications not in the Application and URL Filtering Database (for example, proprietary applications). After importing the file, you can include them in your Rule Base. The custom applications have an .apps suffix.

To import an application or site file:
1. From the Applications/Sites pane, select Actions > Import. The Import Applications/Sites window opens.
2. Browse to the location of the .apps file, select it and click Open.
3. Click OK. The Custom Application object is added to the Applications/Sites list.

Advanced Settings for Application and URL Filtering

This section describes settings that you can configure in the Application and URL Filtering tab, in the Advanced section of the navigation tree. These settings apply globally for all Security Gateways with Application Control and URL Filtering.

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 Application and URL Filtering policy inspects all HTTP traffic, even if it is sent using non-standard ports. This option is selected by default. You can configure this option in the Advanced section of the Application and URL Filtering tab.

You can also configure IPS to inspect HTTP traffic on non-standard ports.

Overriding Categorization

In some cases, the category data in the Application and URL Filtering Database for a URL is not applicable for your organization. You can use the override categorization option to update the category and risk definitions of a URL.
This definition overrides the information in the Application and URL Filtering Database and the responses received from the Check Point Online Web Service. The Rule Base will use the newly specified categorization when matching rules with URLs.

You can use the toolbar buttons to create, edit, search, and delete a categorization entry.

To override categorization for a URL:
1. In the Advanced > Override Categorization pane, select New.
   The Override Categorization for URL window opens.
2. Enter a URL in the field. You do not need to include the prefix http:\.
3. If the URL contains a regular expression, select URL is defined as a Regular Expression.
4. Enter a comment (optional).
5. Select a Primary Category from the list.
6. Select a Risk from the list.
7. To add additional categories, click Add.
8. Select the categories and click OK.
   The selected categories are shown in the Additional Categories list.
9. Click OK.
   The URL with its newly defined categories is shown in the list in the Override Categorization 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 server certificate.
3. Creates a new SSL certificate for the communication between the Security Gateway and the client, sends the client the new certificate and continues the SSL negotiation with it.
4. Using the two SSL connections:
   a) It decrypts the encrypted data from the client.
   b) Inspects the clear text content for all blades set in the Policy.
   c) Encrypts the data again to keep client privacy as the data travels to the destination web server resource.

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

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

Configuring Outbound HTTPS Inspection

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

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

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

Enabling HTTPS Inspection

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

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

Creating an Outbound CA Certificate

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

After you create an outbound CA certificate, you must export it so it can be distributed to clients. If you do not deploy the generated outbound CA certificate on clients, users will receive SSL error messages in their browsers when connecting to HTTPS sites. You can configure a troubleshooting option that logs such connections ("Troubleshooting" on page 43).

After you create the outbound CA certificate, a certificate object named Outbound Certificate is created. Use this in rules that inspect outbound HTTPS traffic in the HTTPS inspection Rule Base.
To create an outbound CA certificate:
1. In SmartDashboard, right-click the Security Gateway object and select Edit. The Gateway Properties window opens.
2. In the navigation tree, select HTTPS Inspection.
3. In the HTTPS Inspection page, click Create.
4. Enter the necessary information:
   - Issued by (DN) - Enter the domain name of your organization.
   - Private key password - Enter the password that is used to encrypt the private key of the CA certificate.
   - Retype private key password - Retype the password.
   - Valid from - Select the date range for which the CA certificate is valid.
5. Click OK.
6. Export and deploy the CA certificate ("Exporting and Deploying the Generated CA" on page 35).

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

Note - It is recommended that you use private CA Certificates.

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 34) 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 35) on the client machines if it has not already been deployed.

To import a CA certificate:
1. In SmartDashboard, right-click a Security Gateway object, select Edit > HTTPS Inspection > Import
   Or
   From the HTTPS Inspection > Gateways pane of a supported blade, click the arrow next to Create Certificate and select Import certificate from file.
   The Import Outbound Certificate window opens.
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:
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 computers.

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

**To distribute a certificate with a GPO:**

1. From the HTTPS Inspection window of the Security Gateway, click Export certificate
   Or
   From the HTTPS Inspection > Gateways pane in a supported blade, click Export.
2. Save the CA certificate file.
3. Use the Group Policy Management Console ("Deploying Certificates by Using Group Policy" on page 35) to add the certificate to the Trusted Root Certification Authorities certificate store.
4. Push the Policy to the client computers in the organization.
   **Note** - Make sure that the CA certificate is pushed to the client computer organizational unit.
5. Test the distribution by browsing to an HTTPS site from one of the clients and verifying that the CA certificate shows the name you entered for the CA certificate that you created in the **Issued by** field.

**Deploying Certificates by Using Group Policy**

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

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

**To deploy a certificate using Group Policy:**

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

**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 organization Security Gateways ("Server Certificates" on page 36).
• Generate an HTTPS inspection policy by defining relevant rules in the HTTPS inspection Rule Base ("The HTTPS Inspection Policy" on page 36).

• Make sure to configure the relevant server certificate in the HTTPS inspection Rule Base ("Certificate" on page 39).

Server Certificates

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

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 36).

• Add the server certificate object to the Certificate column in the HTTPS Inspection Policy to enforce it in rules ("Certificate" on page 39).

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 and URL Filtering 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.

**Parts of the Rule**

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

**Number (No.)**

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

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

**Name**

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

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

**Source**

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

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

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

**Destination**

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

- **Important** - A rule that blocks traffic, with the Source and Destination parameters defined as Any, also blocks traffic to and from the Captive Portal.
To choose other destinations, put your mouse in the column and a plus sign shows. Click the plus sign to open the list of network objects and select one or multiple destinations.

**Services**

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

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

**Site Category**

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

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

You can also include custom applications, sites, and hosts. You can select a custom defined application or site object (“Creating Applications or Sites” on page 29) 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 www.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 details in SmartView Tracker. This option is useful for obtaining general information on your network traffic. There is one or more log for each session depending on the suppression option.
- **Alert** - Logs the event and executes a command, such as display a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in **Policy > Global Properties > Log and Alert > Alert Commands**
- **Mail** - Sends an email to the administrator, or runs the mail alert script defined in **Policy > Global Properties > Log and Alert > Alert Commands**
- **SNMP Trap** - Sends 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 Security Gateways the rule will be installed on. The default is **All**, which means all Security Gateways that have HTTPS inspection enabled. Put your mouse in the column and a plus sign shows. Click the plus sign to open the list of available Security Gateways and select.

**Certificate**

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

- **For outbound HTTPS inspection** - choose the **Outbound Certificate** object (default) that reflects the CA certificate you created/imported and deployed on the client machines in your organization.
For inbound 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 know 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 Security Gateways from here.

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

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

If the Security Management Server managing the selected Security Gateway does not have a generated CA certificate installed on it, you can add it with Import certificate from file. 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 34) it from the Security Management Server on which it was created.

**Adding Trusted CAs for Outbound HTTPS Inspection**

When a client initiates an HTTPS connection to a web site server, the Security Gateway intercepts the connection. The Security Gateway inspects the traffic and creates a new HTTPS connection from the Security Gateway to the designated server. When the Security Gateway establishes a secure connection (an SSL tunnel) to the designated web site, it must validate the site server certificate.

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

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

You can change the default setting to block untrusted server certificates ("Server Validation" on page 41). The trusted CA list is based on the Microsoft Root Certificate Program (http://technet.microsoft.com/en-us/library/cc751157.aspx).

**Automatically Updating the Trusted CAs List**

Updates for the trusted CA list 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.
Managing Application Control and URL Filtering

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:**
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 list and the validity date range of the certificates.
3. Click **Proceed** to confirm the update.
   - The certificates will be added or removed respectively from the list.
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 update file is available for installation checkbox.

---

**Manually Updating a Trusted CA**

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

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

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

**Saving a CA Certificate**

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

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

**HTTPS Validation**

**Server Validation**

When a Security Gateway receives an untrusted certificate from a web site server, the settings in this section define when to drop the connection.
Untrusted server certificate
When selected, traffic from a site with an untrusted server certificate is immediately dropped. The user gets an error page that states that the browser cannot display the webpage.

When cleared, a self-signed certificate shows on the client machine when there is traffic from an untrusted server. The user is notified that there is a problem with the website 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 environment, you must configure the proxy for the Security Gateway.

To configure the proxy:
1. From the Firewall tab, double-click the Security Gateway that requires proxy configuration.
2. Select Topology > Proxy.
3. Select Use custom proxy settings for this network object and Use proxy server and enter the proxy IP address.
4. Optionally, you can use the default proxy settings.
5. Click OK.

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

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

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

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

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

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

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

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

- **None** - Does not record the event.
- **Log** - Records the event details in SmartView Tracker
- **Alert** - Logs the event and executes a command, such as shows a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in Policy > Global Properties > Log and Alert > Alert Commands

- **Mail** - Sends an email to the administrator, or runs the mail alert script defined in Policy > Global Properties > Log and Alert > Alert Commands
- **SNMP Trap** - Sends an SNMP alert to the SNMP GUI, or runs the script defined in Policy > Global Properties > Log and Alert > Alert Commands
- **User Defined Alert** - Sends one of three possible customized alerts. The alerts are defined by the scripts specified in Policy > Global Properties > Log and Alert > Alert Commands

Troubleshooting

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

- The generated CA was not deployed on clients (“Exporting and Deploying the Generated CA” on page 35).
- The DN in the certificate does not match the actual URL (for example, when you browse to https://www.gmail.com, the DN in the certificate states mail.google.com).
- Applications (such as Firefox and anti-viruses) that use an internal trusted CA list (other than Windows). Adding the CA certificate to the Windows repository does not solve the problem.

The option in the HTTPS Validation pane:

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

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

**HTTP/HTTPS Proxy**

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

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

**Proxy Modes**

Two proxy modes are supported:

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

**Access Control**

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

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

**Ports**

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

**Advanced**

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

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

**Logging**

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

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

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

**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 41) 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 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 shows the SSL validation events that occurred.
- The Details and Summary tabs in the event record show if the traffic was detected or rejected due to SSL Validation settings.

Blade Queries

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

Engine Settings

On the Advanced > Engine Settings pane, configure settings related to engine inspection, the Check Point Online Web Service, Application Control and URL Filtering sessions, and compatibility with gateways from lower versions (Web Browsing application and session unification).
Managing Application Control and URL Filtering

**Fail Mode**
Select the behavior of the Application Control and URL Filtering engine, if it is overloaded or fails during inspection. For example, if the application inspection is terminated in the middle for any reason. By default, in such a situation all application and site traffic is blocked.

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

**Check Point Online Web Service**
The Check Point Online Web Service is used by the URL Filtering engine for updated website categorization and by the Application Control engine for updated Widget definitions. The responses the Security Gateway gets are cached locally to optimize performance.

- **Block requests when the web service is unavailable**
  - When selected, requests are blocked when there is no connectivity to the Check Point Online Web Service.
  - When cleared, requests are allowed when there is no connectivity (default).
- **Website categorization mode** - You can select the mode that is used for website categorization:
  - **Background - requests are allowed until categorization is complete** - When a request cannot be categorized with a cached response, an uncategorized response is received. Access to the site 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 procedure.
  - **Hold - requests are blocked until categorization is complete** - When a request 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 URL Filtering and Social Networking Widgets. For example, click Customize to set URL Filtering to Background mode and Social Networking Widgets to Hold mode.
- **Use web service to detect Social Network Widgets**
  - When selected, the Security Gateway connects to the Check Point Online Web Service to identify social networking widgets that it does not recognize (default).
  - When cleared or there is no connectivity between the Security Gateway and the Service, the unknown widget is treated as Web Browsing traffic.

**Connection Unification**
Application and URL traffic generate a large quantity of logs. To make the quantity of logs manageable, you can consolidate logs by session. A session is a period that starts when the user first accesses an application or site. During a session, the Security Gateway records one log for each application or site that a user browses to. All actions that the user does in the session are included in the log.

There are 3 tracking options you can use:

- **Log** - Records the event details in SmartView Tracker. This option is useful to get general information on your network traffic. It consolidates logs by session (there is one log for each session). It shows the initial URL browsed and the number of suppressed logs it includes.
- **Extended Log** - Consolidates logs by session, shows the number of suppressed logs and includes data for each URL request in the session time frame. Each of the URLs has an entry in the **URLs** tab of the log in SmartView Tracker. Using this option can have an effect on performance.
- **Complete Log** - Records logs for each URL request made regardless of session. Each URL request has its own log. This option also generates an event in SmartEvent for each URL browsed and is intended only for troubleshooting purposes. Note that this option generates many logs.

To adjust the length of a session:

- For applications and sites that are allowed in the Rule Base, the default session is three hours (180 minutes). To change this, click **Session Timeout** and enter a different value, in minutes.
• For applications and sites that are blocked in the Rule Base, a session is 30 seconds. You cannot change this in SmartDashboard.

**Web Browsing**

**Enable Web Browsing logging and policy enforcement** - The Web Browsing application includes all HTTP traffic that is not a defined application. Web Browsing is enabled by default. If you disable it:

• Instances of the Web Browsing in the Application and URL Filtering Control Rule Base are not enforced. For example, if you have a rule that blocks Web Browsing, this traffic will not be blocked if Web Browsing is turned off.

• No Web Browsing logs are recorded.

**Application Control Backwards Compatibility**

For compatibility with Security Gateway versions earlier than R75.20, click **Settings** to configure backwards compatibility for use with Application Control.

• **Unify connections from the same user/IP to a specific domain into a single session/log**
  - When selected, all application or site traffic during a session is combined into one log (default).
  - When cleared, each connection to an application or site generates a different log.

• **Issue a separate log per each domain accessed**
  - When cleared (default), all Web Browsing connections from a user or IP address during a session are combined into one log.
  - When selected, the Web Browsing application generates one log for each domain that a user or IP address browses to for each session.

**Application and URL Filtering and Identity Awareness**

Identity Awareness and Application and URL Filtering can be used together to add user awareness, computer awareness, and application awareness to the Check Point Security Gateway. They work together in these procedures:

• Use Identity Awareness Access Roles in Application and URL Filtering rules as the source of the rule.

• You can use all the types of identity sources to acquire identities of users who try to access applications.

In SmartView Tracker logs and SmartEvent events, you can see which user and IP address accesses which applications. For more details, see the *R75.40 Identity Awareness Administration Guide*.

**Using Identity Awareness in the Application and URL Filtering Rule Base**

The Security Gateway inspects Application and URL Filtering requests and applies rules in a sequential manner. When a Security Gateway receives a packet from a connection, it examines the packet against the first rule in the Rule Base. If there is no match, it goes on to the second rule and continues until it completes the Rule Base. If no rule matches, the packet is allowed.

In rules with access roles, you can add a property in the **Action** field to redirect traffic to the Captive Portal. If this property is added, when the source identity is unknown and traffic is HTTP, the user is redirected to the Captive Portal. If the source identity is known, the **Action** in the rule (Allow or Block) is enforced immediately and the user is not sent to the Captive Portal. After the system gets the credentials from the Captive Portal, it can examine the rule for the next connection.
In rules with access role objects, criteria matching operates like this:

- **When identity data for an IP is known:**
  - If it matches an access role, the rule is enforced and traffic is allowed or blocked based on the specified action.
  - If it does not match an access role, it goes on to examine the next rule.

- **When identity data for an IP is unknown and:**
  - All the rule’s fields match besides the source field with an access role.
  - The connection protocol is HTTP.
  - The action is set to redirect to the Captive Portal.
    - If all the conditions apply, the traffic is redirected to the Captive Portal to get credentials and see if there is a match.
    - If not all conditions apply, there is no match and the next rule is examined.

- **When the criteria does not match any of the rules in the Rule Base, the traffic is allowed.**

**To redirect HTTP traffic to the Captive Portal:**

1. In a rule that uses an access role in the **Source** column, right-click the **Action** column and select **Edit Properties**.
   - The Action Properties window opens.
2. Select **Redirect HTTP connections**.
3. Click **OK**.
   - The Action column shows that a redirect to the Captive Portal occurs.

This is an example of an Application and URL Filtering Rule Base that shows how criteria matching operates:

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Applications/Sites</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Finance_Dept</td>
<td>Internet</td>
<td>Any</td>
<td>Salesforce</td>
<td>Allow (display Captive Portal)</td>
</tr>
<tr>
<td></td>
<td>(Access Role)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Any_identified_user</td>
<td>Internet</td>
<td>Any</td>
<td>Remote Administration Tool</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td>(Access Role)</td>
<td></td>
<td></td>
<td>(non-HTTP category)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Any_identified_user</td>
<td>Internet</td>
<td>Any</td>
<td>Any recognized</td>
<td>Block</td>
</tr>
<tr>
<td></td>
<td>(Access Role)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

When browsing the Internet, different users experience different outcomes:

**Example 1** - An unidentified Finance user that attempts to access Salesforce is sent to the Captive Portal. This happens because the action is set to redirect to the Captive Portal. After entering credentials and being identified, the user is granted access according to rule number 1.

**Example 2** - An unidentified user that attempts to access the Remote Administration Tool matches rule 2, but not the Source column. Because the application is not HTTP, traffic cannot be redirected to the Captive Portal. Since none of the rules match, the user is granted access to the Remote Administration Tool.

**Example 3** - An unidentified user that browses to Gmail does not match rules 1 and 2 because of the application. In rule 3 there is also no match because the action is not set to redirect to the Captive Portal. Since none of the rules match, the user is granted access to Gmail.

**Identifying Users Behind a Proxy**

If your organization uses an HTTP proxy server behind the Security Gateway, the Rule Base cannot match taking into account identities. Therefore, you cannot see identities of users behind the proxy. Application Control and URL Filtering logs show the proxy as their source IP address and not the user identity. Application Control, URL Filtering and Identity Awareness Security Gateways can use X-Forward-For HTTP header, which is added by the proxy server, to resolve this issue. When you configure the proxy server to
add X-Forward-For HTTP header and the Check Point gateways to use it, you will see the correct source identities for traffic that goes through the proxy.

You can also configure the gateways to hide and strip the X-Forward-For header in outgoing traffic so that internal IP addresses will not be seen in requests to the internet.

**To use X-Forwarded-For HTTP header:**
1. Configure your proxy server to use X-Forwarded-For HTTP Header.
2. In SmartDashboard, on the Identity Awareness page of each gateway object, select Detect users located behind HTTP proxy using X-Forward-For header.
3. To configure the gateway to hide the X Forwarded-For header to not show internal IP addresses in requests to the internet, select Hide X Forward-For header in outgoing traffic.
4. Install the Policy.

**Legacy URL Filtering**

To manage URL Filtering on Security Gateway versions earlier than R75.20, use the Legacy URL Filtering Policy.

**To enable Legacy URL Filtering on Security Gateway versions earlier than R75.20:**
1. On the Firewall tab, double-click the required Security Gateway network object.
2. Select Other > More Settings > Enable Legacy URL Filtering.
3. Click OK.

**Terminology**

The following terms are used in URL Filtering applications:

- **Allow List**: A list of allowed URL addresses, for example, a URL in the Allow List is allowed even if it is associated with a category that is blocked.
- **Block List**: A list of blocked URL addresses, for example, a URL in the Block List is blocked even if it is associated with a category that is not blocked.
- **Blocking Notifications**: Contains the message that appears when a URL address is blocked and the URL to which a blocked URL address is redirected.
- **Category**: Contains a group of topics sharing a common attribute (for example, crime, education and games).
- **Network Exceptions**: Contains a list of connections for which URL Filtering should not be enforced.
- **Web Filter**: Enables you to allow or block URLs based on network connections and/or an external categorized database and local exception lists.

**Architecture**

When a URL request arrives at a local machine, the machine checks the Network Exceptions List to determine whether to enforce the URL Filtering policy. The URL Filtering policy is activated if the connection is accepted by the Security Policy. If the URL Filtering policy is enforced, the URL header is stripped and the address is sent to the Web Filter engine.

The URL is allowed or blocked based on URL request information in the predefined database and/or the Web Filter Allow/Block Lists. For example, if the URL address matches two or more categories, and one of them is blocked, the URL address is denied, however, if the same address appears in the Allow List it is accepted.

The Web Filter engine is installed on the Security Gateway and the categories are updated by selecting: SmartDashboard > Anti-Virus & URL Filtering > URL Filtering > URL Filtering Policy.

**Important** - During installation of the Web Filter engine, no default database is installed; therefore, the Web Filtering policy is not enforced until a signature update is performed. The first update may take a long time, depending on your environment. Subsequent updates should take significantly less time, as only incremental information is downloaded.
Configuring Legacy URL Filtering

To configure Legacy URL Filtering:

1. Enable legacy URL Filtering (on page 50).
2. In the Application and URL Filtering tab of SmartDashboard, select Legacy URL Filtering > URL Filtering Policy.
3. On the URL Filtering Policy page, configure the following:
   a) Select one of the following URL Filtering Policy Modes:
      - **On**: URL Filtering is active and URLs associated with blocked categories are blocked. To activate URL Filtering, you must configure automatic updates of the URL Filtering database. To configure automatic updates, click the Automatic updates link. URL Filtering will not work if automatic updates have not been configured.
      - **Monitor**: URLs associated with blocked categories are logged and not blocked.
      - **Off**: URL Filtering is off and does not inspect URL addresses.

   b) In the Enforcing Gateways window, select the Security Gateways for which you want to activate URL Filtering. This window contains all of the Security Gateways for which URL Filtering can and has been enforced.

   c) In the Categories list, select the URL categories to block.
      - A green icon indicates that URLs associated with this category are allowed.
      - A red icon indicates that URLs associated with this category are blocked.

   d) In the Tracking section, select how to track a detected URL address. All options other than **None** generate a log record in SmartView Tracker.

4. Select Advanced > Allow URLs/IPs to add a URL or IP address to be allowed even if it is associated with a blocked category.

5. Select Advanced > Block URLs/IPs to add a URL or IP address to be blocked even if it is associated with an allowed category.

6. Select Advanced > Network Exceptions to create a list of the networks connections through which traffic should not be inspected or in order to enforce URL Filtering on all Web traffic. Network Exceptions works according to a source and destination Rule Base and does not use the URL Filtering engine.

7. Select Advanced > Blocking Notifications to notify the user when the URL request is blocked. Choose one of the options:
   - Enter the message to be displayed when a URL address is blocked according to the URL Filtering Policy.
   - Enter the URL to which the user is to be redirected.
Chapter 4

Application Control and URL Filtering in SmartView Tracker

In This Chapter

Log Sessions 52
Application Control and URL Filtering Logs 52
Viewing Logs 53

Log Sessions

Application traffic generates a very 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 Security 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 applications or sites, including Web Browsing:

- For applications or sites that are allowed in the Rule Base, the default session is three hours. You can change this in SmartDashboard from the Application and URL Filtering tab > Advanced > Engine Settings > Session Timeout.
- For applications or sites that are blocked in the Rule Base, a session is 30 seconds.

Application Control and URL Filtering Logs

Logs from Application Control and URL Filtering are shown in SmartView Tracker. The logs that Application Control and URL Filtering generate depend on the Tracking settings that you configure in:

- Each Application Control and URL Filtering rule in the Rule Base - sets logs for the traffic. These can be regular logs, extended logs or complete logs:
  - Log - Records the event details in SmartView Tracker. This option is useful to get general information on your network traffic. It consolidates logs by session (there is one log for each session). It shows the initial URL browsed and the number of suppressed logs it includes.
  - Extended Log - Consolidates logs by session, shows the number of suppressed logs and includes data for each URL request in the session time frame. Each of the URLs has an entry in the URL tab of the log in SmartView Tracker. Using this option can have an effect on performance.
  - Complete Log - Records logs for each URL request made regardless of session. Each URL request has its own log. This option also generates an event in SmartEvent for each URL browsed and is intended only for troubleshooting purposes. Note that this option generates many logs.
Note - For versions earlier than R75.20, the logging option that you select for Session Unification on the Advanced > Engine Settings > Settings page - sets logging options for the Web Browsing application.

Logs related to Application and URL Filtering Database updates on the Security Gateway are in Application Control > System Logs.

Logs related to Application and URL Filtering Database updates on the management are in the Management tab.

### Viewing Logs

To open SmartView Tracker do one of these:

- Click Start > Check Point > SmartView Tracker.
- From the Application and URL Filtering Overview pane > Detected in My Organization, click SmartView Tracker.
- From the SmartDashboard toolbar of any SmartConsole application, select Window > SmartView Tracker or press Control +Shift +T.

### Predefined Queries

There are multiple predefined queries in Predefined > Network Security Blades > Application and URL Filtering. You can filter the queries to focus on logs of interest.

- **All** - Shows all Application Control and URL Filtering traffic, including allowed and blocked.
- **High Risk** - Shows traffic of Risk Levels 4 and 5.
- **More > Applications** - Shows all Application Control traffic.
- **More > Sites** - Shows all URL Filtering traffic.
- **More > Bandwidth Consuming** - Shows logs from traffic that has the High Bandwidth tag.
- **More > Blocked** - Shows all blocked traffic.
- **More > HTTPS Inspection** - Shows all Application Control and URL Filtering traffic that passed through HTTPS inspection.
- **More > System** - Shows logs related to Application and URL Filtering Database updates and other system related issues. This includes logs related to problems that the application detection service might encounter.

### Permissions for Logs

Most information in Application Control and URL Filtering logs is classified and only administrators with at least Read permissions for Application Control Logs can see it.

**To set these permissions for an administrator in a new profile:**

1. Open SmartDashboard.
2. In the Users and Administrators tree, select an administrator > Edit.
3. In the Administrator Properties > General Properties page in the Permissions Profile field, click New.
4. In the Permissions Profile Properties window:
   - Enter a Name for the profile.
   - Select Customized and click Edit.
   - The Permissions Profile Custom Properties window opens.
5. In the Monitoring and Logging tab, select Application Control Logs for permission to see the classified information in the Application Control and URL Filtering logs.
6. 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.
Chapter 5

Application Control and URL Filtering in SmartEvent

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.

The administrator must have HTTPS Inspection permissions to see classified data in HTTPS inspected traffic.

You can filter the Application Control and URL Filtering information for fast monitoring and useful reporting on application traffic.

- Real-time and historical graphs and reports of application and site traffic.  
- 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 Application and URL Filtering as the SmartEvent Intro Mode, it shows the Application Control and URL Filtering information.

To use SmartEvent or SmartEvent Intro, you must enable it on the Security Management Server or on a dedicated machine. See the R75.40 SmartEvent Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=13943).

Viewing Information in SmartEvent
To open SmartEvent do one of these:

- Click Start > Check Point > SmartEvent.
- From the Application and URL Filtering Overview pane > Detected in My Organization, click More graphs.
- From the SmartDashboard toolbar of any SmartConsole application, select Window > SmartEvent or press Control +Shift +A.

When SmartEvent opens, go to Events > Predefined > Application and URL Filtering to use the predefined queries for Application Control and URL Filtering. Events are grouped by the number of megabytes used.

- All - Shows all Application Control and URL Filtering events, includes allowed and blocked events.  
- High Risk - Shows events of Risk Levels 4 and 5.
Application Control and URL Filtering in SmartEvent

- More > Applications - Shows all Application Control events, includes allowed and blocked events.
- More > Sites - Shows all URL Filtering events, includes allowed and blocked events.
- More > Blocked - Shows all blocked URL Filtering events.
- More > By Category - Shows events by the application/sites category.
- More > By User - Shows events according to the name of the user.
- More > By Rule Name - Shows events by the name of the Application Control or URL Filtering rule that applies to them.
- More > Social Networking - Shows events with Application Control social networking categories. By default, these include: Facebook widgets, LinkedIn widgets, MySpace widgets, Ning.com widgets, Orkut widgets, and Social Networking.
- More > HTTPS Inspection - Shows Application Control and URL Filtering events that passed through HTTPS inspection.


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 Application and URL Filtering.

All of the information in SmartEvent Intro is based on Application Control and URL Filtering events. See the different tabs for detailed information.

The SmartEvent Intro Overview Page

The Overview page shows a quick understandable overview of the Application Control and URL Filtering 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
- Top Users by Traffic
- Top Application / Site by Traffic
- Top Applications Categories by Traffic
- Newly Detected Applications
- Status

Application Control and URL Filtering Event Queries

See detailed event queries in the Events tab. Events are grouped by the number of megabytes used.
- All - Shows all Application Control and URL Filtering events, includes allowed and blocked events.
- High Risk - Shows events of Risk Levels 4 and 5.
- More > Applications - Shows all Application Control events, includes allowed and blocked events.
- More > Sites - Shows all URL Filtering events, includes allowed and blocked events.
- More > Blocked - Shows all blocked URL Filtering events.
- More > By Category - Shows events by the application/sites category.
- More > By User - Shows events according to the name of the user.
- **More > By Rule Name** - Shows events by the name of the Application Control or URL Filtering rule that applies to them.

- **More > Social Networking** - Shows events with Application Control social networking categories. By default, these include: Facebook widgets, LinkedIn widgets, MySpace widgets, Ning.com widgets, Orkut widgets, and Social Networking.

- **More > HTTPS Inspection** - Shows Application Control and URL Filtering events that passed through HTTPS inspection.

See the [R75.40 SmartEvent Intro Administration Guide](http://supportcontent.checkpoint.com/solutions?id=sk67581).
Chapter 6

Configuring UserCheck

In This Chapter
- Configuring the Security Gateway for UserCheck 58
- UserCheck CLI 59
- Revoking Incidents 60

Configuring the Security Gateway for UserCheck

Enable or disable UserCheck directly on the Security Gateway. The Application and URL Filtering tab > Gateways window shows a list of Security Gateways with the Application Control blade enabled.

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

To configure a Security Gateway for UserCheck:
1. Select a Security Gateway and click Edit.
   The Properties window opens.
2. On the UserCheck page, select Enable UserCheck.
3. Enter the information for the UserCheck portal:
   - In the Main URL field, enter the primary URL for the web portal that shows the UserCheck notifications.
     Notes -
     If the Main URL points to an external interface, the Accessibility option must be set to one of these:
     - Through all interfaces
     - According to the firewall Policy
     If users connect to the Security Gateway remotely, set the Security Gateway internal interface (on the Topology page) to be the same as the Main URL for the UserCheck portal.
   - In the IP address field, enter the IP address that the URL resolves to.
   - Click Aliases to add URL aliases that redirect different hostnames to the Main URL, for example: Usercheck.mycompany.com. The aliases must be resolved to the portal IP address on the corporate DNS server
4. In the Certificate area, click Import to import a certificate that the portal uses to authenticate to the server.
   By default, the portal uses a certificate from the Check Point Internal Certificate Authority (ICA). This might generate warnings if the user browser does not recognize Check Point as a trusted Certificate Authority. To prevent these warnings, import your own certificate from a recognized external authority.
5. In the Accessibility area, click Edit to configure interfaces on the Security Gateway through which the portal can be accessed. These options are based on the topology configured for the Security Gateway. Users are sent to the UserCheck portal if they connect:
   - Through all interfaces
   - Through internal interfaces (default)
     - Including undefined internal interfaces
     - Including DMZ internal interfaces
     - Including VPN encrypted interfaces (default)
• **According to the Firewall Policy.** Select this option if there is a rule that states who can access the portal.

6. Click OK.
7. Install Policy.

**Notes**-

- If **Through internal interfaces > Including VPN encrypted interfaces** is selected, add a Firewall rule that looks like this:

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

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

## UserCheck CLI

You can use the `usrchk` command in the gateway command line to show or clear the history of UserCheck objects.

**Description**

`usrchk`

**Syntax**

`usrchk [debug] [hits]`

**Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug</td>
<td>Controls debug messages</td>
</tr>
</tbody>
</table>

**hits**

Shows user incident options:

- `list` - Options to list user incidents:
  - `all` - List all existing incidents.
  - `user <username>` - List incidents of a specified user.
  - `uci <name of interaction object>` - List incidents of a specified UserCheck interaction object

- `clear` - Options to clear user incidents:
  - `all` - Clear all existing incidents
  - `user <username>` - Clear incidents for a specified user
  - `uci <name of interaction object>` - Clear incidents of a specified UserCheck interaction object

**Examples:**

- To show all UserCheck interaction objects, run: `usrchk hits list all`
- To clear the incidents for a specified user, run: `usrchk hits clear user <username>`

**Notes:**

- You can only run a command that contains `user <username>` if:
  - Identity Awareness is enabled on the gateway.
  - Identity Awareness is used in the same policy rules as UserCheck objects.
- To run a command that contains a specified UserCheck interaction object, first run `usrchk hits list all` to see the names of the interaction objects. Use the name of the interaction object as it is shown in the list.
Revoking Incidents

The Revoke Incidents URL can revoke a user’s responses to UserCheck notifications. The URL is:

://<IP of gateway>/UserCheck/RevokePage

If users regret their responses to a notification and contact their administrator, the administrator can send users the URL.

After a user goes to the URL, all of the user’s responses to notifications are revoked. The logs in SmartView Tracker will show the user’s activity, and that the actions were revoked afterwards.

Administrators can use the usrchk command of the CLI to revoke incidents for one user, all users, or a specified interaction object ("UserCheck CLI" on page 59).
Chapter 7

UserCheck Client

In This Chapter

UserCheck Client Overview 61
UserCheck Requirements 61
Enabling UserCheck Client 61
Client and Gateway Communication 62
Getting the MSI File 68
Distributing and Connecting Clients 68
Helping Users 70

UserCheck Client Overview

The UserCheck client is installed on endpoint computers to communicate with the gateway and show UserCheck interaction notifications to users. It works with these Software Blades:

DLP - Notifications of DLP incidents can be sent by email (for SMTP traffic) or shown in a popup from the UserCheck client in the system tray (for SMTP, HTTP and FTP).

Application and URL Filtering and URL Filtering - The UserCheck client adds the option to send notifications for applications that are not in a web browser, such as Skype, iTunes, or browser add-ons (such as radio toolbars). The UserCheck client can also work together with the UserCheck portal to show notifications on the computer itself when:

- The notification cannot be displayed in a browser, or
- The UserCheck engine determines that the notification will not be shown correctly in the browser and the Fallback Action for the UserCheck object is Allow.

Users select an option in the notification message to respond in real-time.

For DLP, administrators with full permissions or the View/Release/Discard DLP messages permission can also send or discard incidents from SmartView Tracker.

Workflow for installing and configuring UserCheck clients:
1. Configure how the clients communicate with the gateway and create trust with it.
2. Enable UserCheck and the UserCheck client on the gateway.
3. Download the UserCheck client MSI file.
4. Install the UserCheck client on the endpoint computers.
5. Make sure that the UserCheck clients can connect to the gateway and receive notifications.

UserCheck Requirements


Enabling UserCheck Client

Enable UserCheck and the UserCheck client on the gateway in the Properties window of the gateway object in SmartDashboard. This is necessary to let clients communicate with the gateway.
To enable UserCheck and the UserCheck client on the gateway:

1. In SmartDashboard, open the General Properties window of the gateway object.
2. If Data Loss Prevention is enabled on the gateway, select Data Loss Prevention from the tree. In the UserCheck area:
   a) Select Enable Check Point UserCheck. This enables UserCheck notifications from the client.
   b) Optional: Select Place Check Point UserCheck download links on email notifications. When selected, DLP email notifications also contain a link to download the UserCheck client directly from the email.
3. If Application and URL Filtering is enabled on the gateway, select UserCheck from the tree:
   a) Select Enable UserCheck for Application Control and URL Filtering. This enables UserCheck notifications from the gateway.
   b) In the UserCheck Client area, select Activate UserCheck Client support. This enables UserCheck notifications from the client.
4. Click OK.
5. Install the policy on the gateway.

Client and Gateway Communication

In an environment with UserCheck clients, the gateway acts as a server for the clients. Each client must be able to discover the server and create trust with it.

To create trust, the client makes sure that the server is the correct one. It compares the server fingerprint calculated during the SSL handshake with the expected fingerprint. If the server does not have the expected fingerprint, the client asks the user to manually confirm that the server is correct.

Here is a summary of the methods that you can use for clients to discover and trust the server. More details are described later in this section.

- File name based server configuration – If no other method is configured (default, out-of-the-box situation), all UserCheck clients downloaded from the portal are renamed to have the portal machine IP address in the filename. During installation, the client uses this IP address to connect to the gateway. Note that the user has to click Trust to manually trust the server.
- AD based configuration – If client computers are members of an Active Directory domain, you can deploy the server addresses and trust data using a dedicated tool.
- DNS SRV record based server discovery – Configure the server addresses in the DNS server. Note that the user has to click Trust to manually trust the server.
- Remote registry – All of the client configuration, including the server addresses and trust data reside in the registry. You can deploy the values before installing the client (by GPO, or any other system that lets you control the registry remotely). This lets you use the configuration when the client is first installed.

Option Comparison

<table>
<thead>
<tr>
<th></th>
<th>Requires AD</th>
<th>Manual User Trust (one time) Required?</th>
<th>Multi-Site</th>
<th>Client Remains Signed?</th>
<th>Still works after Gateway Changes</th>
<th>Level</th>
<th>Recommended for...</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name based</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Very Simple</td>
<td>Single Security Gateway deployments</td>
</tr>
<tr>
<td>AD based</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Simple</td>
<td>Deployments with AD that you can modify</td>
</tr>
</tbody>
</table>
**File Name Based Server Discovery**

This option is the easiest to deploy, and works out-of-the-box. It requires that users manually click **Trust** to trust the server the first time they connect. You can use this option if your deployment has only one Security Gateway with the relevant Software Blades.

**How does it work?**

When a user downloads the UserCheck client from UserCheck notification, the address of the Security Gateway is inserted into the file name. During the installation sequence, the client checks if there is any other discovery method configured (AD based, DNS based, or local registry). If no method is configured and the gateway can be reached, it is used as the server. In the UserCheck Settings window, you can see that the server you connect to is the same as the Security Gateway in the UserCheck client filename.

Users must manually make sure that the trust data is valid because the file name can easily be changed.
Renaming the MSI

You can manually change the name of the MSI file before it is installed on a computer so that it connects to different gateway.

To rename the MSI file:

1. Make sure the gateway has a DNS name.
2. Rename the MSI using this syntax: \UserCheck\~GWname.msi
   Where GWname is the DNS name of the gateway.
   Optional: Use \UserCheck\~GWname-port.msi
   Where port is the port number of notifications. For example, UserCheck_~mygw-18300.msi.

   Notes - The prefix does not have to be "UserCheck". The important part of the syntax is underscore tilde (_~), which indicates that the next string is the DNS of the gateway.
   If you want to add the port number for the notifications to the client from the gateway, the hyphen (-) indicates that the next string is the port number.

Active Directory Based Configuration

If your client computers are members of an Active Directory domain and you have administrative access to this domain, you can use the Distributed Configuration tool to configure connectivity and trust rules.

The Distributed Configuration tool has three windows:

- Welcome - Describes the tool and lets you enter different credentials that are used to access the AD.
- Server configuration – Configure which Security Gateway the client connects to, based on its location.
- Trusted gateways – View and change the list of fingerprints that the Security Gateways consider secure.

To enable Active Directory based configuration for clients:

1. Download and install the UserCheck client MSI on a computer.
   From the command line on that computer, run the client configuration tool with the AD utility.
   For example, on a Windows 7 computer:
   "C:\Users\<user name>\Local Settings\Application Data\Checkpoint\UserCheck\UserCheck.exe" -adtool
   The Check Point UserCheck - Distributed Configuration tool opens.
2. In the Welcome page, enter the credentials of an AD administrator. By default, your AD username is shown. If you do not have administrator permissions, click Change user and enter administrator credentials.
3. In the Server Configuration page, click Add.
   The Identity Server Configuration window opens.
4. Select Default and then click Add.
5. Enter the IP address or Fully Qualified Domain Name (FQDN) and the port for the AD Server.
6. Click OK.
   The identity of the AD Server for the UserCheck client is written in the Active Directory and given to all clients.

   Note - The entire configuration is written under a hive named Check Point under the Program Data branch in the AD database that is added in the first run of the tool. Adding this hive does not affect other AD based applications or features.

Server Configuration Rules

If you use the Distributed Configuration tool and you configure the client to Automatically discover the server, the client fetches the rule lists. Each time it must connect to a server, it tries to match itself against a rule, from top to bottom.
When the tool matches a rule, it uses the servers shown in the rule, according to the priority specified.

![Server Configuration](image)

The configuration in this example means:

1. If the user is coming from ‘192.168.0.1 – 192.168.0.255’, then try to connect to US-GW1. If it is not available, try BAK-GS2 (it is only used if US-GW1 is not available, as its priority is higher).
2. If the user is connected from the Active Directory site ‘UK-SITE’, connect either to UK-GW1 or UK-GW2 (choose between them randomly, as they both have the same priority). If both of them are not available, connect to BAK-GS2.
3. If rules 1 and 2 do not apply, connect to BAK-GS2 (the default rule is always matched when it is encountered).

Use the Add, Edit and Remove buttons to change the server connectivity rules.

**Trusted Gateways**

The Trusted Gateways window shows the list of servers that are trusted - no messages open when users connect to them.

You can add, edit or delete a server. If you have connectivity to the server, you can get the name and fingerprint. Enter its IP address and click Fetch Fingerprint in the Server Trust Configuration window. If you do not have connectivity to the server, enter the same name and fingerprint that is shown when you connect to that server.
**DNS Based Configuration**

If you configure the client to **Automatic Discovery** (the default), it looks for a server by issuing a DNS SRV query for the address of the gateway (the DNS suffix is added automatically). You can configure the address in your DNS server.

**To configure DNS based configuration on the DNS server:**
1. Go to **Start** > **All Programs** > **Administrative Tools** > **DNS**.
2. Go to **Forward lookup zones** and select the applicable domain.
3. Go to the **tcp** subdomain.
4. Right click and select **Other new record**.
5. Select **Service Location, Create Record**.
6. In the **Service** field, enter **CHECKPOINT_DLP**.
7. Set the **Port number** to 443.
8. In **Host offering this server**, enter the IP address of the Security Gateway.
9. Click **OK**.

**Note** - To configure load sharing for the Security Gateway create multiple SRV records with the same priority. To configure High Availability, create multiple SRV records with different priorities.
If you configure AD based and DNS based configuration, the results are combined according to the specified priority (from the lowest to highest).

Troubleshooting DNS Based Configuration

To troubleshoot issues in DNS based configuration, you can see the SRV records that are stored on the DNS server.

To see SRV records on the DNS server:

Run:

```
C:\> nslookup
> set type=srv
> checkpoint_dlp._tcp
```

The result is:

```
C:\> nslookup
> set type=srv
> checkpoint_dlp._tcp
Server: dns.company.com
Address: 192.168.0.17

checkpoint_dlp._tcp.ad.company.com SRV service location:
priority = 0
weight = 0
port = 443
svr hostname = dlpserver.company.com
dlpserver.company.com internet address = 192.168.1.212
```
Remote Registry

If you have a way to deploy registry entries to your client computers, for example, Active Directory or GPO updates, you can deploy the Security Gateway addresses and trust parameters before you install the clients. Clients can then use the deployed settings immediately after installation.

To configure the remote registry option:
1. Install the client on one of your computers. The agent installs itself in the user directory, and saves its configuration to HKEY_CURRENT_USER.
2. Connect manually to all of the servers that are configured, verify their fingerprints, and click Trust on the fingerprint verification dialog box.
3. Configure the client to manually connect to the requested servers (use the Settings window).
4. Export these registry keys (from HKEY_CURRENT_USER):
   a) SOFTWARE\CheckPoint\UserCheck\TrustedGateways (the entire tree)
   b) SOFTWARE\CheckPoint\UserCheck\DefaultGateway
      (i) DefaultGateway
      (ii) DefaultGatewayEnabled
5. Import the exported keys to the endpoint computers before you install the UserCheck client.

Getting the MSI File

Use the Check_Point_UserCheck.MSI file to install the client on user machines. Each UserCheck client must be configured to connect to the gateway and to use the port needed for notifications. The default ports are 443 and 80. Download the MSI file from the gateway through the Properties window of the gateway object in SmartDashboard. The MSI file is available after the first time that policy is installed on the gateway.

To get the MSI file:
1. In SmartDashboard, open the General Properties window of the gateway object.
2. If Data Loss Prevention is enabled on the gateway, select Data Loss Prevention.
   • In the UserCheck area, click Download Client.
3. If Application and URL Filtering is enabled on the gateway, select UserCheck.
   • In the UserCheck Client area, click Download Client.

If DLP and Application and URL Filtering are enabled on the gateway, you can get the MSI file from the Data Loss Prevention page or the UserCheck page.

Distributing and Connecting Clients

After configuring the clients to connect to the gateway, install the clients on the user machines. You can use any method of MSI or EXE mass deployment and installation that you choose. For example, you can send users an email with a link to install the client. When a user clicks the link, the MSI file automatically installs the client on the computer.

Alternatively, users can download the installation package from the regular DLP UserCheck notifications. The installation is silent and generally, no reboot is required.

When the client is first installed, the tray icon indicates that it is not connected. When the client connects to the gateway, the tray icon shows that the client is active.
The first time that the client connects to the gateway, it asks for verification from the user and approval of the fingerprint.

![UserCheck Client](Image)

Do you approve this Fingerprint as Valid?

Certificate Status: issued by unknown certificate authority

Server: 190.0.2.0

Fingerprint: 60CK CDAL RUEHARD IOWA GANG RUNG NUMB THIS

We recommend that you let the users know this will happen.

We recommend that you use a server certificate that is trusted by the certificate authority installed on users' computers. Then users do not see a message that says: Issued by unknown certificate authority.

If UserCheck for DLP is enabled on the gateway, users are required to enter their username and password after the client installs.

**Example of message to users about the UserCheck client installation (for DLP):**

```
Dear Users,

Our company has implemented a Data Loss Prevention automation to protect our confidential data from unintentional leakage. Soon you will be asked to verify the connection between a small client that we will install on your computer and the computer that will send you notifications.

This client will pop up notifications if you try to send a message that contains protected data. It might let you to send the data anyway, if you are sure that it does not violate our data-security guidelines.

When the client is installed, you will see a window that asks if you trust the DLP server. Check that the server is SERVER NAME and then click Trust.

In the next window, enter your username and password, and then click OK.
```

**Note** - If the UserCheck client is not connected to the gateway, the behavior is as if the client was never installed. Email notifications are sent for SMTP incidents and the Portal is used for HTTP incidents.

**UserCheck with Check Point Password Authentication**

For DLP, by default, a UserCheck client always authenticates with the credentials of the user that is currently logged in to the AD Domain.

Authenticating with another domain user is not supported. You can configure the UserCheck client to be able to authenticate with a user account that was manually defined by the administrator in SmartDashboard. You can see and edit those users in the Data Loss Prevention tab, Additional Settings > Users page.

**To configure authentication with a user account in SmartDashboard:**

**SmartDashboard Configuration**

1. Open SmartDashboard.
2. For each user, edit the user object. You can do this in the Data Loss Prevention tab in the Additional Settings > Users page.
3. In the General Properties page of the user, make sure that an email address is defined.
**UserCheck Client Configuration**

Ask your users to configure their UserCheck client:

1. On the UserCheck client computer, right click the UserCheck icon in the Notification Area (next to the system clock).
2. Select **Settings**.
3. Click **Advanced**.
4. Select **Allow authentication with alternate user account**.

**Helping Users**

If users require assistance to troubleshoot issues with the UserCheck client, you can ask them to send you the logs.

**To configure the client to generate logs:**

1. Right-click the UserCheck tray icon and select **Settings**.
   - The **Settings** window opens.
2. Click **Log to** and browse to a pathname where the logs are saved.
3. Click **OK**.

**To send UserCheck logs from the client:**

1. Right-click the UserCheck tray icon and select **Status**.
   - The **Status** window opens.
2. Click **Advanced** and then click the **Collect information for technical support** link.
   - The default email client opens, with an archive of the collected logs attached.
Chapter 8

Setting up a Mirror Port

In This Chapter

Technical Requirements 71
Configuring a Mirror Port 71

You can configure a mirror port on a Check Point gateway to monitor and analyze network traffic with no effect on your production environment. The mirror port duplicates the network traffic and records the activity in logs.

You can use mirror ports:

- As a permanent part of your deployment, to monitor the use of applications in your organization.
- As an evaluation tool to see the capabilities of the Application Control and IPS blades before you decide to purchase them.

The mirror port does not enforce a Policy and therefore you can only use it to see the monitoring and detecting capabilities of the blades.

Benefits of a mirror port include:

- There is no risk to your production environment.
- It requires minimal set-up configuration.
- It does not require TAP equipment, which is much more expensive.

Technical Requirements

You can configure a mirror port on gateways with:

- SecurePlatform 32 bit or 64 bit.
- Check Point version R75 and higher.

Mirror ports are not supported with:

- Management servers- you can only configure it on a gateway
- The Data Loss Prevention Software Blade
- NAT of any kind
- Clusters
- IPS protections that are performance critical
- Legacy User Authority features - you cannot have Authentication (Client, Session, or User) in the Action column of the Firewall Rule Base.

Configuring a Mirror Port

This section assumes basic knowledge of how to configure a SPAN port in a Cisco switch, or the equivalent in a Nortel switch.

To use the mirror port, you need a Check Point deployment that includes a Security Management Server, a gateway, and a SmartDashboard. For more about evaluating Check Point products or setting up the mirror port, contact your Check Point representative.
Connecting the Gateway to the Traffic

To connect the Security Gateway to your network traffic:

Configure a SPAN port on a switch that your network traffic travels through, and connect it with a cable to an interface of a Check Point gateway machine. After you configure the interface as a mirror port, all of the traffic on the switch is duplicated and sent through this interface.

Configuring the Interface as a Mirror Port

To set the connected interface as mirror port

1. In the command line of the Security Gateway, run: `sysconfig`.
2. Select Network Connections.
3. Select Configure Connections.
4. Select the interface that should be configured as mirror-port. This is the one that you connected.
5. Select Define as connected to a mirror port.
6. Enable the Application Control blade in SmartDashboard. You can also enable the IPS blade to see IPS traffic. If you only want to enable the IPS blade, you must activate at least one HTTP protection.
7. Install the Policy.

Checking that it Works

To make sure the mirror port is configured and connected properly:

- Browse to an internet site, such as Google.
- Open SmartView Tracker. You should see traffic of the blade you enabled.

Removing the Mirror Port

To remove the mirror port from the interface:

1. In the command line of the Security Gateway, run: `sysconfig`.
2. Select Network Connections.
3. Select Configure Connections.
4. Select the interface that you want to remove the mirror-port from.
5. Select Remove the connection to the mirror port.
6. Install the Policy.
Index

A
Action • 17, 38
Active Directory Based Configuration • 64
Adding a New Host Site • 38
Adding a Server Certificate • 35
Adding Trusted CAs for Outbound HTTPS Inspection • 40
Advanced Settings for Application and URL Filtering • 31
Application and URL Filtering and Identity Awareness • 48
Application Categories • 26
Application Control and URL Filtering Event Queries • 56
Application Control and URL Filtering in SmartEvent • 55
Application Control and URL Filtering in SmartView Tracker • 52
Application Control and URL Filtering Licensing and Contracts • 9
Application Control and URL Filtering Logs • 52
Application Control Backwards Compatibility • 47
Application Risk Levels • 26
Applications/Sites • 17
Applications/Sites Pane • 29
AppWiki • 28
Architecture • 50
Automatically Updating the Trusted CAs List • 40

B
Blade • 39
Blade Queries • 45
Blocking Applications • 11
Blocking Sites • 13
Blocking URL Categories • 14
Bypassing HTTPS Inspection to Software Update Services • 39

C
Certificate • 39
Certificate Blacklisting • 42
Check Point Online Web Service • 46
Checking that it Works • 72
Client and Gateway Communication • 62
Configuring a Mirror Port • 71
Configuring Inbound HTTPS Inspection • 35
Configuring Legacy URL Filtering • 50
Configuring Outbound HTTPS Inspection • 32
Configuring the Hit Count Display • 21
Configuring the Hit Count Timeframe • 22
Configuring the Interface as a Mirror Port • 72
Configuring the Security Gateway for UserCheck • 58
Configuring UserCheck • 58
Connecting the Gateway to the Traffic • 72
Connecting to the Internet for Updates • 27
Connection Unification • 47
Creating an Application Control and URL Filtering Policy • 10
Creating an Outbound CA Certificate • 33
Creating Application or Site Groups • 30
Creating Applications or Sites • 29
Creating Categories • 30
Creating Rules • 10
Creating UserCheck Interaction Objects • 22

D
Default Rule and Monitor Mode • 15
Deploying Certificates by Using Group Policy • 35
Destination • 17, 37
Detected in My Organization • 28
Distributing and Connecting Clients • 68
DNS Based Configuration • 66

E
Enabling Application Control on a Security Gateway • 9
Enabling HTTPS Inspection • 33
Enabling or Disabling Hit Count • 20
Enabling URL Filtering on a Security Gateway • 9
Enabling UserCheck Client • 61
Engine Settings • 46
Event Analysis in SmartEvent • 45
Event Analysis in SmartEvent or SmartEvent Intro • 55
Exporting a Certificate from the Security Management Server • 34
Exporting and Deploying the Generated CA • 34
Exporting and Importing Applications or Sites • 31

F
Fail Mode • 46
File Name Based Server Discovery • 63

G
Gateways Pane • 39
GatewaysPane • 29
Getting Started • 9
Getting the MSI File • 68
Glossary • 7

H
Helping Users • 70
Hit Count • 20
Hits • 16
How It Operates • 32
HTTP Inspection on Non-Standard Ports • 31
HTTP/HTTPS Proxy • 43
HTTPS Inspection • 32
HTTPS Inspection in SmartEvent • 45
HTTPS Inspection in SmartView Tracker • 44
HTTPS Inspection Queries • 44
HTTPS Validation • 41

I
Identifying Users Behind a Proxy • 49
Important Information • 3
Importing an Outbound CA Certificate • 33
| L | Legacy URL Filtering • 49  
| Limit Objects • 20  
| Limiting Application Traffic • 11  
| Log Sessions • 52 |
| M | Main Features • 7  
| Managing Application Control and URL Filtering • 15  
| Manually Updating a Trusted CA • 40  
| Messages and Action Items • 28  
| Monitoring Applications • 10  
| More UserCheck Interaction Options • 24  
| My Organization • 28 |
| N | Name • 16, 37  
| Number (No.) • 37  
| Number (NO.) • 16 |
| O | Option Comparison • 62  
| Overriding Categorization • 31 |
| P | Parts of the Rule • 36  
| Parts of the Rules • 16  
| Permissions for HTTPS Logs • 45  
| Permissions for Logs • 53  
| Predefined Queries • 53  
| Predefined Rule • 36 |
| R | Refreshing the Hit Count Data • 22  
| Remote Registry • 68  
| Removing the Mirror Port • 72  
| Renaming the MSI • 64  
| Revoking Incidents • 60 |
| S | Saving a CA Certificate • 41  
| Scheduling Updates • 27  
| Security Category Updates • 25  
| Server Certificates • 35  
| Server Configuration Rules • 64  
| Server Validation • 41  
| Services • 37  
| Setting up a Mirror Port • 71  
| Site Category • 37  
| Source • 16, 37 |
| T | Technical Requirements • 71  
| Terminology • 49  
| The Application and URL Filtering Database • 25  
| The Application and URL Filtering Overview Pane • 28  
| The Check Point Solution for Application Control and URL Filtering • 7  
| The HTTPS Inspection Policy • 36  
| The Need for Application Control • 6  
| The Need for URL Filtering • 6  
| The Policy Rule Base • 15  
| The SmartEvent Intro Overview Page • 56  
| Time • 19  
| Top Users • 28  
| Track • 18, 38  
| Troubleshooting • 43  
| Troubleshooting DNS Based Configuration • 67  
| Trusted Gateways • 65 |
| U | Updating the Application and URL Filtering Database • 27  
| UserCheck CLI • 59  
| UserCheck Client • 61  
| UserCheck Client Overview • 61  
| UserCheck Frequency and Scope • 23  
| UserCheck Interaction Objects • 22  
| UserCheck Page • 24  
| UserCheck Requirements • 61  
| UserCheck with Check Point Password Authentication • 69  
| Using Identity Awareness Features in Rules • 12  
| Using Identity Awareness in the Application and URL Filtering Rule Base • 48  
| Using the AppWiki • 26 |
| V | Viewing Information in SmartEvent • 46, 55  
| Viewing Information in SmartEvent Intro • 56  
| Viewing Logs • 53 |
| W | Web Browsing • 47 |