Application Control and URL Filtering

Pre-R80 Security Gateways with R80 Security Management

Administration Guide
Important Information

Check Point R80
For more about this release, see the R80 home page

Latest Version of this Document
Download the latest version of this document
To learn more, visit the Check Point Support Center

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 Pre-R80 Security Gateways with R80 Security Management
Administration Guide.

Searching in Multiple PDFs
To search for text in all the R80 PDF documents, download and extract the complete
R80 documentation package
Use Shift-Control-F in Adobe Reader or Foxit reader.
To search for all text in the R77 PDF documents, download and extract the R77
documentation package

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>31 March 2016</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
About this Guide

In This Section:
R80 SmartConsole Toolbars ................................................................. 6

This guide explains how to manage backward compatible (R77.xx and lower) Security Gateways with the R80 SmartConsole.

This guide shows only the updated procedures. To learn more about earlier features, see the R77 documentation http://supportcontent.checkpoint.com/documentation_download?ID=26770.

R80 SmartConsole Toolbars

Global Toolbar (top left of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description and Keyboard Shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>The main R80 SmartConsole Menu</td>
</tr>
<tr>
<td>The <strong>Objects</strong> menu.</td>
</tr>
<tr>
<td>Also leads to the Object Explorer <strong>Ctrl+E</strong></td>
</tr>
<tr>
<td>Install policy on managed gateways</td>
</tr>
<tr>
<td><strong>Ctrl+Shift+Enter</strong></td>
</tr>
</tbody>
</table>

Navigation Toolbar (left side of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description and Keyboard Shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway configuration view</td>
</tr>
<tr>
<td><strong>Ctrl+1</strong></td>
</tr>
<tr>
<td>Security Policies Access Control view</td>
</tr>
<tr>
<td>Security Policies Threat Prevention view</td>
</tr>
<tr>
<td><strong>Ctrl+2</strong></td>
</tr>
<tr>
<td>Logs &amp; Monitor view</td>
</tr>
<tr>
<td><strong>Ctrl+3</strong></td>
</tr>
<tr>
<td>Manage &amp; Settings view - review and configure the Security Management Server settings</td>
</tr>
<tr>
<td><strong>Ctrl+4</strong></td>
</tr>
</tbody>
</table>
# Command Line Interface Button (left bottom corner of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description and Keyboard Shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open a command line interface for management scripting and API</td>
</tr>
<tr>
<td>F9</td>
</tr>
</tbody>
</table>

# What’s New Button (left bottom corner of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description and Keyboard Shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open a tour of the R80 SmartConsole</td>
</tr>
</tbody>
</table>

# Objects and Validations Tabs (right side of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objects</td>
</tr>
<tr>
<td>Validations</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Objects</td>
</tr>
<tr>
<td>Manage security and network objects</td>
</tr>
<tr>
<td>Validations</td>
</tr>
<tr>
<td>Validation warnings and errors</td>
</tr>
</tbody>
</table>

# System Information Area (bottom of R80 SmartConsole)

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task List</td>
</tr>
<tr>
<td>Server Details</td>
</tr>
<tr>
<td>Connected Users</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task List</td>
</tr>
<tr>
<td>Management activities, such as policy installation tasks</td>
</tr>
<tr>
<td>Server Details</td>
</tr>
<tr>
<td>The IP address of the Security Management Server</td>
</tr>
<tr>
<td>Connected Users</td>
</tr>
<tr>
<td>The administrators that are connected to the Security Management Server</td>
</tr>
</tbody>
</table>
Getting Started with URL Filtering

In This Section:

- Application Control and URL Filtering Contracts ......................................................... 8
- Enabling Application and URL Filtering on a Security Gateway ............................... 8
- Enabling Application and URL Filtering in the Access Control Policy ....................... 9
- Monitoring Application and URL Filtering ................................................................. 9
- Creating an Application Control and URL Filtering Policy ......................................... 10

The information here applies to the second Policy Layer, which is Application and URL Filtering.

Application Control and URL Filtering Contracts

You must have a contract for Application Control and URL Filtering for each Security Gateway on which these blades are enabled. This is in addition to the Security Gateway license. For clusters, make sure you have a contract and license for each cluster member.

New installations and upgraded installations include a 30 day trial license and contract. 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 the URL Filtering blade are disabled. When contracts are about to expire or are already expired, warnings show in:

- The Audit tab of the Logs & Monitor view.
- The Check Point User Center, when you log in to your account.

Enabling Application and URL Filtering on a Security Gateway

You can enable the Application Control Software Blade, the URL Filtering Software Blade, or both of them, on each Security Gateway.

Note - For Application and URL Filtering to work properly, you must also enable Application and URL Filtering in the Access Control Policy.

To enable Application and URL Filtering on a Security Gateway:

1. In R80 SmartConsole go to the Gateways & Servers view.
2. Double-click a Security Gateway object.
   - The Gateway Properties window opens.
4. In the Network Security tab, select Application Control or URL Filtering, or both, as necessary.
5. Click OK.
6. Install the Policy.
To see which Security Gateways enforce Application and URL Filtering:
1. In the **Gateways & Servers** view of R80 SmartConsole, look at the **Active Blades** column.
2. Look for the Gateways with these Software Blades enabled:
   - Application Control
   - URL Filtering

### Enabling Application and URL Filtering in the Access Control Policy

After upgrading a Security Management Server from R77.x to R80, the Firewall Policy and the Application and URL Filtering Policy are converted to these Policy Layers:
- **Network** - Firewall Software Blade is enabled
- **Application** - Firewall and Application and URL Filtering Software Blades are enabled

For the Application Control Policy Layer to work, make sure that both - Firewall and Application and URL Filtering Software Blades are enabled in it.

To enable Application and URL Filtering in the Access Control Policy:
1. In R80 SmartConsole go to the **Security Policies** view.
2. In the Access Control section, right-click **Policy** and select **Edit Layer**.
   The **Policy** window opens.
3. Make sure that **Access Control Policy Type** is selected.
4. In the Access Control Policy section, double-click Policy Layer.
5. In the window that opens, select **Applications & URL Filtering**.
6. Click **OK**.
7. Click **OK**.
8. Install the Policy.

### Monitoring Application and URL Filtering

To see logs for Application and URL Filtering:
1. In R80 SmartConsole, go to the **Logs & Monitor** view.
2. Click the **Favorites** icon 🌟.
3. Select **Access > By Blade > Application Control** or **Access > By Blade > URL Filtering**.

The logs show how applications are used in your environment and help you create effective Rule Bases.
Creating an Application Control and URL Filtering Policy

Create and manage the Policy for Application Control and URL Filtering in the Access Control Policy, in the Security Policies view of R80 SmartConsole. The Access Control 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 Policy pane contains the Rule Base, which is the primary component of your Application Control and URL Filtering Policy. Click one of the Add rule buttons to get started.
- To learn which applications and categories have a high risk, look through the AppWiki in the Access Tools part of the Security Policies view. Find ideas of applications and categories to include in your Policy.
- To see an overview of your Access Control Policy and traffic, see Access tab of the Logs & Monitor view. (SmartEvent license required.)

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 Security Policies view of R80 SmartConsole, go to the Access Control Policy.
2. Choose the Application Control Layer.
3. 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.
4. Create 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.
   - Services & Applications - Click the plus sign to open the Application viewer. Add the Facebook application to the rule:
### Getting Started with URL Filtering

- Start to type "face" in the Search field. In the Available list, see the Facebook application.

  ![Facebook Application Screen](image)

- Click each item to see more details in the description pane.
- Select the items to add to the rule.

  **Note** - Applications are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control Web browsing services: `http`, `https`, `HTTP_proxy`, and `HTTPS_proxy`. To change this see Changing Services for Applications and Categories (on page 20).

  - **Action** - Select **Accept**
  - **Track** - Select **Log**
  - **Install On** - Keep it as **Policy Targets** for or all gateways, or choose specific Security Gateways on which to install the rule

The rule allows all Facebook traffic but logs it. You can see the log data in the **Logs & Monitor** view, in the **Logs** tab. To monitor how people use Facebook in your organization, see the **Access Control** tab (SmartEvent Server required).

### Blocking Applications

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

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

1. In the Security Policies view of R80 SmartConsole, go to the **Access Control** Policy.
2. Choose the **Application Control** Layer.
3. Click one of the **Add Rule** toolbar buttons to add the rule in the position that you choose in the Rule Base.
4. Create a rule that includes these components:
   - **Services & Applications** - Select the **YouTube** category.
Note - Applications are matched on their Recommended services, where each service runs on a specific port, such as the default Application Control Web browsing services: http, https, HTTP_proxy, and HTTPS_proxy. To change this see Changing Services for Applications and Categories [on page 20].

- **Action** - Drop, and optionally, a UserCheck **Blocked Message - Access Control**
  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

**Note**: This Rule Base example contains only those columns that are applicable to this subject.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Porn</td>
<td>Any</td>
<td>Internet</td>
<td>YouTube</td>
<td>Drop</td>
<td>Log</td>
<td>Policy Targets</td>
</tr>
</tbody>
</table>

The rule blocks traffic to YouTube and logs attempts to access sites that are in the pornography category. Users who violate the rule receive a 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 different 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 Security Policies view of R80 SmartConsole, go to the **Access Control** Policy.
2. Choose the **Application Control** Layer.
3. Click one of the **Add Rule** toolbar buttons to add the rule in the position that you choose in the Rule Base.
4. Create a rule that includes these components:
   - **Services & Applications - Media Streams** category.

**Note** - Applications are matched on their Recommended services, where each service runs on a specific port, such as the default Application Control Web browsing services: http, https, HTTP_proxy, and HTTPS_proxy.
**Getting Started with URL Filtering**

Application Control and URL Filtering Administration Guide Pre-R80 Security Gateways with R80 Security Management

https, HTTP_proxy, and HTTPS_proxy. To change this see Changing Services for Applications and Categories (on page 20).

- **Time** - Add a Time object that specifies the hours or time period in which the rule is active.

  **Note** - The Time column is not shown by default in the Rule Base table. To see it, right-click on the table header and select Time.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services and Applications</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 Upload_1Gbps</td>
<td>Log</td>
<td>All</td>
<td>Off-Work</td>
</tr>
</tbody>
</table>

**Note** - In a cluster environment, the specified bandwidth limit is divided between all defined cluster members, whether active or not. For example, if a rule sets 1Gbps limit in a three member cluster, each member has a fixed limit of 333 Mbps.

**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 Identified_Users 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
   - **Services & Applications** - Radmin
   - **Action** - Accept

2. Create another rule below and include these components:
   - **Source** - Any
   - **Destination** - Internet
   - **Services & Applications** - The category: Remote Administration
   - **Action** - Block
Getting Started with URL Filtering

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</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>Log</td>
<td>All</td>
</tr>
<tr>
<td>Block other Remote Admins</td>
<td>Any</td>
<td>Internet</td>
<td>Remote Administration</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.

- Applications are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control Web browsing services: http, https, HTTP_proxy, and HTTPS_proxy. To change this see Changing Services for Applications and Categories (on page 20).

**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.
  - A custom application for a site named FreeMovies.

- 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 the previously defined custom site named FreeMovies.

**To create a custom group:**

1. In the Object Explorer, click **New > More > Custom Application/Site > Application/Site Group**.
2. Give the group a name. For example, **Liability_Sites**.
3. Click + to add the group members:
   - Search for and add the custom application FreeMovies.
   - You can now use the group in the Access Control Rule Base.
4. Click **Close**
In the Rule Base, add a rule similar to this:

In the Security Policies view of R80 SmartConsole, go to the **Access Control** Policy.

- **Source** - The **Identified_Users** access role
- **Destination** - Internet
- **Services & Applications** - **Liability_Sites**
- **Action** - Drop

**Note** - Applications are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control Web browsing services: **http**, **https**, **HTTP_proxy**, and **HTTPS_proxy**. To change this see Changing Services for Applications and Categories (on page 20).

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</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>Drop</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:

- **Source** - The **Identified_Users** access role
- **Destination** - Internet
- **Services & Applications** - **Pornography** category
- **Action** - Drop

**Note** - Categories are matched on their **Recommended** services, where each service runs on a specific port, such as the default Application Control Web browsing services: **http**, **https**, **HTTP_proxy**, and **HTTPS_proxy**. To change this see Changing Services for Applications and Categories (on page 20).

**Changed Behavior with R80 Management**

After an upgrade to R80 management, all applications and categories use the recommended services. To change this see Changing Services for Applications and Categories (on page 20).
Managing Application and URL Filtering

In This Section:

Managing Pre-R80 Security Gateways ................................................................. 16
The Columns of the Access Control Rule Base ...................................................... 17
Types of Rules in the Rule Base .............................................................................. 18
Services & Applications ......................................................................................... 18
Changing Services for Applications and Categories .............................................. 20
Overriding Categorization for a URL ................................................................. 20
Log Sessions ......................................................................................................... 20
Tracking Options .................................................................................................. 21
Time ..................................................................................................................... 21
Adding a Limit Object to a Rule ........................................................................... 22
Enabling or Disabling Hit Count ........................................................................... 23
Configuring the Hit Count Display ....................................................................... 23
UserCheck Interaction Objects ............................................................................. 24
The Application and URL Filtering Database .................................................. 26
Application and URL Filtering Advanced Settings ............................................. 30
HTTPS Inspection ................................................................................................ 31
Using Identity Awareness in the Rule Base ............................................................ 37
Using Application and URL Filtering with VSX .................................................. 38


See the logs in the Logs tab of the Logs & Monitor view.

See real-time traffic statistics and analysis in the Access Control tab of the Logs & Monitor view, and in the SmartEvent GUI.

This chapter explains the Application Control and URL Filtering configuration and management that you do in the Access Control Policy section of R80 SmartConsole.

Managing Pre-R80 Security Gateways

When you upgrade a pre-R80 Security Management Server that manages pre-R80 Security Gateways to R80, the existing Access Control policies are converted in this way:

- The pre-R80 Firewall policy is converted into the Network Policy Layer of the R80 Access Control Policy. The implicit cleanup rule for it is set to Drop all traffic that is not matched by any rule in this Layer.
- The pre-R80 Application & URL Filtering policy is converted into the Application Policy Layer, which is the second Layer of the R80 Access Control Policy. The implicit cleanup rule for it is set to Accept all traffic that is not matched by any rule in this Layer.

Important – After upgrade, do not change the Action of the implicit cleanup rules, or the order of the Policy Layers. If you do, the policy installation will fail.
New Access Control Policy for pre-R80 Security Gateways on an R80 Security Management Server must have this structure:

1. The first Policy Layer is the Network Layer (with the Firewall blade enabled on it).
2. The second Policy Layer is the Application and URL Filtering Layer (with the Application & URL Filtering blade enabled on it).
3. There are no other Policy Layers.

If the Access Control Policy has a different structure, the policy will fail to install.

You can change the names of the Layers, for example, to make them more descriptive.

Each new Policy Layer will have the explicit default rule, added automatically and set to Drop all the traffic that does not match any rule in that Policy Layer. We recommend that the Action is set to Drop for the Network Policy Layer and Accept for the Application Control Policy Layer.

If you remove the default rule, the Implicit Cleanup Rule will be enforced. The Implicit Cleanup Rule is configured in the Policy configuration window and is not visible in the Rule Base table. Make sure the Implicit Cleanup Rule is configured to Drop the unmatched traffic for the Network Policy Layer and to Accept the unmatched traffic for the Application Control Policy Layer.

The Columns of the Access Control Rule Base

These are the fields of the rules in the Access Control policy. Not all of these are shown by default. To select a field that does not show, right-click on the Rule Base table header, and select it.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Rule number in the Rule Base Layer.</td>
</tr>
<tr>
<td>Hits</td>
<td>Number of connections that match this rule.</td>
</tr>
<tr>
<td>Name</td>
<td>Name that the system administrator gives this rule.</td>
</tr>
<tr>
<td>Source</td>
<td>Network object that defines where the traffic starts.</td>
</tr>
<tr>
<td>Destination</td>
<td>Network object that defines the destination of the traffic.</td>
</tr>
<tr>
<td>Services &amp; Applications</td>
<td>Services, Applications, Categories, and Sites. If Application and URL Filtering is not enabled, only Services show.</td>
</tr>
<tr>
<td>Action</td>
<td>Action that is done when traffic matches the rule. Options include: Accept, Drop, Ask, Inform [UserCheck message], and Reject.</td>
</tr>
<tr>
<td>Track</td>
<td>Tracking and logging action that is done when traffic matches the rule.</td>
</tr>
<tr>
<td>Install On</td>
<td>Network objects that will get the rule(s) of the policy.</td>
</tr>
<tr>
<td>Time</td>
<td>Time period that this rule is enforced.</td>
</tr>
<tr>
<td>Comment</td>
<td>An optional field that lets you summarize the rule.</td>
</tr>
</tbody>
</table>
Types of Rules in the Rule Base

There are three types of rules in the Rule Base - explicit, implied and implicit.

Explicit rules
The rules that the administrator configures explicitly, to allow or to block traffic based on specified criteria.

⚠️ Important - The Cleanup rule is a default explicit rule and is added with every new layer. You can change or delete the default Cleanup rule. We recommend that you have an explicit cleanup rule as the last rule in each layer.

Implied rules
The default rules that are available as part of the Global properties configuration and cannot be edited. You can only select the implied rules and configure their position in the Rule Base:

- First - Applied first, before all other rules in the Rule Base - explicit or implied
- Last - Applied last, after all other rules in the Rule Base - explicit or implied, but before the Implicit Cleanup Rule
- Before Last - Applied before the last explicit rule in the Rule Base

Implied rules are configured to allow connections for different services that the Security Gateway uses. For example, the Accept Control Connections rules allow packets that control these services:

- Installation of the security policy on a Security Gateway
- Sending logs from a Security Gateway to the Security Management Server
- Connecting to third party application servers, such as RADIUS and TACACS authentication servers

Implicit cleanup rule
The default "catch-all" rule that deals with traffic that does not match any explicit or implied rules in the Policy Layers. For R77.30 or earlier versions Security Gateways, the action of the implicit rule depends on the Policy Layer:

- Drop - for the Network Layer
- Accept - for the Application Control Layer

Note - If you change the default values, the policy installation will fail.

The implicit rules do not show in the Rule Base.

Services & Applications
In the Services & Applications column, define the Web applications, sites, services and protocols that are included in the rule. A rule can contain one or more:

- Applications
- Web sites
- Services
• Default categories of Internet traffic
• Custom groups or categories that you create, that are not included in the Check Point Application and URL Filtering Database.

Notes -
It is not supported to configure a service and application in the same rule.

Applications are matched on their Recommended services, where each service runs on a specific port. The recommended services for Facebook, for example, are the default Application Control Web browsing services: http, https, HTTP_proxy, and HTTPS_proxy. To change this see Changing Services for Applications and Categories (on page 20).

To add an application or site to a rule:
1. In the Security Policies view of R80 SmartConsole, go to the Access Control Policy.
2. Select the Application Control Layer.
3. Right-click the Services & Applications cell for the rule and select Add New Items.
   The Application viewer window opens.
4. Search for the applications or categories.
5. Click the + next to the ones you want to add.

To create a new application or site:
1. In the Security Policies view of R80 SmartConsole, go to the Access Control Policy.
2. Select the Application Control Layer.
3. Right-click the Services & Applications cell for the rule and select Add New Items.
   The Application viewer window opens.
4. Click New > Custom Applications/Site > User Application.
5. Enter a name for the object.
6. Enter one or more URLs.
   If you used a regular expression in the URL, click URLs are defined as Regular Expressions.
   Note - If the application or site URL is defined as a regular expression you must use the correct syntax.
7. Click OK.

To create a custom category:
1. In the Security Policies view of R80 SmartConsole, go to the Access Control Policy.
2. Select the Application Control Layer.
3. Right-click the Services & Applications cell for the rule and select Add New Items.
   The Application viewer window opens.
4. Click New > Custom Applications/Site > User Category.
5. Enter a name for the object.
6. Enter a description for the object.
7. Click OK.
Changing Services for Applications and Categories

By default, applications and categories are matched on their recommended services.

To change the services that are matched for an application or category:

1. In the Application and URL Filtering Layer, double-click an application or category in a rule.
2. Select Match Settings.
3. Select an option:
   a) To add or remove services, select Customize and use the Application Viewer to add all
      services that are matched for this application in the Rule Base.
   b) To match the application with all services, select Any.
   c) To exclude specified services, select Negate and use the Application Viewer to select the
      services to exclude.
4. Click OK

The application or category is changed everywhere that it is used in the policy.

Overriding Categorization for a URL

To override categorization for a URL:

1. From the Objects tab of R80 SmartConsole, select New > More > Custom Application/Site >
   Override Categorization.
   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. Select a Primary Category from the list.
5. Select a Risk from the list.
6. To add additional categories, click Add +.
7. Select the categories and click OK.
   The selected categories are shown in the Additional Categories list.
8. Click OK.

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.
Tracking Options

- **Network Log** - Generates a log with only basic Firewall information: Source, Destination, Source Port, Destination Port, and Protocol.

- **Log** - Equivalent to the Network Log option, but also includes the application name (for example, Dropbox), and application information (for example, the URL of the Website). This is the default Tracking option.

- **Full Log** - Equivalent to the log option, but also records data for each URL request made.
  - If suppression is not selected, it generates a **complete log** (as defined in pre-R80 management).
  - If suppression is selected, it generates an **extended log** (as defined in pre-R80 management).

- **None** - Do not generate a log.

You can add these options to a **Log**, **Full Log**, or **Network Log**:

- **Accounting** - If selected, update the log every 10 minutes, to show how much data has passed in the connection: Upload bytes, Download bytes, and browse time.

- **Suppression** - If selected, one log is generated every three hours for all the connections.

**Alert**:

If an **Alert** is selected, **Log** is selected automatically.

- **None** - Do not generate an alert.

- **Alert** - Generate a log and run a command, such as: Show a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in the **Menu > Global Properties > Log and Alert > Alerts**.

- **SNMP** - Send an SNMP alert to the SNMP GUI, or run the script defined in: **Menu > Global Properties > Log and Alert > Alerts**.

- **Mail** - Send an email to the administrator, or run the mail alert script defined in: **Menu > Global Properties > Log and Alert > Alerts**.

- **User Defined Alert** - Send one of three possible customized alerts. The alerts are defined by the scripts specified in the **Menu > Global Properties > Log and Alert > Alerts**.

**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 one or more Time objects and Time Groups in a rule. A Time Group contains 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.

To add the Time Column to the Access Control Policy:
1. Right-click the heading row of the Access Control Policy.
2. Select Time.

To create a new Time object:
1. In the Time column of a rule, select Add New Items.
2. Click New and select Time.
3. Enter a Name without spaces.
4. Select one or more options:
   - Time Period - Select a Start and End date and time for the rule.
   - Hour Ranges - Select hours of the day when the rule is active.
   - Day Recurrence - Select days of the week or month when the rule is active. The default is Every Day.
5. Click OK.

To add Time objects to a rule:
1. In the Time column of a rule, select Add New Items.
2. Select from the available objects.

Notes -
- 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.
- If a rule in a Policy Layer has the Time criteria specified, acceleration templates for rules that follow it in the same Policy Layer are disabled.

Adding a Limit Object to a Rule

To add a Limit object to a rule:
1. In the Access Control Rule Base, in an Application Control Layer rule that has the action Accept, Ask or Inform, select the Action cell.
2. Select More > Limit.
3. Select a limit.
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.
Enabling or Disabling Hit Count

By default, Hit Count is globally enabled for all supported Security Gateways (from R75.40). The timeframe setting that defines the data collection time range is configured globally. If necessary, you can disable Hit Count for one or more Security Gateways.

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. In R80 SmartConsole, click Menu > 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 for the Security Gateway, select Hit Count from the navigation tree.
2. Select Enable Hit Count to enable the feature or clear it to disable Hit Count.
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
  - 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.

<table>
<thead>
<tr>
<th>Hit Count Level</th>
<th>Icon</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero</td>
<td>![Icon]</td>
<td>0 hits</td>
</tr>
<tr>
<td>Low</td>
<td>![Icon]</td>
<td>Less than 10 percent of the hit count range</td>
</tr>
<tr>
<td>Medium</td>
<td>![Icon]</td>
<td>Between 10 - 70 percent of the hit count range</td>
</tr>
<tr>
<td>High</td>
<td>![Icon]</td>
<td>Between 70 - 90 percent of the hit count range</td>
</tr>
<tr>
<td>Very High</td>
<td>![Icon]</td>
<td>Above 90 percent of the hit count range</td>
</tr>
</tbody>
</table>

**To show the Hit Count in the Rule Base:**
Right-click the heading row of the Rule Base and select **Hits**.

**To configure the Hit Count in a rule:**
1. Right-click the rule number of the rule.
2. Select **Hit Count** and one of these options (you can repeat this action to configure more options):
   - **Timeframe** - Select **All**, **1 day**, **7 days**, **1 month**, or **3 months**
   - **Display** - Select **Percentage**, **Value**, or **Level**

**To update the Hit Count in a rule:**
1. Right-click the rule number of the rule.
2. Select **Hit Count > Refresh**.

**UserCheck Interaction Objects**
UserCheck Interaction Objects add flexibility and give the Security Gateway a mechanism to communicate with users. UserCheck objects are used in a Rule Base to:

- Help users with decisions that can be dangerous to the organization security.
- Share the organization 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 browser redirects to the Gaia Administration web portal on port 443 or 80. The portal hosts UserCheck notifications.

**Working with UserCheck Interaction Objects**
- 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.

For more about configuring UserCheck on the gateway and the UserCheck client, see Configuring UserCheck (“Working with UserCheck” on page 46).

Creating UserCheck Interaction Objects

Create a UserCheck Interaction object from the **Access Tools > UserCheck** page of the Access Control tab.

**To create a UserCheck object that includes a message:**

1. In the Security Policies view of R80 SmartConsole, go to the **Access Control** Policy.
2. Click **Access Tools > UserCheck**.
3. Click **New**, and select one of these interaction modes:
   - **Ask UserCheck** - Show a message to users that asks them if they want to continue with the request or not.
   - **Block UserCheck** - Show a message to users and block the application request.
   - **Inform UserCheck** - Show an informative message to users. Users can continue to the application or cancel the request.

   The **UserCheck Interaction** window opens on the **Message** page.
4. Enter a name for the UserCheck object and, optionally, a comment.
5. Select a language (English is the default) from the **Languages** tabs.
6. Enter the message content. You can:
   - Use the formatting toolbar to change text color, alignment, add or remove bullets.
   - Use the **Insert field** variables.
7. In the **Settings** tab, configure optional settings:
   - **Fallback Action** - When UserCheck notification cannot be displayed, this action is taken
   - **External Port** - When selected, redirects the user to the specified **External Port** (enter the URL), and the UserCheck message is not shown to the end-user
     Select **Add UserCheck Incident ID to the URL query**, to log the incident
8. Click **OK**.

   This creates the UserCheck object and web page notification for the portal.

Localizing and Customizing the UserCheck Portal

After you set the UserCheck interaction object language, you can translate the Portal **OK** and **Cancel** buttons to the applicable language. For more information, see: sk83700 http://supportcontent.checkpoint.com/solutions?id=sk83700.

The UserCheck predefined notifications are translated to English, French, Spanish, and Japanese.

**To support more languages:**

1. In **UserCheck Interaction > Message**, click **Languages**.
2. In the list, select the languages.
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 the Action cell of a rule in the Access Control Policy, and click More.
2. In the Action Settings window, select the UserCheck Frequency. The options are:
   - Once a day
   - Once a week
   - Once a month
   - Custom frequency
3. Select Confirm UserCheck. This sets if the notifications are:
   - Per rule
   - Per category
   - Per application
   - Per data type

Example:
In a rule that contains:

<table>
<thead>
<tr>
<th>Services &amp; Applications</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Networking category</td>
<td>Inform</td>
</tr>
</tbody>
</table>

If you select a UserCheck Frequency of Once a day, and Confirm UserCheck of Per rule:
A user who accesses Facebook and then LinkedIn on the same day gets one Inform message.

If you select a UserCheck Frequency of Once a day, and Confirm UserCheck of Per application:
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 Confirm UserCheck Scope default is Per category.
In upgrades from a version before R75.40, the Confirm UserCheck default is Per Rule.

The Application and URL Filtering Database

The Check Point Application and URL Filtering Database contains thousands of known applications, social media widgets, and more than 150 million categorized URLs. Check Point continuously updates this database with new and changed applications and URLs. Each database record contains a description, one or more categories, and a risk level.

Security Gateways keep these resources on its local disk to improve inspection performance:
- A database with the most commonly used URLs and their related categories.
- A local cache that can return results for up to 99% of URL categorization requests.
If the cache does not contain the category information for a URL, Application and URL Filtering looks in the local database and then goes to the Check Point Online Web Service. If a URL is likely to be a widget, Application and URL Filtering goes directly to the Check Point Online Web Service.

**Working with the Application and URL Filtering Database**

You can work with the Application and URL Filtering Database from:

- **R80 SmartConsole** - From the Application Control Rule Base in R80 SmartConsole, click the plus sign in the **Services & Application** column. You can select and add applications and categories directly into a Rule Base.

- **AppWiki** - Click **Access Tools > AppWiki** on the lower, left side of the **Access Control** page, or go to the Check Point AppWiki website http://appwiki.checkpoint.com/appwikisdb/public.htm.

**Security Category Updates**

The local cache on each Security Gateway keeps URL categorization data up to 24 hours. The frequency of local cache updates are based on the security category.

It is possible that the category assigned to a site or application changes on the Check Point Online Web Service while it is still in the local cache. For example, a URL that was categorized as *Search Engines / Portals*, changed to *phishing*. The Online Web Service updates the local cache for URLs with critical security categories (such as phishing, malware, botnet, and spam) more frequently.

**Application Categories**

In the Application Database, each application has one **primary category** based on its most defining aspect. You can see the category in the description of each application and in the logs.

Each application can also have additional categories, called **Tags**, which are secondary application characteristics. For example, the primary category for Gmail is *Email*. Gmail also has these additional Tags:

- ‘Sends mail’
- ‘Encrypts communications’

When you use the AppWiki or add applications to a Rule Base, you can filter by Tags and risk level to see all applications with that characteristic. This is a good way to see which types of applications you can block or allow.

Access Control Rules match an application’s primary category and its Tags. If the primary category changes, or if Tags are added or deleted, the rule matching behavior changes automatically when the Application and URL Filtering Database is updated. For example, if you have a rule that:

- Blocks all applications with the ‘High Bandwidth’ Tag
  and
- And the ‘High Bandwidth’ tag is added to some applications in the Application and URL Filtering Database

Rules that once allowed these applications now block them. If an allowed application is suddenly blocked, use the AppWiki to see if a Tag or the primary category changed.
### Application Risk Levels

The Application and URL Filtering Database and AppWiki show a Risk Level for each application. This table explains what each risk 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>Web Anonymizers, VPN4ALL, VTunnel, Kazaa</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 sharing (uTorrent), Instant Messaging</td>
</tr>
<tr>
<td>3 - Medium</td>
<td>Can cause data leakage or malware infection</td>
<td>Instant messaging, File storage (Dropbox, OneDrive, iDisk, SharePoint-Online), WebEx, Gmail, Instant Messaging</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 an AppWiki or Application and URL Filtering Database search based on the risk level. For example, select risk level 5 to see all applications with a critical risk level. The risk level is also a Tag that shows in the details of each application.

### Updating the Application and URL Filtering Database

The Application and URL Filtering Database on the Security Gateway gets regular, automatic updates that make sure that you have the most current data and newly added applications and websites in the Application and URL Filtering Layer of the Access Control Policy.

By default, updates run on the Security Management Server and Security Gateways once a day. 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 Application and URL Filtering Database on the management server:**

1. In R80 SmartConsole, click **Security Policies > Access Tools > Updates**.
2. In the **Application and URL Filtering** section, click **Update Now**.

**To change the schedule for Application and URL Filtering Database updates on the management server:**

1. In R80 SmartConsole, click **Security Policies > Access Tools > Updates**.
2. Click **Schedule Update**.
3. Select **Enable Application Control & URL Filtering Scheduled Update**.
4. Click **Configure** to schedule when the updates will run. By default, a scheduled update runs once a day.
In Multi-Domain Security Management, update the database for all Domain Management Servers in the Global R80 SmartConsole 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.

Security Policies > Access Tools > Updates shows if the Security Management Server uses a proxy to connect to the Internet.

To configure a proxy for the Security Management Server:

2. Click Configure Proxy.
3. In the Proxy Configuration window, in the Use proxy field, enter the domain name or IP address of the proxy, and the Port number.

To Configure IPv6 proxy support:

If the proxy uses an IPv6 address:

1. On the Windows computer, running R80 SmartConsole client, go to Start menu and open Control Panel > System and Security > System > Advanced System Settings.
2. Open the Advanced tab > Environment variables.
3. Create a new User Variable.
4. Set the value to: updates_over_IPv6=1

**Scheduling Updates**

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

2. Click Schedule Update.
3. Select the target for updates:
   - Security Management Server
   - Security Gateway
4. Click Configure.
5. Set the Time of Event. Set the update interval, and a time of day for updates to occur.
6. Click OK.

If you have Security Gateways or Security Management Servers in different time zones, they will not be synchronized until all of them are updated.
Application and URL Filtering Advanced Settings

You can configure advanced Application and URL Filtering settings. These are global settings that apply to all Security Gateways that have Application and URL Filtering enabled.

To work with advanced settings:

1. On the Main Navigation bar, click Manage & Settings.
2. Select Blades > Application and URL Filtering > Advanced Settings. The Application Settings window opens.
3. Configure settings in the General tab view:
   - **Fail mode** - Select to Allow all requests or to Block all requests when an internal error happens
   - **URL Filtering** - Select one or more of these - Categorize HTTPS websites, Enforce safe search on search engines, Categorize cached pages and translated pages in search engines
   - **Connection unification** - Set Session unification timeout (the default is 180 minutes)
   - **Application Control Web Browsing Services** - Modify service match criteria for web applications
     Select Match web application on 'Any' port when used in 'Block' rule, to optimize resources for processing blocked traffic
   - **Web browsing** - Select Enable web browsing logging and policy enforcement
   - **HTTP Inspection** - Select Enable HTTP Inspection on non-standard ports for Application and URL Filtering
   - **Compatibility with R75 and R75.10 gateways settings** - Select Unify connections from the same User/IP to a specific application into a single session/log and Issue a separate log per each domain accessed, if needed
4. Configure settings in the Check Point online web service tab view:
   - **Block requests when web service is unavailable** - Select to minimize unnecessary traffic processing
   - **Website categorization mode: Hold** - Select Hold to block requests until categorization is complete, Background - to allow requests until categorization is complete, or Custom - to configure different settings for different services
   - **Categorize social networking widgets** - Select to ensure user privacy
5. Click OK.
6. Publish the session and install the policy.

Application Control Web Browsing Services

Application Control Web browsing services are the services that match a Web-based custom Application/Site.

These are the default Application Control Web browsing services:

- http on port 80
- https on port 443
- HTTPS_proxy on port 8080
- HTTP_proxy on port 8080
Other services, such as SSH are not matched.

To add to the list of services that match Web applications:
1. Go to Manage & Settings > blades > Application and URL Filtering > Advanced Settings.
2. In the Application and URL Filtering Settings window:
   a) Click the add icon to open the list of services.
   b) Select a service.

   **Match Web application on 'Any' port when used in Block rule** - By default, this is selected, and applications are matched on all services when used in a Block rule.

**HTTPS Inspection**

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

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

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

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

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

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

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

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 is also used by other Security Management Servers that import the CA certificate to decrypt the file.

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

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

To create an outbound CA certificate:

1. In R80 SmartConsole, go Manage & Settings > Blades > HTTPS Inspection > Configure In SmartDashboard.
2. In SmartDashboard, right-click the Security Gateway object and select Edit.
   The Gateway Properties window opens.
3. In the navigation tree, select HTTPS Inspection.
4. In the HTTPS Inspection page, click Create.
5. 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.
6. Click OK.
7. Export and deploy the CA certificate ("Exporting and Deploying the Generated CA" on page 33).
Exporting and Deploying the Generated CA

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

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

To distribute a certificate with a GPO:
1. From the HTTPS Inspection window of the Security Gateway, click Export certificate.
2. Save the CA certificate file.
3. Use the Group Policy Management Console 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.

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

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

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

To access the HTTPS Inspection Rule Base:
1. In R80 SmartConsole, click Manage & Settings > Blades > HTTP Inspection > Configure in SmartDashboard.
2. In SmartDashboard, click Policy.

Bypassing HTTPS Inspection for Software Update Services

Check Point dynamically updates a list of approved domain names of services from which content is always allowed. This option makes sure that Check Point updates or other 3rd party software updates are not blocked. For example, updates from Microsoft, Java, and Adobe.
To bypass HTTPS inspection for software updates:
1. In R80 SmartConsole, go Manage & Settings > Blades > HTTPS Inspection > Configure In SmartDashboard.
2. In SmartDashboard, click the HTTPS Inspection tab.
3. Click Policy.
4. In the Policy pane, select Bypass HTTPS Inspection of traffic to well known software update services (list is dynamically updated). This option is selected by default.
5. Click list to see the list of approved domain names.

HTTPS Validation

Server Validation

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

Untrusted server certificate

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

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

Revoked server certificate (validate CRL)

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

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

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

To configure the proxy:
1. In R80 SmartConsole, from the Gateways & Servers view, double-click the Security Gateway that requires proxy configuration.
2. Select Network Management > 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 the Logs tab of the R80 SmartConsole Logs & Monitor view or if it triggers other notifications. For the options, see Track.

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.

HTTP/HTTPS Proxy
In R80 SmartConsole, in the Gateways & Servers view, or in SmartDashboard, in the HTTPS Inspection tab > Gateways pane, you can edit a Gateway object. In the HTTP/HTTPS Proxy page, 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 Logs
Logs from HTTPS Inspection are shown in the **Logs & Monitor > Logs** tab. Under **Favorites**, there is a predefined query for HTTPS Inspection logs. It shows all HTTPS traffic that matched the HTTPS Inspection policy and was configured to be logged.

The log includes an **HTTP Inspection Action** 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 R80 SmartConsole, select **Manage & Settings > Permissions and Administrators > Administrator**.
2. Double-click an administrator to edit it.
3. In the **General** page in the **Permissions Profile** field, select the permission profile and click **New**.
4. In the **New Profile** window:
   - Enter a **Name** for the profile.
   - Select **Customized**.
5. In the **Monitoring and Logging** page, select **HTTPS Inspection logs** for permission to see the classified information in the HTTPS Inspection logs.
6. Click **OK** on all of the open windows.

To edit an existing permissions profile:

1. In R80 SmartConsole, select **Manage & Settings > Permissions and Administrators > Permission Profiles**.
2. Double-click a profile to edit it.
3. In the **Monitoring and Logging** page, select **HTTPS Inspection logs** for permission to see the classified information in the HTTPS Inspection logs.
4. Click **OK** on all of the open windows.

Using Identity Awareness in the Rule Base

The Security Gateway examines packets 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 then goes on to the second rule and continues until it matches a rule.

In rules with access roles, you can add a property in the **Action** field to enable 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. The packet is matched according to the other fields in the rule.

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 works 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 action.
  - If it does not match an access role, the next rule is examined.

- When identity data for an IP is unknown and:
  - All rule fields match, other than the source field with an access role.
  - The connection 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.

**Note** - When you set the option to redirect http traffic from unidentified IP addresses to the Captive Portal, make sure to place the rule in the correct position in the Rule Base to avoid unwanted behavior.

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

1. In a policy rule that uses an access role in the **Source** column, right-click the **Action** column and select **More**.
   
   The **Action Settings** window opens.

2. Select the **Enable Identity Captive Portal**.

3. Click **OK**.
   
   The Action column shows that a redirect to the Captive Portal occurs.

This is an example of a Rule Base that describes how matching operates:

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Services &amp; Applications</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Finance_Dept (Access Role)</td>
<td>Finance_web_server</td>
<td>Any</td>
<td>Accept (display Captive Portal)</td>
</tr>
<tr>
<td>2</td>
<td>Admin_IP</td>
<td>Any</td>
<td>Any</td>
<td>Accept</td>
</tr>
<tr>
<td>3</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
</tr>
</tbody>
</table>

**Example 1** - If an unidentified Finance user tries to access the Finance Web Server with http, a redirect to the Captive Portal occurs. After the user enters credentials, the Security Gateway allows access to the Finance Web Server. Access is allowed based on rule number 1, which identifies the user through the Captive Portal as belonging to the Finance access role.

**Example 2** - If an unidentified administrator tries to access the Finance Web Server with http, a redirect to the Captive Portal occurs despite rule number 2. After the administrator is identified, rule number 2 matches. To let the administrator access the Finance Web Server without redirection to the Captive Portal, switch the order of rules 1 and 2 or add a network restriction to the access role.

**Using Application and URL Filtering with VSX**

When you configure Virtual Systems to use the Application Control and URL Filtering, make sure that the VSX Gateway (VS0) can connect to the Internet. Updates are done only through this Virtual System.

**To enable Application and URL Filtering Categories on Virtual Systems:**

1. If applicable, configure proxy settings for the VSX Gateway (VS0):
   a) In R80 SmartConsole, from the **Gateways & Servers** view, double-click the VSX Gateway (VS0).
   b) From the navigation tree, select **Network Management > Proxy**.
   c) Configure the proxy settings, and click **OK**.
2. Enable Application Control and URL Filtering on the required Virtual Systems.
   
   **Note** - You do not have to enable them on the VSX Gateway (VS0).

3. Install policies on the relevant Virtual Systems.
Monitoring Logs and Events for Application and URL Filtering

In This Section:
- Using Logs with Application and URL Filtering .......................................................... 40
- Application Control and URL Filtering in the SmartEvent GUI .................................. 41
- Administrator Permission Profiles.............................................................................. 42

Using Logs with Application and URL Filtering

Viewing Rule Logs

To see logs generated by a specified rule:

1. In R80 SmartConsole, go to the Security Policies view.
2. In the Access Control Policy or Threat Prevention Policy, select a rule.
3. In the bottom pane, click one of these tabs to see:
   - **Summary** - Rule name, rule action, rule creation information, and the hit count. Add custom information about the rule.
   - **Details** - Details per column. Select columns as necessary.
   - **Logs** - Log entries according to specific filter criteria - Source, Destination, Blade, Action, Service, Port, Source Port, Rule (Current rule is the default), Origin, User, or Other Fields.
   - **History** - List of rule operations in chronological order, including the information about the rule type and the administrator that made the change.

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:
In the Logs tab of the Logs & Monitor view, see the Suppressed Logs field of the log.

To configure the session duration:

- For applications or sites that are allowed in the Rule Base, the default session is three hours. You can change this in R80 SmartConsole from the Manage & Settings view, in Blades > Application and URL Filtering > Advanced Settings > General > Connection unification.
- For applications or sites that are blocked in the Rule Base, a session is 30 seconds.
Application Control and URL Filtering Logs

To see logs from Application Control and URL Filtering:

Go to the Logs tab of the Logs & Monitor view, click the Favorites (star) icon, and select Predefined > Access > By Blade > Application Control or URL Filtering. The logs that you see depend on the Tracking Options (on page 21) that you configure in each Application Control and URL Filtering rule in the Access Control Policy Rule Base.

To see logs related to Application and URL Filtering Database updates on the Security Gateway:

Go to the Logs tab of the Logs & Monitor view, click the Favorites (star) icon, and select Predefined > Access >> System.

This also shows logs related to other system related issues, such as problems that the application detection service encounters.

To learn more about logging, see the R80 Logging and Monitoring Administration Guide http://supportcontent.checkpoint.com/documentation_download?ID=46535.

Application Control and URL Filtering in the SmartEvent GUI

Event Analysis in the SmartEvent GUI

SmartEvent has advanced analysis tools with filtering, charts, reporting, and statistics for all events.

The administrator must have HTTPS Inspection permissions to see 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.

We recommend that you use SmartEvent only for these purposes:

• To schedule reports
• To edit the event policy settings

Use R80 SmartConsole for real-time event and log viewing.

To use SmartEvent, you must enable it on the Security Management Server or on a dedicated computer. See the R80 Logging and Monitoring Administration Guide http://supportcontent.checkpoint.com/documentation_download?ID=46535.
Viewing Information in the SmartEvent GUI

To view Application and URL Filtering events in SmartEvent GUI:
1. In R80 SmartConsole, go to the Logs & Monitor view.
2. Click to open a New Tab, and in the External Apps section, click SmartEvent Settings & Policy.
3. In the window that opens, select a Security Management Server.
4. Click OK.
The R80 SmartEvent opens.
5. In SmartEvent, open the Application and URL Filtering tab view.

   The default view shows these panels:
   - Top High Risk Application/Site by Risk
   - Timeline View - Shows High Risk Applications & Sites based on the number of events, and All Applications & Sites based on the traffic load in Megabytes
   - Top Sources by Event Count
   - All Events - Shows the last 200 events

You can customize the view and modify the filters as necessary. For more information, see the R80 Logging and Monitoring Administration Guide

Administrator Permission Profiles

You can give an administrator permissions for:
- Monitoring and Logging
- Events and Reports

To define an administrator with these permissions:
1. Define an administrator or an administrator group.
2. Define a Permission Profile with the required permissions in R80 SmartConsole (Manage & Settings > Permission Profiles).
3. Assign that profile to the administrator or to the administrator group.

Creating and Changing Administrator Accounts

Create an administrator for R80 SmartConsole or one of the R80 SmartConsole clients.

If you create an administrator account through the Check Point Configuration Tool or the First Time Configuration Wizard, the authentication credentials are a username and a password. If you create it through the R80 SmartConsole, you can choose one of these authentication methods:
- Check Point Password - For each user defined on the Security Management Server, a password is stored on the Security Gateway
- OS Password - User’s credentials for logging in to the operating system of the gateway
- SecurID - A challenge response method that uses a token device or a software token
To create an administrator account using R80 SmartConsole:

1. Click Manage & Settings > Permissions and Administrators.
   The Administrators pane shows by default.

2. Click New Administrator.
   The New Administrators window opens.

3. Enter a unique name for the administrator account.
   Note - This parameter is case-sensitive.

4. Set the Authentication Method, or create a certificate, or the two of them.
   Note - If you do not do this, the administrator will not be able to log in to R80 SmartConsole or other R80 SmartConsole clients, such as SmartEvent.

   To define an Authentication Method:
   Select one of the methods and follow the instructions in Configuring Authentication Methods for Administrators.
   - Check Point Password
   - OS Password
   - SecurID
   - RADIUS
   - TACACS

   To create a Certificate:
   In the Certificate Information section, click Create, enter a password, and save the certificate to a secure location.

5. Select a Permissions profile for this administrator, or create a new one ["Creating and Changing Permission Profiles" on page 44].

6. Set the account Expiration date:
   - For a permanent administrator - select Never
   - For a temporary administrator - select an Expire At date from the calendar

   The default expiration date shows, as defined in the Default Expiration Settings. After the expiration date, the account is no longer authorized to access network resources and applications.

7. Optional: Configure Additional Info - Contact Details, Email and Phone Number of the administrator.

8. Click OK.

To change an existing administrator account:

1. Click Manage & Settings > Permissions and Administrators.

2. Double-click an administrator account.
   The Administrators properties window opens.
Creating and Changing Permission Profiles

Administrators with Super User permissions can create, edit, or delete permission profiles.

To create a new permission profile:
1. In R80 SmartConsole, go to Manage & Settings > Permissions and Administrators > Permission Profiles.
2. Click New Profile.
   The New Profile window opens.
3. Enter a unique name for the profile.
4. Select a profile type:
   • Read/Write All - Administrators can change the configuration
   • Auditor (Read Only All) - Administrators can see the configuration, but cannot change it
   • Customized - Configure custom settings
5. Click OK.

To change a permission profile:
1. In R80 SmartConsole, go to Manage & Settings > Permissions and Administrators > Permission Profiles.
2. Double-click the profile to change.
3. In the Profile configuration window that opens, change the settings as needed.
4. Click Close.

To delete a permission profile:
1. In R80 SmartConsole, go to Manage & Settings > Permissions and Administrators > Permission Profiles.
2. Select a profile and click Delete.
   You cannot delete a profile that is assigned to an administrator. To see which administrators use a profile, in the error message, click Where Used.
   If the profile is not assigned to administrators, a confirmation window opens.
3. Click Yes to confirm.

Permissions for Monitoring, Logging, Events, and Reports

In the Profile object, select the features and the Read or Write administrator permissions for them.

Monitoring and Logging Features

These are some of the available features:

- Monitoring
- Management Logs
- Track Logs
- Application and URL Filtering Logs
Events and Reports Features

These are the permissions for the SmartEvent GUI:

- **SmartEvent**
  - Events - The **Events** tab
  - Policy - Events correlation on the **Policy** tab
  - Reports - **Reports** tab

- **SmartEvent Application and URL Filtering reports only**

Assigning Permission Profiles to Administrators

To assign a permission profile to an administrator:

1. Click **Manage & Settings > Permissions and Administrators**.
2. Double-click an administrator account.
   - The **Administrators** properties window opens.
3. In the **Permissions** section, from the drop-down menu, select a **Permission Profile**.
4. Click **OK**.
CHAPTER 5

Working with UserCheck

In This Section:

Configuring the Security Gateway for UserCheck ...................................................... 46
Revoking Incidents........................................................................................................ 47

Configuring the Security Gateway for UserCheck

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

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

To configure UserCheck on a Security Gateway:

1. In R80 SmartConsole, click Gateways & Servers and double-click the Security Gateway. The Gateway Properties window opens.

2. From the navigation tree, click UserCheck. The UserCheck page opens.

3. Make sure Enable UserCheck for active blades is selected

4. In the UserCheck Web Portal section:
   - In the Main URL field, enter the primary URL for the web portal that shows the UserCheck notifications.
   - If users connect to the Security Gateway remotely, make sure that the Security Gateway internal interface (in the Network Management page) is the same as the Main URL.
   - Note - The Main URL field must be manually updated if:
     - The Main URL field contains an IP address and not a DNS name.
     - You change a gateway IPv4 address to IPv6 or vice versa.

5. Optional: Click Aliases to add URL aliases that redirect different hostnames to the Main URL. The aliases must be resolved to the portal IP address on the corporate DNS server

6. In the Certificate section, click Import to import a certificate that the portal uses to authenticate to the Security Management Server.
   - By default, the portal uses a certificate from the Check Point Internal Certificate Authority (ICA). This might generate warnings if the user browser does not recognize Check Point as a trusted Certificate Authority. To prevent these warnings, import your own certificate from a recognized external authority.

7. In the Accessibility section, click Edit to configure interfaces on the Security Gateway through which the portal can be accessed. These options are based on the topology configured for the Security Gateway. The topology must be configured.
Users are sent to the UserCheck portal if they connect:

- **Through all interfaces**
- **Through internal interfaces** (default)
  - Including undefined internal interfaces
  - Including DMZ internal interfaces
  - Including VPN encrypted interfaces (default)
  
  Note: Make sure to add a rule to the Firewall Rule Base that allows the encrypted traffic.

- **According to the Firewall Policy**: Select this option if there is a rule that states who can access the portal.

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

- **Through all interfaces** - necessary in VSX environment
- **According to the Firewall Policy**

8. Click **OK**.

9. If there is encrypted traffic through an internal interface, add a new rule to the Firewall Layer of the Access Control Policy. This is a sample rule:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>VPN</th>
<th>Services &amp; Applications</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Security Gateway on which UserCheck client is enabled</td>
<td>Any</td>
<td>UserCheck</td>
<td>Accept</td>
</tr>
</tbody>
</table>

10. Install the Access Control Policy.

---

### 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 the R80 SmartConsole **Logs & Monitor** view **Logs** tab 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.
Index

A
About this Guide • 6
Adding a Limit Object to a Rule • 22
Administrator Permission Profiles • 41
Application and URL Filtering Advanced Settings • 30
Application Categories • 27
Application Control and URL Filtering Contracts • 8
Application Control and URL Filtering in the SmartEvent GUI • 40
Application Control and URL Filtering Logs • 40
Application Control Web Browsing Services • 30
Application Risk Levels • 28
Assigning Permission Profiles to Administrators • 44

B
Blocking Applications • 11
Blocking Sites • 14
Blocking URL Categories • 15
Bypassing HTTPS Inspection for Software Update Services • 33

C
Changed Behavior with R80 Management • 15
Changing Services for Applications and Categories • 20
Configuring Outbound HTTPS Inspection • 31
Configuring the Hit Count Display • 23
Configuring the Security Gateway for UserCheck • 45
Connecting to the Internet for Updates • 29
Creating an Application Control and URL Filtering Policy • 10
Creating an Outbound CA Certificate • 32
Creating and Changing Administrator Accounts • 41
Creating and Changing Permission Profiles • 42
Creating UserCheck Interaction Objects • 25

E
Enabling Application and URL Filtering in the Access Control Policy • 9
Enabling Application and URL Filtering on a Security Gateway • 8
Enabling or Disabling Hit Count • 22
Event Analysis in the SmartEvent GUI • 40
Exporting and Deploying the Generated CA • 32

G
Getting Started with URL Filtering • 8

H
HTTP/HTTPS Proxy • 35
HTTPS Inspection • 31
HTTPS Inspection Logs • 36
HTTPS Validation • 34

I
Important Information • 3

L
Limiting Application Traffic • 12
Localizing and Customizing the UserCheck Portal • 25
Log Sessions • 20, 39

M
Managing Application and URL Filtering • 16
Managing Pre-R80 Security Gateways • 16
Monitoring Application and URL Filtering • 9
Monitoring Applications • 10
Monitoring Logs and Events for Application and URL Filtering • 39

O
Overriding Categorization for a URL • 20

P
Permissions for HTTPS Logs • 36
Permissions for Monitoring, Logging, Events, and Reports • 43

R
R80 SmartConsole Toolbars • 6
Revoking Incidents • 46

S
Scheduling Updates • 29
Security Category Updates • 27
Server Validation • 34
Services & Applications • 18

T
The Application and URL Filtering Database • 26
The Columns of the Access Control Rule Base • 17
The HTTPS Inspection Policy • 33
Time • 21
Tracking Options • 20
Types of Rules in the Rule Base • 18

U
Updating the Application and URL Filtering Database • 28
UserCheck Frequency and Scope • 26
UserCheck Interaction Objects • 24
Using Application and URL Filtering with VSX • 38
Using Identity Awareness Features in Rules • 13
Using Identity Awareness in the Rule Base • 37
Using Logs with Application and URL Filtering • 39

V
Viewing Information in the SmartEvent GUI • 41
Viewing Rule Logs • 39

W
Working with the Application and URL Filtering Database • 27
Working with UserCheck • 45
Working with UserCheck Interaction Objects • 24