Important Information

Latest Documentation

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=11658

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

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 May 2011</td>
<td>Updated information about tracking for Application Database</td>
</tr>
<tr>
<td></td>
<td>updates.</td>
</tr>
<tr>
<td>15 December 2010</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback

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

Please help us by sending your comments
(mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Application Control R75 Administration Guide).
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introduction to Application Control</td>
<td>6</td>
</tr>
<tr>
<td>The Need for Application Control</td>
<td>6</td>
</tr>
<tr>
<td>The Check Point Solution for Application Control</td>
<td>6</td>
</tr>
<tr>
<td>Main Features</td>
<td>7</td>
</tr>
<tr>
<td>Application Control Glossary</td>
<td>7</td>
</tr>
<tr>
<td>Topology</td>
<td>7</td>
</tr>
<tr>
<td>Getting Started with Application Control</td>
<td>8</td>
</tr>
<tr>
<td>Licensing and Contracts</td>
<td>8</td>
</tr>
<tr>
<td>Enabling Application Control on a Gateway</td>
<td>8</td>
</tr>
<tr>
<td>Creating an Application Control Policy</td>
<td>9</td>
</tr>
<tr>
<td>Creating Application Control Rules</td>
<td>9</td>
</tr>
<tr>
<td>Managing Application Control</td>
<td>12</td>
</tr>
<tr>
<td>The Application Control Rule Base</td>
<td>12</td>
</tr>
<tr>
<td>Default Rule and Monitor Mode</td>
<td>12</td>
</tr>
<tr>
<td>Parts of the Rules</td>
<td>13</td>
</tr>
<tr>
<td>Rule Actions</td>
<td>15</td>
</tr>
<tr>
<td>The Application Database</td>
<td>16</td>
</tr>
<tr>
<td>Application Categories and Tags</td>
<td>16</td>
</tr>
<tr>
<td>Application Risk Levels</td>
<td>16</td>
</tr>
<tr>
<td>Using the AppWiki</td>
<td>16</td>
</tr>
<tr>
<td>Updating the Application Database</td>
<td>17</td>
</tr>
<tr>
<td>The Application Control Overview Page</td>
<td>18</td>
</tr>
<tr>
<td>My Organization</td>
<td>18</td>
</tr>
<tr>
<td>Messages and Action Items</td>
<td>18</td>
</tr>
<tr>
<td>Detected in My Organization</td>
<td>18</td>
</tr>
<tr>
<td>AppWiki</td>
<td>18</td>
</tr>
<tr>
<td>Gateways Page</td>
<td>18</td>
</tr>
<tr>
<td>Advanced Settings for Application Control</td>
<td>20</td>
</tr>
<tr>
<td>HTTP Inspection on Non-Standard Ports</td>
<td>20</td>
</tr>
<tr>
<td>Engine Settings</td>
<td>20</td>
</tr>
<tr>
<td>Blocking Notifications</td>
<td>21</td>
</tr>
<tr>
<td>Application Control and Identity Awareness</td>
<td>22</td>
</tr>
<tr>
<td>Using Identity Awareness in the Application Control Rule Base</td>
<td>22</td>
</tr>
<tr>
<td>Identifying Users Behind a Proxy</td>
<td>23</td>
</tr>
<tr>
<td>Application Control in SmartView Tracker</td>
<td>24</td>
</tr>
<tr>
<td>Application Control Logs</td>
<td>24</td>
</tr>
<tr>
<td>Log Sessions</td>
<td>24</td>
</tr>
<tr>
<td>Viewing Logs</td>
<td>25</td>
</tr>
<tr>
<td>Predefined Queries</td>
<td>25</td>
</tr>
<tr>
<td>Permissions for Logs</td>
<td>25</td>
</tr>
<tr>
<td>Application Control in SmartEvent</td>
<td>26</td>
</tr>
<tr>
<td>Event Analysis in SmartEvent or SmartEvent Intro</td>
<td>26</td>
</tr>
<tr>
<td>Viewing Information in SmartEvent</td>
<td>26</td>
</tr>
<tr>
<td>Viewing Information in SmartEvent Intro</td>
<td>27</td>
</tr>
<tr>
<td>The SmartEvent Intro Overview Page</td>
<td>27</td>
</tr>
<tr>
<td>Application Control Event Queries</td>
<td>27</td>
</tr>
<tr>
<td>Setting up a Mirror Port</td>
<td>28</td>
</tr>
<tr>
<td>Technical Requirements</td>
<td>28</td>
</tr>
<tr>
<td>Configuring a Mirror Port</td>
<td>28</td>
</tr>
<tr>
<td>Connecting the Gateway to the Traffic</td>
<td>29</td>
</tr>
<tr>
<td>Configuring the Interface as a Mirror Port</td>
<td>29</td>
</tr>
</tbody>
</table>
Checking that it Works .................................................................29
Removing the Mirror Port ...............................................................29
Index ...............................................................................................31
Chapter 1

Introduction to Application Control

In This Chapter

- The Need for Application Control
- The Check Point Solution for Application Control
- Main Features
- Application Control Glossary
- Topology

The Need for Application Control

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

The use of internet applications comes with problems that administrators must know about:

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

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

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

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

The Check Point Solution for Application Control

Check Point’s latest firewall innovation brings the industry’s strongest application and identity control to organizations of all sizes. You can easily create policies which detect or block thousands of applications.

Use the Application Control Software Blade to:

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

- **Create a Granular Application Control Policy**
  Make rules to allow or block applications, by individual application, application tags, or risk levels.

- **Learn What Your Employees are Doing**
  After you start to use Application Control, use SmartView Tracker and SmartEvent to understand the application traffic that really occurs in your environment. Then change the Application Control policy to make it even more effective.

- **Keep Your Policies Updated**
  The Check Point Application Database is updated regularly to help you keep your Application Control policy current.
Main Features

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

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

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

- **Central Management** – Lets you centrally manage security policies from one user-friendly console for easy administration.

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

Application Control Glossary

- **Application** - In Application Control, applications include:
  - Programs you install on a desktop, for example Microsoft Office.
  - Programs you use through a browser, for example Google chat.
  - Social Network widgets that reside in social networking sites, for example Farmville on Facebook.

- **Category** - Group of applications with a common defining aspect. Each application has one primary category which is the most defining aspect of the application. See the category in the application descriptions and in the logs.

- **Tag** - Characteristics of the application. In the Application Database applications can have multiple tags. For example, Gmail tags include: Supports File Transfer, Sends mail, and Instant Chat. You can include tags in rules in the Rule Base. If a tag is in a rule, the rule matches all applications that are marked with that tag. For example if you block the "Sends mail" tag: Gmail, Yahoo! Mail, and others will be blocked.

- **Bytes** - As used in Application Control, it means the quantity of bytes of traffic. It does not mean the rate of bytes transferred for a specific unit of time.

- **AppWiki** - The searchable applications database. It is available in SmartDashboard and from Check Point's public website. For each application it gives: a description, risk level, category, and properties.

Topology

Application Control can be enabled on R75 gateways to control traffic that relates to applications. It can also be deployed on a mirror port to monitor traffic only.
Chapter 2

Getting Started with Application Control

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

In This Chapter

Licensing and Contracts 8
Enabling Application Control on a Gateway 8
Creating an Application Control Policy 9

Licensing and Contracts

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

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

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

- The Message and Action item section of the Overview page of the Application Control tab.
- The Check Point User Center when you log in to your account.

Enabling Application Control on a Gateway

Enable the Application Control Software Blade on each gateway.

To enable the Application Control Software Blade on a gateway:

1. In SmartDashboard right-click the gateway object and select Edit. The Gateway Properties window opens.
3. Click OK.
Creating an Application Control Policy

Create and manage the Application Control policy in the Application Control tab of SmartDashboard. The policy says who can access which applications from within your organization and what applications usage is recorded in the logs.

- The Overview page gives an overview of your application control policy and traffic.
- The Application Control Policy page contains your Rule Base, which is the primary component of your Application Control policy. Click the Add Rule buttons to get started.
- Look through the AppWiki to learn which applications and categories have high risk levels. Find ideas of applications and tags to include in your policy.

Creating Application Control Rules

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

Monitoring Applications

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

To monitor all Facebook application traffic:

1. In the Application Control tab of SmartDashboard, open the Policy page.
2. Click one of the Add Rule toolbar buttons to add the rule in the position that you choose in the Rule Base. The first rule matched is applied.
3. Make a rule that includes these components:

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Application</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Facebook</td>
<td>Any</td>
<td>Internet</td>
<td>Facebook</td>
<td>Allow</td>
<td>Log</td>
<td>All</td>
</tr>
</tbody>
</table>

- **Name** - Give the rule a name such as Monitor Facebook traffic.
- **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.
- **Application** - Click the plus sign to open the Application viewer. Add the Facebook application to the rule.
Start to type “face” in the Search field. In the Applications and Tags list, see the Facebook application.

Hover on each item to see more details in the description pane.

Click on an item one time to add it to the rule.

Open the Application viewer again to add more applications or tags.

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

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

### Blocking Applications

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

**To block an application, such as YouTube, in your organization:**

1. In the Application Control tab of SmartDashboard, open the Policy page.
2. Click one of the Add Rule toolbar buttons to add the rule in the position that you choose in the Rule Base. The first rule matched is applied.
3. Make a rule that includes these components:
   - **Application** - YouTube
   - **Action** - Block
   - **Track** - Log

The rule blocks traffic to YouTube and logs attempts to connect to YouTube.

To block all streaming media applications including YouTube, add the **Supports Streaming** tag to the Application field. All applications that have the **Supports Streaming** tag are blocked.
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 gateway, you can use it together with Application Control to make rules that apply to an access role. Use access role objects to define users, machines, and network locations as one object.

In this example:

- You have already created an Access Role that represents all identified users in the organization. You can use this to allow access to applications only for users who are identified on the 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 Application Control Rule Base:

1. Create a rule and include these components:
   - **Source** - The Identified Users access role
   - **Destination** - Internet
   - **Action** - Allow
   - **Application** - Radmin

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

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

Notes on these rules:

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

Chapter 3

Managing Application Control

Application Control is configured and managed in SmartDashboard. SmartView Tracker shows the logs and SmartEvent shows real-time traffic statistics and analysis. This chapter explains the Application Control configuration and management that you do in SmartDashboard.

In This Chapter

The Application Control Rule Base 12
The Application Database 16
The Application Control Overview Page 18
Gateways Page 18
Advanced Settings for Application Control 20
Application Control and Identity Awareness 22

The Application Control Rule Base

The Application Control policy determines who can access which applications from an organization. The primary component of the Application Control policy is the Rule Base. The rules use the Application Database and network objects.

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

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

For examples of how to create different types of rules, see Creating Application Control Rules (on page 9).

Default Rule and Monitor Mode

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

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

The result of this rule is that all application traffic is monitored. Therefore you can see logs related to application traffic in SmartView Tracker and SmartEvent. Use the data there to better understand the use of applications in your environment and create an effective Rule Base.

If you enabled Identity Awareness on the gateway, you will also see names of identified users in the logs.

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

If you change the default rule, for example:

- You change the tracking to none
- You change known applications to a specified application,
Then all traffic will no longer be monitored.

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

**Parts of the Rules**

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

<table>
<thead>
<tr>
<th>NO.</th>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Application</th>
<th>Action</th>
<th>Track</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Block high risk apps</td>
<td>Any</td>
<td>Internet</td>
<td>High Risk</td>
<td>Block</td>
<td>Log</td>
<td>All</td>
</tr>
<tr>
<td>2</td>
<td>Block malwares</td>
<td>Any</td>
<td>Internet</td>
<td>Used by Malware</td>
<td>Block</td>
<td>Log</td>
<td>All</td>
</tr>
<tr>
<td>3</td>
<td>Allow TeamViewer</td>
<td>John_Smith</td>
<td>Any</td>
<td>TeamViewer</td>
<td>Allow</td>
<td>Log</td>
<td>All</td>
</tr>
<tr>
<td>4</td>
<td>Allow remote admin</td>
<td>JT_Depart</td>
<td>Any</td>
<td>RadNet</td>
<td>Allow</td>
<td>Log</td>
<td>All</td>
</tr>
</tbody>
</table>

**Number (NO.)**

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

For example, Gmail's tags include **Send Messages**, **User Generated Content**, and **Instant Chat**. If rule 3 allows Gmail and rule 4 blocks applications with the **Instant Chat** tag, Gmail will be allowed based on rule 3.

**Name**

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

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

**Source**

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

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

**Destination**

Choose the destination for the traffic. The default is the **Internet**, which includes all traffic with the destination of DMZ or external.

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

**Application**

The Application column contains the applications and application tags that you choose to include. One rule can include multiple items and items of different types. For example, one rule can include 2 applications, and 3 tags. The default is that the rule applies to all known applications.

There is also an application called Web Browsing. The Web Browsing application includes all HTTP traffic that is not a defined application. Because Web Browsing traffic can generate a lot of logs, the Web browsing application has its own logging settings. Configure them in **Advanced > Engine Settings**.

**To add applications, or tags to a rule:**

Put your mouse in the column and a plus sign shows. Click the plus sign to open the Application viewer. For each application, the viewer shows a short description and its category and tags.
To add an item to the rule, click it one time.
To see the details of an item without adding it to the rule, put your mouse on it.
You can only select an application or tag to add to the rule from the left column.
To see the list of applications or tags, click the icons in the toolbar of the viewer. The list opens in the left column and then you can add items to the rule.
To see all applications in a risk level, select the level from the Risk field in the toolbar of the viewer.
If an application or tag is already in a rule, it will not show in the Application viewer.

**Action**

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

- **Block** - The traffic is blocked.
- **Allow** - The traffic is allowed.

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

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

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

**Track**

Choose if the traffic is logged in SmartView Tracker or if it triggers other notifications. Logs are grouped by session. Click in the column and the options open. The options include:

- **None** - Does not record the event
- **Log** - Records the event's details in SmartView Tracker. This option is useful for obtaining general information on your network's traffic.
- **Account** - Records the event in SmartView Tracker with byte information
- **Alert** - Logs the event and executes a command, such as display a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in Policy > Global Properties > Log and Alert > Alert Commands

- **Mail** - Sends an email to the administrator, or runs the mail alert script defined in Policy > Global Properties > Log and Alert > Alert Commands

- **SNMP Trap** - Sends a SNMP alert to the SNMP GUI, or runs the script defined in Policy > Global Properties > Log and Alert > Alert Commands

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

### Install On

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

### Rule Actions

From the toolbar at the top of the Application Control Policy page, click the icons to create new rules or to delete the selected rules.

If you right-click in a column of the Rule Base and select Rule Actions, a menu opens with these options:

- **New Rule** - Select to create a new rule Above or Below the rule that is currently selected.
- **Delete Rule** - Deletes the selected rule or rules.
- **Disable Rule** - The rule stays in the Rule Base but is not active.
- **Select All Rules** - Selects all the rules and you can then choose another action to apply to them.
- **View rule logs in SmartView Tracker** - Opens SmartView Tracker and shows logs related to the rule.
- **View rule logs in SmartEvent** - Opens SmartEvent and shows logs related to the rule.
The Application Database

The Check Point Application Database contains more than 4,500 applications and more than 100,000 social networking widgets. Each item has a description, a category, multiple tags, and a risk level. You can include applications and tags in your Application Control rules. When you have a valid Application Control contract, the database is updated regularly with new applications and social networking widgets. This lets you easily create and maintain an up to date policy.

Access the Application Database from:

- **SmartDashboard** - From the Application Control Rule Base in SmartDashboard, click the plus sign in the Application column, and the Application viewer opens. From there you can add applications and tags directly into the Rule Base.
- **AppWiki** - An easy to use tool to see the Application Database. Open it from the Application Control tab or from the Check Point website (http://appwiki.checkpoint.com/appwiki/applications.htm).

Application Categories and Tags

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

In the Application Database, each application can have multiple tags, which are characteristics of the application. For example, some of the tags of Gmail include: Supports File Transfer, Sends mail, and Instant Chat. If a tag is in a rule, the rule matches all applications that are marked with that tag.

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

If new applications are added to a tag that is in an Application Control rule, the rule is updated automatically when the database is updated.

Application Risk Levels

The Application Database and AppWiki show a Risk Level for each application.

This table explains what each level means and gives examples of applications or types of applications with that level.

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

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

Using the AppWiki

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

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

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

Updating the Application Database

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

By default, updates run on the Security Management Server and gateways every two hours. You can change the update schedule or choose to manually update the management server.

To manually update the management server only:
- On the Updates page of the Application Control tab, click Update Management to update the management only.

To change the schedule for updates on the management server and gateways:
1. Before you run the scheduled update, in the Automatic Application Updates section of the Updates page, select both:
   - Update Application Database on the Security Management Server
   - Update Application Database on the Security Gateway

   When you update the database on the Security Management Server, you can see relevant database changes in SmartDashboard. If you only update the gateways, you will see in SmartDashboard that the gateway has a new version of the Application Database.

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

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

Connecting to the Internet for Updates

The gateway or Security Management Server connects to the internet to get the Application Database updates. To make sure that it can get the updates successfully:

- Make sure that there is a DNS server configured.
- Make sure a proxy is configured for each gateway and the Security Management Server, if necessary.

To configure a proxy:

- The Updates page shows if the Security Management Server uses a proxy to connect to the internet or not. Click Configure Proxy to go to the SmartDashboard page to configure the proxy for the Security Management Server.
- In the SmartDashboard, in the object properties of a gateway or Security Management Server, go to > Topology > Proxy.
- In a Multi-Domain Security Management environment, configure a proxy in Policy > Global Properties > Proxy.

Scheduling Updates

To change the update schedule from the default scheduled Application Database updates:
1. On the Advanced Update Settings page, under Schedule, click Configure.
   The Scheduled Event Properties window opens.
2. In the General page, set the Time of Event.
   - Select Every and adjust the setting to run the update after an interval of time.
The Application Control Overview Page

In the Application Control Overview page you can quickly see the status of machines and incidents. Access the windows for the most urgent or commonly-used management actions.

My Organization

- Shows a summary of which Security Gateways enforce Application Control. It also has a link to the Gateways page.
- Shows a summary of the Application Control Rule Base.

Messages and Action Items

- Shows if a new Application Database update package is available.
- Shows if Security Gateways require renewed licenses or Application Control contracts.
- Open SmartView Tracker - Link to open the Application Control logs in SmartView Tracker.
- Open SmartEvent - Link to open SmartEvent where you can see the traffic statistics and analysis.

Detected in My Organization

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

- Select a time interval for graphs data.
- Select the criteria for the graph data: Bandwidth or Sessions.

AppWiki

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

The gateway connects to the internet to get the most current AppWiki.

- Make sure that there is a DNS server configured.
- Make sure a proxy is configured for each gateway and the Security Management Server, if necessary.

Gateways Page

The Gateways page lists the gateways with Application Control enabled. Select a gateway and click Edit to edit the gateway properties.

For each gateway, you see the gateway name and IP address and also:

- Identity Awareness - If Identity Awareness is enabled, and if so, a summary of its Identity Awareness status.
- Update Status - If the Application Database is up to date on the gateway or if an update is necessary.

If you have Security Gateways in different time zones, they will not be synchronized when one updates and the other did not update yet.
• **Comments** - All relevant comments.

In the **Application Database Updates** section, you can also see the status of the Application Database on the Security Management Server. A message shows if the Management server is up to date or if a new update is available. Click **Update Settings** to go to the **Updates** page.
Advanced Settings for Application Control

This section describes settings that you can configure in the Application Control tab, in the Advanced section of the navigation tree. These settings apply globally for all Application Control gateways.

HTTP Inspection on Non-Standard Ports

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

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

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

Engine Settings

On the Advanced > Engine Settings page, configure settings related to engine inspection, Application Control sessions, and the Web Browsing application.

Social Network Widget Detection

By default, the gateway connects to the Check Point Online Web Service to identify social networking widgets that it does not recognize. To ensure privacy, no identifying information is sent to the Service, only obscured URLs. You can change this setting on the Engine Settings page:

- Social Network Widgets detection will consult with the Check Point Online Web Service
  - If this option is selected, the gateway connects to the Check Point Online Web Service to identify social networking widgets that it does not recognize (default).
  - If this option is cleared or the gateway cannot communicate with the Service, the unknown widget is treated as Web Browsing traffic.

Application Control Engine Inspection

Select the behavior of the Application Control engine if it is overloaded or fails during inspection. For example, if the application inspection is terminated in the middle for any reason. By default, in such a situation all application traffic is allowed. You can change this setting on the Engine Settings page:

- In case of an internal system error or a high load, the Application Control policy for relevant traffic will be 'Accept' (Fail-Open)
  - If this option is selected, all application traffic is allowed in a situation of engine overload or failure (default).
  - If this option is cleared, all application traffic is blocked in a situation of engine overload or failure.

Note - This behavior is different from the default action in the Rule Base, which is that all traffic that is not explicitly blocked is allowed. That applies when the engine works correctly.

Application Control 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 the user first accesses an application. During a session, the gateway records one log for each application that a user browses to. All activity that the user does within the application is included in the log.

If you do not want logs consolidated by session, you can change this setting on the Engine Settings page:

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

You can also adjust the length of a session.

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

**Web Browsing Settings**

The Web Browsing application includes all HTTP traffic that is not a defined application. Because Web Browsing traffic can generate a lot of logs, the Web browsing application has its own logging settings. Configure them in Advanced > Engine Settings.

• Web Browsing is enabled by default. If you disable it:
  • Instances of the Web Browsing in the Application Control Rule Base are not enforced. For example, if you have a rule that blocks Web Browsing, Web Browsing traffic will not be blocked if Web Browsing is turned off.
  • No Web Browsing logs are recorded.

By default, all Web Browsing connections from a user or IP address during a session are combined into one log. For example, if a user, Ava, browses to Google, CNN, and her company intranet in one session, the gateway records one log. The Resource field of the log does not have a value. You can change this setting on the Engine Settings page:

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

**Blocking Notifications**

You can configure what happens when a user's request is blocked by the Application Control policy:

• Users get a message that tells them that their request was blocked. You can customize the message.
• Users are redirected to a URL that you enter.
• The request is blocked with no message.

Configure this in the Application Control tab in Advanced > Blocking Notifications.

**Choose one of the options:**

• **When a request is blocked, display this message:** When a request is blocked, an automatically generated HTML page opens that contains the message entered in the text box.
• **When a request is blocked, redirect to the following URL:** When a request is blocked, users are sent to the URL address that you enter here.
• **Do not show notification when a request is blocked** - The request is blocked with no message.

**Customizing a Blocking Notification Page**

By default, a Check Point logo shows on the blocking notification page. You can replace the Check Point logo with your company's logo.

**Note** - If you change the logo on the Application Control blocking notification page, the same logo will show on the URL Filtering blocking notification page.
To add your company logo to the blocking notification page:
1. Save the image that you want to use as cp_logo.jpg.
3. Replace the cp_logo.jpg file on the gateway with your file that has the same name.
4. Run: chmod 440 cp_logo.jpg
5. Run: chown nobody.nobody cp_logo.jpg
6. Repeat on each relevant gateway.

Application Control and Identity Awareness

Identity Awareness and Application Control can be used together to add user awareness, machine awareness, and application awareness to the Check Point gateway. They work together in these procedures:

- Use Identity Awareness Access Roles in Application Control rules as the source or destination of the rule.
- You can use all the types of identity sources to acquire identities of users who try to access applications.
- In SmartView Tracker logs and SmartEvent events, you can see which user and IP address accesses which applications.

For more details, see the *R75 Identity Awareness Administration Guide*.
(http://supportcontent.checkpoint.com/documentation_download?ID=11662)

Using Identity Awareness in the Application Control Rule Base

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

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

In rules with access role objects, criteria matching operates like this:

- When identity data for an IP is known:
  - If it matches an access role, the rule is applied and the traffic is allowed/blocking based on the action.
  - If it does not match an access role, it goes on to examine the next rule.
- When identity data for an IP is unknown and:
  - All the rule’s fields match besides the source field with an access role.
  - The connection protocol is HTTP.
  - The action is set to redirect to the Captive Portal.
    - If all the conditions apply, the traffic is redirected to the Captive Portal to get credentials and see if there is a match.
    - If not all conditions apply, there is no match and the next rule is examined.
- When the criteria does not match any of the rules in the Rule Base:
  - The traffic is allowed.

To redirect HTTP traffic to the Captive Portal:
1. In a rule that uses an access role in the Source column, right-click the Action column and select Edit Properties.
The Action Properties window opens.

2. Select **Redirect HTTP connections**.
3. Click **OK**.

The Action column shows that a redirect to the Captive Portal occurs.

Below is an example of an Application Control Rule Base that shows how criteria matching operates:

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

When browsing the Internet, different users experience different outcomes:

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

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

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

**Identifying Users Behind a Proxy**

If your organization uses an HTTP proxy server, you cannot see the identities of users behind the proxy. Application Control logs show the proxy as their source IP address and not the user's identity. Application Control and Identity Awareness gateways can use X-Forwarded-For HTTP header, which is added by the proxy server, to resolve this issue. When you configure the proxy server to add X-Forwarded-For HTTP header and the Check Point gateways to use it, you will see the correct source identities for traffic that goes through the proxy.

**To use X-Forwarded-For HTTP header with Application Control:**
1. Configure your proxy server to use X-Forwarded-For HTTP Header.
2. In SmartDashboard, on the **Identity Awareness** page of each gateway object, select **For Application Control blade**, detect users located behind HTTP proxy using X-Forwarded-For header.
3. Install the policy.
Chapter 4

Application Control in SmartView Tracker

In This Chapter

- Application Control Logs 24
- Log Sessions 24
- Viewing Logs 25

Application Control Logs

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

- Each Application Control rule in the Rule Base - sets logs for the application traffic.
- The logging option that you select for Web Browsing on the Advanced > HTTP Inspection page - sets logs for the Web Browsing application.

Logs related to Application Database updates on the gateway are in Application Control > System Logs. Logs related to Application Database updates on the management are in the Management tab.

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 the user first accesses an application. During a session, the gateway records one log for each application that a user browses to. All activity that the user does within the application is included in the log.

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

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

The Web Browsing application has different logging options than all other applications. See Web Browsing Settings (on page 21).

For all applications, including Web Browsing:

- For applications that are allowed in the Rule Base, the default session is three hours. You can change this in the Application Control tab > Advanced > Engine Settings > Timeout.
- For applications that are blocked in the Rule Base, a session is 30 seconds.
**Viewing Logs**

To open SmartView Tracker:

- From the Application Control Overview page, click **Open SmartView Tracker**.
- From the SmartDashboard toolbar, select **Window > SmartView Tracker**.
- Press Control + Shift + T.

**Predefined Queries**

There are multiple predefined queries in **Predefined > Network Security Blades > Application Control**.

- **All** - Shows all Application Control traffic, including allowed and blocked.
- **High Risk Applications** - Shows traffic of Risk Levels 4 and 5.
- **Bandwidth Consuming** - Shows logs from traffic that has the **High Bandwidth** tag.
- **Allowed** - Shows all accepted traffic.
- **Blocked** - Shows all rejected traffic.
- **System** - Shows logs related to Application Database updates and other system related issues. This includes logs related to problems that the application detection service might encounter.

**Permissions for Logs**

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

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

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

**To edit an existing permissions profile:**

1. From the SmartDashboard toolbar, select **Manage > Permissions Profiles**.
2. Select a profile and click **Edit**.
3. Follow the instructions above from step 3.
Chapter 5

Application Control in SmartEvent

In This Chapter

Event Analysis in SmartEvent or SmartEvent Intro 26
Viewing Information in SmartEvent 26
Viewing Information in SmartEvent Intro 27

Event Analysis in SmartEvent or SmartEvent Intro

SmartEvent and SmartEvent Intro supply advanced analysis tools with filtering, charts, reporting, statistics, and more, of all events that travel through enabled Security Gateways. SmartEvent and SmartEvent Intro put all Application Control logs of the same incident into a single event, for example, all matching rules, applications, and user information.

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

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

SmartEvent shows information for all Software Blades in the environment. SmartEvent Intro shows information for one SmartEvent Intro mode. If you select APP as the SmartEvent Intro Mode, it shows the Application Control information.

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

- R75 SmartEvent Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11668)
- R75 SmartEvent Intro Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11669)

Viewing Information in SmartEvent

To open SmartEvent do any of these:

- From the Application Control Overview page, click Open SmartEvent.
- From the SmartDashboard toolbar, select Window > SmartEvent.
- Press Control + Shift + A.

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

- All Applications - Shows all Application Control events, including allowed and blocked.
Viewing Information in SmartEvent Intro

To open SmartEvent Intro:

From the SmartDashboard toolbar, select **Window > SmartEvent Intro** or Press Control +Shift +E.

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

The SmartEvent Intro Overview Page

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

The **Overview** page includes these panes:

- Timeline View
- Top Users by Traffic
- Top Applications by Traffic
- Applications Categories by Traffic
- Newly Detected Applications
- Status

Application Control Event Queries

See detailed event queries in the **Events** tab. Events are grouped by the number of megabytes used.

- **All Applications** - Shows all Application Control events, including allowed and blocked.
- **High Risk Applications** - Shows events of Risk Levels 4 and 5.
- **Bandwidth Consuming** - Shows events from traffic that has the **High Bandwidth** tag.
- **By Application Category** - Shows events organized by the application category.
- **Applications by User** - Shows events according to the name of the user.
- **By Application Rule Name** - Shows events by the name of the Application Control rule that applies to them.

See the **R75 SmartEvent Intro Administration Guide**.

(http://supportcontent.checkpoint.com/documentation_download?ID=11669)
Setting up a Mirror Port

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

You can use mirror ports:

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

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

Benefits of a mirror port include:

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

In This Chapter

Technical Requirements 28
Configuring a Mirror Port 28

Technical Requirements

You can configure a mirror port on gateways with:

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

Mirror ports are not supported with:

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

Configuring a Mirror Port

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

To use the mirror port, you need a Check Point deployment that includes a Security Management Server, a gateway, and a SmartDashboard. For details on how to set this up, see the R75 Installation and Upgrade Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11648). For additional details
about evaluating Check Point products or setting up the mirror port, contact your Check Point representative.

Connecting the Gateway to the Traffic

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

Configuring the Interface as a Mirror Port

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

Checking that it Works

To make sure the mirror port is configured and connected properly:
- Browse to an internet site, such as Google.
- Open SmartViewTracker. You should see traffic of the blade you enabled.

Removing the Mirror Port

To remove the mirror port from the interface:
1. In the command line of the Check Point gateway, run: `sysconfig`.
2. Select Network Connections.
3. Select Configure Connections.
4. Select the interface that you want to remove the mirror-port from.
5. Select Remove the connection to the mirror port.
6. Install the policy.