Important Information

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

Latest Documentation
The latest version of this document is at: http://supportcontent.checkpoint.com/documentation_download?ID=11668
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>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 SmartEvent R75 Administration Guide).
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introducing SmartEvent</td>
<td>6</td>
</tr>
<tr>
<td>The SmartEvent Solution</td>
<td>6</td>
</tr>
<tr>
<td>Scalable, Distributed Architecture</td>
<td>6</td>
</tr>
<tr>
<td>Centralized Event Correlation</td>
<td>6</td>
</tr>
<tr>
<td>Easy Deployment</td>
<td>7</td>
</tr>
<tr>
<td>Real-Time Threat Analysis and Protection</td>
<td>7</td>
</tr>
<tr>
<td>Intelligent Event Management</td>
<td>7</td>
</tr>
<tr>
<td>Event Investigation Tracking</td>
<td>7</td>
</tr>
<tr>
<td>The SmartEvent Architecture</td>
<td>7</td>
</tr>
<tr>
<td>Data Analysis and Event Identification</td>
<td>8</td>
</tr>
<tr>
<td>Event Management</td>
<td>9</td>
</tr>
<tr>
<td>Interoperability with Security Management</td>
<td>9</td>
</tr>
<tr>
<td>SmartEvent Client</td>
<td>9</td>
</tr>
<tr>
<td>Basic Concepts and Terminology</td>
<td>9</td>
</tr>
<tr>
<td>Initial Configuration</td>
<td>11</td>
</tr>
<tr>
<td>Check Point Licenses</td>
<td>11</td>
</tr>
<tr>
<td>Initial Configuration of SmartEvent and SmartReporter Clients</td>
<td>12</td>
</tr>
<tr>
<td>Define the Internal Network for SmartEvent</td>
<td>12</td>
</tr>
<tr>
<td>Defining Correlation Units and Log Servers for SmartEvent</td>
<td>12</td>
</tr>
<tr>
<td>Creating a Consolidation Session for SmartReporter</td>
<td>12</td>
</tr>
<tr>
<td>Enabling Connectivity with Multi-Domain Security Management</td>
<td>13</td>
</tr>
<tr>
<td>Installing the Network Objects in the SmartEvent Database</td>
<td>13</td>
</tr>
<tr>
<td>Configuring SmartEvent to work with Multi-Domain Security Management</td>
<td>13</td>
</tr>
<tr>
<td>Incorporating Third-Party Devices</td>
<td>14</td>
</tr>
<tr>
<td>Syslog Devices</td>
<td>14</td>
</tr>
<tr>
<td>Windows Events</td>
<td>14</td>
</tr>
<tr>
<td>SNMP Traps</td>
<td>15</td>
</tr>
<tr>
<td>Analyzing Events</td>
<td>16</td>
</tr>
<tr>
<td>Event Queries</td>
<td>16</td>
</tr>
<tr>
<td>Predefined Queries</td>
<td>16</td>
</tr>
<tr>
<td>Custom Queries</td>
<td>16</td>
</tr>
<tr>
<td>Event Query Results</td>
<td>19</td>
</tr>
<tr>
<td>Event Log</td>
<td>19</td>
</tr>
<tr>
<td>Event Statistics Pane</td>
<td>23</td>
</tr>
<tr>
<td>Event Details</td>
<td>23</td>
</tr>
<tr>
<td>Presenting Event Data</td>
<td>25</td>
</tr>
<tr>
<td>Overview Tab</td>
<td>25</td>
</tr>
<tr>
<td>Reports Tab</td>
<td>27</td>
</tr>
<tr>
<td>Timeline Tab</td>
<td>28</td>
</tr>
<tr>
<td>Charts Tab</td>
<td>29</td>
</tr>
<tr>
<td>Maps Tab</td>
<td>32</td>
</tr>
<tr>
<td>Administrator Permission Profiles - Events and Reports</td>
<td>33</td>
</tr>
<tr>
<td>Multi-Domain Security Management</td>
<td>33</td>
</tr>
<tr>
<td>Investigating Events</td>
<td>34</td>
</tr>
<tr>
<td>Tracking Event Resolution using Tickets</td>
<td>34</td>
</tr>
<tr>
<td>Editing IPS Protection Details</td>
<td>34</td>
</tr>
<tr>
<td>Displaying an Event's Original Log Information</td>
<td>34</td>
</tr>
<tr>
<td>Packet Capture</td>
<td>35</td>
</tr>
<tr>
<td>Using Custom Commands</td>
<td>35</td>
</tr>
<tr>
<td>Configuring Event Definitions</td>
<td>36</td>
</tr>
<tr>
<td>Tuning SmartEvent Using Learning Mode</td>
<td>37</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Running Learning Mode</td>
<td>37</td>
</tr>
<tr>
<td>Working with Learning Mode Results</td>
<td>37</td>
</tr>
<tr>
<td>Modifying Event Definitions</td>
<td>37</td>
</tr>
<tr>
<td>Event Definitions and General Settings</td>
<td>38</td>
</tr>
<tr>
<td>Event Definition Parameters</td>
<td>38</td>
</tr>
<tr>
<td>Creating Event Definitions (User Defined Events)</td>
<td>42</td>
</tr>
<tr>
<td>High Level Overview of Event Identification</td>
<td>42</td>
</tr>
<tr>
<td>Creating a User-Defined Event</td>
<td>46</td>
</tr>
<tr>
<td>Eliminating False Positives</td>
<td>50</td>
</tr>
<tr>
<td>Services that Generate Events</td>
<td>50</td>
</tr>
<tr>
<td>Common Events by Service</td>
<td>50</td>
</tr>
<tr>
<td>Dynamic Updates</td>
<td>56</td>
</tr>
<tr>
<td>Perform a Dynamic Update</td>
<td>56</td>
</tr>
<tr>
<td>View Updated Events</td>
<td>57</td>
</tr>
<tr>
<td>Revert the Dynamic Update to a Previous Version</td>
<td>57</td>
</tr>
<tr>
<td>Administrator Permissions Profile - Policy</td>
<td>57</td>
</tr>
<tr>
<td>Multi-Domain Security Management</td>
<td>57</td>
</tr>
<tr>
<td>System Administration</td>
<td>59</td>
</tr>
<tr>
<td>Modifying the System's General Settings</td>
<td>59</td>
</tr>
<tr>
<td>Adding Network and Host Objects</td>
<td>60</td>
</tr>
<tr>
<td>Defining Correlation Units and Log Servers</td>
<td>60</td>
</tr>
<tr>
<td>Defining the Internal Network</td>
<td>61</td>
</tr>
<tr>
<td>Offline Log Files</td>
<td>61</td>
</tr>
<tr>
<td>Configuring Custom Commands</td>
<td>62</td>
</tr>
<tr>
<td>Creating an External Script</td>
<td>62</td>
</tr>
<tr>
<td>Managing the Event Database</td>
<td>63</td>
</tr>
<tr>
<td>Backup and Restore of the Database</td>
<td>63</td>
</tr>
<tr>
<td>Adjusting the Database Size</td>
<td>63</td>
</tr>
<tr>
<td>SmartEvent High Availability Environment</td>
<td>64</td>
</tr>
<tr>
<td>How it works</td>
<td>64</td>
</tr>
<tr>
<td>Log Server High Availability</td>
<td>64</td>
</tr>
<tr>
<td>Correlation Unit High Availability</td>
<td>64</td>
</tr>
<tr>
<td>Third-Party Device Support</td>
<td>64</td>
</tr>
<tr>
<td>New Device Support</td>
<td>64</td>
</tr>
<tr>
<td>Parsing Log Files</td>
<td>65</td>
</tr>
<tr>
<td>Adding New Devices to Event Definitions</td>
<td>67</td>
</tr>
<tr>
<td>Syslog Parsing</td>
<td>68</td>
</tr>
<tr>
<td>Administrator Support for WinEventToCPLog</td>
<td>79</td>
</tr>
<tr>
<td>Index</td>
<td>81</td>
</tr>
</tbody>
</table>
Chapter 1

Introducing SmartEvent

Today's complex multi layered security architecture consists of many devices to ensure that servers, hosts, and applications running on the network are protected from harmful activity. These devices all generate voluminous logs that are difficult and time-consuming to interpret. In a typical enterprise, an intrusion detection system can produce more than 500,000 messages per day and firewalls can generate millions of log records a day. In addition, the logged data may contain information that appears to reflect normal activity when viewed on its own, but reveal evidence of abnormal events, attacks, viruses, or worms when raw data is correlated and analyzed.

Enterprises need control over and practical value from the deluge of data generated by network and security devices.

In This Chapter

- The SmartEvent Solution 6
- The SmartEvent Architecture 7
- Basic Concepts and Terminology 9

The SmartEvent Solution

SmartEvent provides centralized, real-time event correlation of log data from Check Point perimeter, internal, and Web security gateways as well as third-party security devices automatically prioritizing security events for decisive, intelligent action. By automating the aggregation and correlation of raw log data, SmartEvent not only minimizes the amount of data that needs to be reviewed but also isolates and prioritizes the real security threats. These threats may not have been otherwise detected when viewed in isolation per device, but pattern anomalies appear when data is correlated over time.

With SmartEvent, security teams no longer need to comb through the massive amount of data generated by the devices in their environment. Instead, they can focus on deploying resources on the threats that pose the greatest risk to their business.

Scalable, Distributed Architecture

SmartEvent delivers a flexible, scalable platform capable of managing millions of logs per day per correlation unit in large enterprise networks. Through its distributed architecture, SmartEvent can be installed on a single server but has the flexibility to spread processing load across multiple correlation units and reduce network load.

Centralized Event Correlation

SmartEvent provides centralized event correlation and management for all Check Point products such as Security Gateway, InterSpect, and Connectra, as well as third-party firewalls, routers and switches, intrusion detection systems, operating systems, applications and Web servers. Raw log data is collected via secure connections from Check Point and third-party devices by SmartEvent correlation units where it is centrally aggregated, normalized, correlated, and analyzed. Data reduction and correlation functions are performed at various layers, so only significant events are reported up the hierarchy for further analysis. Log data that exceeds the thresholds set in predefined event policies triggers security events. These events can be unauthorized scans targeting vulnerable hosts, unauthorized logging, denial of service attacks, network anomalies, and other host-based activity. Events are then further analyzed and severity levels assigned. Based on the severity level, an automatic reaction may be triggered at this point to stop the harmful activity.
immediately at the gateway. As new information flows in, severity levels can be adjusted to adapt to changing conditions.

Easy Deployment

SmartEvent provides a large number of predefined, but easily customizable, security events for quick deployment. Its tight integration with the Security Management server architecture, allows it to interface with existing Security Management log servers, eliminating the need to configure each device log server separately for log collection and analysis. In addition, all objects defined in the Security Management server are automatically accessed and used by the SmartEvent server for event policy definition and enforcement. An enterprise can easily install and have SmartEvent up and running and detecting threats in a matter of hours.

Real-Time Threat Analysis and Protection

SmartEvent performs real-time event correlation based on pattern anomalies and previous data, as well as correlation based on predefined security events. Once installed on the network, SmartEvent has an intelligent, self-learning mode where it automatically learns the normal activity pattern for a given site and suggests policy changes to reduce false-alarm events. By weeding out irrelevant data and by correlating data between multiple devices, SmartEvent is able to zero in on threats that pose greatest risk to the enterprise. SmartEvent is fully integrated with the Security Management server and can access all Check Point gateways and enforce automatic actions on these gateways against critical threats, for real-time, dynamic threat mitigation.

Intelligent Event Management

SmartEvent enables administrators to customize event thresholds, assign severity levels to event categories, and choose to ignore rules on specific servers and services- greatly reducing the number of false alarms. Administrators may perform event search queries, sorts and filters, as well as manage event status. With new information the open event may easily be closed or changed to a false alarm. Daily or weekly events reports can be distributed automatically for incident management and decision support.

Event Investigation Tracking

SmartEvent enables administrators to investigate threats using flexible data queries which are presented in timelines or charts. Once suspect traffic is identified, actions taken to resolve the threats are tracked using work tickets, allowing you to keep a record of progress made using statuses and comments.

In addition, daily or weekly events reports can be distributed automatically for incident management and decision support.

The SmartEvent Architecture

SmartEvent has several components that work together to help track down security threats and make your network more secure:

- Correlation Unit, which analyzes log entries on Log servers
- SmartEvent server, which contains the Events Database
- SmartEvent client, which manages SmartEvent

They work together in the following manner:

- The Correlation Unit analyzes each log entry as it enters a Log server, looking for patterns according to the installed Event Policy. The logs contain data from both Check Point products and certain third-party devices. When a threat pattern is identified, the Correlation Unit forwards what is known as an event to the SmartEvent server.
The SmartEvent Architecture

- When the SmartEvent server receives events from a Correlation Unit, it assigns a severity level to the event, invokes any defined automatic reactions, and adds the event to the Events Database, which resides on the server. The severity level and automatic reaction are based on the Events Policy.

- The SmartEvent client displays the received events, and is the place to manage events (such as filtering and closing events) and fine-tune and install the Events Policy.

The SmartEvent components can be installed on a single machine (i.e., a standalone deployment), or spread out over multiple machines and sites (i.e., a distributed deployment) to handle higher volumes of logging activity.

The SmartEvent and SmartReporter can be installed together on the same machine. In addition to generating Check Point reports, SmartReporter provides reporting services for SmartEvent.

Depending on the volume of logging activity, you may want to install multiple Correlation Units, each of which can analyze the logs of multiple Log servers.

Data Analysis and Event Identification

The Correlation Unit is responsible for analyzing the log entries and identifying events from them. When analyzing a log entry, the Correlation Unit does one of the following:

- Marks log entries that by themselves are not events, but may be part of a larger pattern to be identified in the near future.
- Takes a log entry that meets one of the criteria set in the Events Policy and generates an event.
- Takes a log entry that is part of a group of items that depict a security event together. New log entries may be added to ongoing events.
• Discards all log entries that do not meet event criteria.

Event Management

The SmartEvent server receives all the items that are identified as an event by the Correlation Unit(s). Further analysis takes place on the SmartEvent server to determine the severity level of the event and what action should take place. The event is then stored in the system database.

Interoperability with Security Management

SmartEvent imports certain objects from the Security Management server without having to recreate the objects in the SmartEvent client. Changes made to the objects on the Security Management server are reflected in the SmartEvent client.

SmartEvent Client

The SmartEvent client provides all of the tools necessary for configuring definitions which will recognize security-related issues in your network infrastructure. It also provides a wide variety of methods for you to view the resulting data, including timelines, reports and charts which allow you to drill down into the underlying data.

What can I do with the SmartEvent client?

• Real-time Monitoring - The SmartEvent Overview presents all of the critical information that you need for ongoing monitoring of security events and security updates. This view can be displayed in a Network Operations Center to provide engineers with a clear understanding of the network's current status.

• Event Investigation - The timelines, charts and events lists are all customizable to allow you to restructure the events data in a way that will assist you to accurately understand the security of your environment and drive your security decisions.

• Resolution Tracking - Actions taken by administrators to investigate and resolve issues can be tracked in event tickets and comments.

• Security Status Reporting - The event reports reveal the who is attacking your network, how they are attacking and where the attacks originate. These reports, either generated from default definitions or customized in SmartReporter, are a compelling way to present the organization's security status to management.

What tools are included in the SmartEvent client?

The SmartEvent client is divided into seven sections:

• The Overview tab contains the latest information about top sources, top destinations and top events over time and differentiated by severity.

• The Events tab is where you can review Events, either according to pre-configured queries or according to queries that you define.

• The Policy tab contains the event definitions and other system configuration parameters.

• The Reports tab displays the output of reports that are defined and generated from SmartReporter.

• The Timeline tab is where you can investigate security issues using a ground-breaking, customizable view of the number of events that occur over a period of time and how serious they are.

• The Charts tab is where you can investigate security issues using pie or bar charts which present event data over time or based on any other event characteristic.

• The Maps tab is where you can view the source and destination countries for the event data on a map.

Basic Concepts and Terminology

• Event Policy - the rules and behavior of IPS Event Analysis

• Event - activity that is perceived as a threat and is classified as such by the Event Policy
- **Log Server** - receives log messages from Check Point and third-party devices
- **Correlation Unit** - component that analyzes logs on Log servers and detects events
- **Event Database** - stores all detected events
- **IPS Event Analysis Server** - houses the Event Database, receives events from Correlation Units, and reacts to events as they occur
- **IPS Event Analysis Client** - Graphic User Interface where the Event Policy is configured and events are displayed
- **Management Server** - Security Management server or, in a Multi-Domain Security Management environment, Domain Management Server
Chapter 2

Initial Configuration

SmartEvent and SmartReporter components require secure internal communication (SIC) with the Management server, either a Security Management server or a Domain Management Server (see "Enabling Connectivity with Multi-Domain Security Management" on page 13).

Once connectivity is established, install SmartEvent and SmartReporter and perform the initial configuration (see "Initial Configuration of SmartEvent and SmartReporter Clients" on page 12).

In This Chapter

Check Point Licenses 11
Initial Configuration of SmartEvent and SmartReporter Clients 12
Enabling Connectivity with Multi-Domain Security Management 13
Incorporating Third-Party Devices 14

Check Point Licenses

Check Point software is activated with a License Key. You can obtain this License Key by registering the Certificate Key that appears on the back of the software media pack, in the Check Point User Center.

The Certificate Key is used in order to receive a License Key for products that you are evaluating.

In order to purchase the required Check Point products, contact your reseller.

Check Point software that has not yet been purchased will work for a period of 15 days. You are required to go through the User Center in order to register this software.

1. Activate the Certificate Key shown on the back of the media pack via Check Point User Center (http://usercenter.checkpoint.com).
   The Certificate Key activation process consists of:
   - Adding the Certificate Key
   - Activating the products
   - Choosing the type of license
   - Entering the software details
   Once this process is complete, a License Key is created and made available to you.

2. Once you have a new License Key, you can start the installation and configuration process. During this process, you will be required to:
   - Read the End Users License Agreement and if you accept it, select Yes.
   - Import the license that you obtained from the User Center for the product that you are installing.
   Licenses are imported via the Check Point Configuration Tool.
   The License Keys tie the product license to the IP address of the SmartEvent server. This means that:
   - Only one IP address is needed for all licenses.
   - All licenses are installed on the SmartEvent server.
Initial Configuration of SmartEvent and SmartReporter Clients

The final stage of getting started with SmartEvent and SmartReporter is the initial configuration of the clients. After installing SmartConsole according to the instructions in the R75 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=11647) and R75 Installation and Upgrade Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11648):

1. For SmartEvent:
   - Define the Internal Network and Correlation Units
   - Install the Event Policy
   Events will begin to appear in the SmartEvent client.
2. For SmartReporter:
   - Create Consolidation Sessions
   Logs will now be created and sent to the SmartReporter database. As a result, reports can be created.

Define the Internal Network for SmartEvent

To help SmartEvent determine whether events have originated internally or externally, the Internal Network must be defined. Certain network objects are copied from the Management server to the SmartEvent server during the initial sync and updated periodically. Define the Internal Network from these objects.

To define the Internal Network, do the following:
1. Start the SmartEvent client.
2. From the Policy view, select General Settings > Initial Settings > Internal Network.
3. Add internal objects.

   Note - It is recommended to add all internal Network objects, and not Host objects.

Defining Correlation Units and Log Servers for SmartEvent

1. From the Policy view of the SmartEvent client, select General Settings > Initial Settings > Correlation Units.
2. Select Add.
3. Click the [...] symbol and select a Correlation Unit from the displayed window.
4. Select OK.
5. Click Add and select the Log servers available as data sources to the Correlation Unit from the displayed window.
6. Select Save.
7. From the Actions menu, select Install Events policy.

Once the Correlation Units and Log servers are defined, and the Events Policy installed, SmartEvent will begin reading logs and detecting events.

To learn to manage and fine-tune the system through the SmartEvent client, see SmartEvent client.

Creating a Consolidation Session for SmartReporter

The consolidation session reads logs from the log server and adds them to the SmartReporter database. If there is a single log server connected to a Security Management server, a consolidation session will automatically be created to read newly generated logs. If multiple log servers connect to one management server, users must manually define consolidation sessions for each log server.
Enabling Connectivity with Multi-Domain Security Management

When creating a Consolidation session you are determining the log server that should be used to extract information and the database table in which the consolidated information should be stored.

1. In the Selection Bar view, select Management > Consolidation.
2. Select the Sessions tab.
3. Click the Create New... button to create a new session.

   The New Consolidation Session - Select Log Server window appears.
4. Select the log server from which logs will be collected and will be used to generate reports.
5. Click Next.

   The New Consolidation Session - Select Log Files and database for consolidation session window appears.
6. Choose whether to use the default source logs and default database tables or select specific source logs and specific database tables for consolidation.

If you select Select default log files and database, click Finish to complete the process. This option indicates that the source of the reports will be preselected logs and all the information will be stored in the default database table named CONNECTIONS. The preselected logs are the sequence of log files that are generated by Check Point products. The preselected logs session will begin at the beginning of last file in the sequence or at the point the sequence was stopped.

If you want to customize the Consolidation session, refer to the R75 SmartReporter Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=11670).

Enabling Connectivity with Multi-Domain Security Management

In a Multi-Domain Security Management environment, the SmartEvent server can be configured to analyze the log information for any or all of the Domain Management Servers on the Multi-Domain Server. In order to do this, the SmartEvent server's database must contain all of the network objects from each of the Domain Management Servers and then be configured to gather logs from the selected log servers.

Installing the Network Objects in the SmartEvent Database

1. From the SmartDomain Manager, open the Global SmartDashboard.
2. In the Global SmartDashboard, create a Host object for the SmartEvent server.
3. Configure the object as an SmartEvent server and Log server.
4. Save the Global Policy.
5. Close the Global SmartDashboard.
6. In the Multi-Domain Security Management client, assign the Global Policy to the Domains with which you will use SmartEvent.

Configuring SmartEvent to work with Multi-Domain Security Management

1. In the SmartEvent client, select Policy > General Settings > Objects > Domains and add all of the Domains you will be working.

   Objects will be synchronized from the Domain Management Servers – this may take some time.
2. Select Policy > General Settings > Objects > Network Objects, and add networks and hosts that are not defined in the Domain Management Servers.
3. Select Policy > General Settings > Initial Settings > Internal Network, and add the networks and hosts that are part of the Internal Network.
4. Select Policy > General Settings > Initial Settings > Correlation Units, click Add and select the SmartEvent Correlation Unit and its Log servers. For traffic logs, select the relevant Domain Log Server or Multi-Domain Log Server. For audit logs, select the relevant Domain Management Server.
5. Install the Event Policy.
Incorporating Third-Party Devices

Syslog Devices

Various third-party devices use the syslog format for logging. SmartEvent and SmartReporter can process third-party syslog messages by reformatting the raw data. As the reformatting process should take place on the SmartEvent or SmartReporter computer, it is recommended to enable a Log server on one of them. Direct all third-party syslog traffic to this Log server.

1. Connect to the Management server using SmartDashboard and edit the properties of the SmartEvent or SmartReporter object. For that object only, enable the property Log Server under Check Point Products. For the purposes of this section, this object will be referred to as the "syslog Log server."

2. Open Logs and Masters > Additional Logging.

3. Enable the property Accept Syslog messages.

4. To enable the log server properties on the SmartEvent server, select SmartDashboard > Policy > Install Database. Select the SmartEvent server as one of the targets.

5. On the third-party device, configure syslogs to be sent to the syslog Log server.

6. On the Management server, make this rule in the Rule Base.

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-party devices that issue syslog messages</td>
<td>syslog Log Server</td>
<td>UDP syslog</td>
</tr>
</tbody>
</table>

7. On the SmartEvent client, add the syslog Log server to a Correlation Unit, if not already enabled (see "Defining Correlation Units and Log Servers for SmartEvent" on page 12).


9. Reboot the syslog Log server.

Windows Events

Check Point Windows Event Service is a Windows service application. It reads Windows events, normalizes the data, and places the data in the Check Point Log Server. SmartEvent processes this data. The process can only be installed on a Windows machine, but it does not have to be a machine running SmartEvent. Thus, Windows events can be processed even if SmartEvent is installed on a different platform.

*How Windows Event Service Works*

Check Point Windows Event Service is given the addresses of Windows computers that it will read and the address of a Log server to which it will write. It reads a Windows event at a time, converts the fields of the event according to configuration files and stores the Windows event as a log in the Log server.

Check Point Windows Event Service is first installed as a service on the user's machine and the user provides a user name and password. The user name can be either that of a domain administrator of the machines whose Windows events will be read, or that of a local administrator on the machine that provides the Windows events.

Check Point Windows Event Service requires trust to be established so it can communicate with the Log server.

*Sending Windows Events to SmartEvent*

In SmartDashboard, create an OPSEC object for Windows Event Service:

1. Open Manage > Servers and OPSEC Applications.
   The Servers and OPSEC Applications window appears.

2. Select New > OPSEC Application.

3. Enter the name of the application that will send log files to SmartEvent.

4. Click on New to create a Host.

5. Enter a name and the IP address of the machine that will run WinEventToCPLog, and click OK.

6. Under Client Entities, select ELA.
Incorporating Third-Party Devices

7. Select Communication.
8. Enter an Activation Key, repeat it in the confirmation line, and keep a record of it for later use.
9. Click Initialize. The system should report the trust state as Initialized but trust not established.
10. Click Close.
11. Click OK.
12. From the File menu, select Save.

On the Windows host, configure the Windows service to send logs to SmartEvent:
1. Install the WinEventToCPLog package from the Check Point DVD.
2. When the installation completes, restart the machine.
3. Open a command prompt window and go to the following location:
   C:\Program Files\CheckPoint\WinEventToCPLog\R75\bin
4. Run: windowEventToCPLog -pull_cert
   a) Enter the IP address of the management server.
   b) Enter the name of the corresponding OPSEC Application object that you created in SmartDashboard for the Windows events.
   c) Enter the Activation Key of the OPSEC object.
5. Restart the Check Point Windows Event Service.
6. If this machine is running a log server then install the Event Policy on this machine.

In the SmartDashboard, establish trust relationship between the Security Management Server and the Windows Host:
1. Edit the OPSEC Application that you created in SmartDashboard for the Windows events.
2. Select Communication and verify that the trust state is Trust Established.
3. From the Policy menu, select Install Database.

On Each Machine that will send Windows Events, configure the Windows Audit Policy:
1. From the Start menu, select Settings > Control Panel > Administrative Tools > Local Security Policy > Local Policies > Audit Policy.
2. Make sure that the Security Setting for the Policy Audit Logon Events is set to Failure. If not, double click and select Failure.
3. Open a command prompt window and change to C:\Program Files\CheckPoint\WinEventToCPLog\R71\WinEventToCPLog\bin.
4. Run the following commands:
   windowEventToCPLog -l <ipaddr>, where <ipaddr> is the IP address of the Log Server that will receive the Windows Events.
   windowEventToCPLog -a <ipaddr>, where <ipaddr> is the IP address of each machine that will send Windows Events.
   windowEventToCPLog -s, where you will be prompted for an administrator name and the administrator password that will be registered with the windowEventToCPLog service.

When configuring windowEventToCPLog so that it should read Windows events from a remote machine, you need to check that the administrator that is registered with windowEventToCPLog has access to the remote machine’s events. A simple way to test this is to log in as the administrator and from this machine attempt to read the events from the remote machine using the Microsoft Event Viewer.

SNMP Traps

To convert SNMP traps to the cplog format, the machine must first be registered as a server that accepts SNMP traps. Run the following commands on a SmartEvent computer:
1. snmpTrapToCPLog -r
2. For each machine from which you want to read SNMP traps: snmpTrapToCPLog -a IPaddress
3. cpstop
4. cpstart
Chapter 3

Analyzing Events

The SmartEvent client provides a wide variety of tools for reviewing security events and pinpointing the traffic which threatens your security environment. Using pre-defined and custom queries you can filter the events generated from the Log server’s database to find events and event patterns that you can then use to improve the security of your network. Once you have found threats, you can identify characteristics of the traffic from events, raw logs or packet captures and use that information to change your Security Policy, IPS protection settings, or other relevant settings to prevent the threats from damaging your network.

SmartEvent also includes an assortment of methods to graphically represent the event data for reviewing the bigger picture, drilling-down to the details, or presenting event data in an intuitive and informative display.

In This Chapter

Event Queries 16
Event Query Results 19
Presenting Event Data 25
Administrator Permission Profiles - Events and Reports 33

Event Queries

SmartEvent uses filtered event views, called queries, to allow you to precisely define the types of events you want to view. Located in the Queries Tree, these queries filter and organize event data for display in the Events, Charts and Maps tabs. Queries are defined by filter properties and charts properties. Filter properties allow you to define what type of events to display and how they should be organized. Charts properties allow you to define how the filtered event data should be displayed in chart form.

Predefined Queries

SmartEvent provides a thorough set of predefined queries, which are appropriate for many scenarios. Queries are organized by combinations of event properties, for example:

- **IPS**, which includes queries of IPS events
- **Direction**, such as **Incoming**, **Internal**, and **Outgoing**
  Direction is determined by the Internal Network (see “Defining the Internal Network” on page 61) settings.
- **IP**, either the **Source** or **Destination** IP address
- **Ticketing**, such as ticket **State** or **Owner**
- **Severity**, such as **Critical**, **High**, and **Medium**

Custom Queries

SmartEvent offers the flexibility to define your own queries for investigating events. This provides you with the ability to create query definitions that return the events that interest you the most. Once you have defined custom queries, you can organize them into folders so that they are easy to find and use.

Your queries can then be used to:

- Generate lists of events with specific characteristics in the Events tab
• Display event count and severity trends in the **Timelines** tab
• Present event data in easy to read charts in the **Charts** tab
• View events by source or destination country in the **Maps** tab

**Creating Custom Queries**

You can create a custom query from the **Custom** folder or from an existing query.

**To create a custom query based on the default query:**

• In the **Selector tree**, right-click on the **Custom** folder, select **New**, and name the customized query.

**To create a custom query based on an existing query:**

1. Right-click on a query you want to use as the basis of your custom query and select **Save As**.
2. Provide a name for the new query.
   • You can save the query with the **Time frame** setting from the Events list by clicking **More** and selecting the **Save time frame** option.
3. Click **Save**.

**Customizing Query Filters**

**To change the filter values of your custom query:**

1. Right-click the new query and select **Properties > Events Query Properties**. The **Events Query Properties** window appears.
   • Use **Add** and **Remove** to include the fields that you would like to use in the query. To help you find a specific field, enter text in Search Fields and the fields that contain that text will be highlighted in both lists.
   • Place check marks in the **Show** column for the fields you want to appear in the **Event Log**.
   • If desired, select fields and use **Group** and **Ungroup** to use those fields to group the results of the query.
   • If desired, select fields and use **Up** and **Down** to sort the order in which the fields will display in the **Event Log**.
2. To specify criteria for a filter, click on the a value in the **Filter** column. A filter relevant to the type of data in this field opens. Enter values for the filter and click **OK**.
3. If desired, select **Prompt for** and choose a filter from the drop-down list. By enabling **When running the query prompt for**, the query presents a **Filter** window and prompts the user to add criteria to the selected filter. This makes the query more dynamic, enabling the user to specify values each time the query is run.
   • **Note** - The **Time Frame** and **# of Events** parameters of a custom query are only saved if **Save As** is selected and the user explicitly requests to **Save Time Frame** information.
4. Click **OK**.

Other settings that you can define for the query are:

• **Auto refresh every 60 seconds** sets this query to automatically update the **Event Log** with the latest detected events every 60 seconds.
• **Run query on OK** displays the results of the query in the Event Log when you finish setting the click **OK**.
• **Use existing value from the toolbar** retrieves the number of events specified by **Show up to #** in the toolbar.
• **Return maximum of X events per query** retrieves the specified number of events irrespective of the **Show up to #** in the toolbar.
To clear filter values from your custom query:

- Right-click on the value in the Filter column. Select Clear Filter to change the current filter to the value Any, or select Clear All Filters to change all filters to the value Any.

**Customizing Query Charts**

To change the way your custom query will display as a chart:

1. Right-click the new query and select Properties > Events Query Properties. The Events Query Properties window appears.
2. Add fields to the column on the right side of the window to make them available in the Split-By menu on the chart. Selecting a field from the Split-By menu displays the event data divided according to the selected event characteristic.
3. In Show top, select the number of top values to show from the chosen Split-By field.
4. Select to display the query by default as a Pie chart or on a Time axis.
   - If you want to display on a Time axis using a pre-defined Time Resolution, choose the Time Resolution you want.

**Organizing Queries in Folders**

You can create custom folders to organize your custom queries, as well as subfolders nested within folders.

To create a custom folder:

1. Right-click on Custom (or any other custom folder you have created previously) and select New Folder.
2. Name the folder.

When you create a new query, you can save it to this new folder by selecting it before selecting Save in the Save to Tree window.
Event Query Results

The Events tab is the heart of SmartEvent.

Figure 3-1  SmartEvent Events Tab

The components of the Events tab are as follows:

1. Query Tree
2. Event Statistics Pane
3. Event Log
4. Log entry detail pane
5. Event Preview Pane

The Events tab is an Event Log that shows events generated by a query. In addition, the Events tab contains the Query Tree, the Event Preview Pane and the Event Statistics Pane.

Double-click a query in the Query Tree to run that query. The results show in the Event Log. The top Events, Destinations, Sources and Users of the query results are displayed in the Event Statistics Pane, either as a chart or in a tallied list. The details of the selected event are displayed in the Event Preview Pane.

Event Log

SmartEvent's Event Log can display up to 30,000 events. The events displayed are the result of a query having been run on the Event Database. To run a different query, double-click on a query in the Selector tree. The Event Log will display the events that match the criteria of the query.

The Event Log is where detected events can be filtered, sorted, grouped, sent for review and exported to a file to allow you to understand your network security status. Event details, such as Start and End Time, Event Name and Severity, are displayed in a grid. In the Status bar at the bottom of the SmartEvent client window, Number of records in view displays a count of new events. Refresh retrieves the data from the database according the active query's filter. AutoRefresh can be selected to continuously monitor for new events.
The details of an event provide important specifics about the event, including type of event, origin, service, and number of connections. You can access event details by double-clicking the event or by displaying the Event Preview Pane.

Queries are built with certain default settings that can be changed directly in the Events tab to provide more specific or more comprehensive results.

1. The Time Frame selection allows you to choose the period of time for which events should be displayed (default is 2 weeks).
2. The Show up to _ Events selection sets the number of events that should be displayed from the query (default is 5,000 events). Up to 30,000 events can be displayed and managed at one time.
3. The Group By selection is particularly useful here to quickly divide the data by specific criteria and immediately show the number of events per grouping.

Filtering Events

After running a query, you can further filter the event data by right-clicking any column and defining the filter parameters. This will temporarily include the filter in the active query and run the query again against the database to return the matching values.

A green filter icon at the top of a column indicates that a filter is applied to that field. You can then choose to save the new set of filters as a custom query by selecting Save from the File menu. Running the query again will discard the filters that have not been saved.

To use filters with query results:
- To change the filter's criteria, right-click on a column header and select Edit Filter.
- To remove events that have any specific field value, right-click on the value and select Filter out.
- To include only events that have a specific field value, right-click on the value and select Follow.
- To remove the extra conditions you have applied, right-click the filter and select Clear Filter.

Sorting and Searching Events

Running a query could return thousands of matching events. To help you organize the events that have already been returned by the query, you can sort them by clicking on any of the column headers.

You can also look for events which have specific values by entering values in the Search field. Searching for multiple values, using commas to separate the values, will return the events that contain all of the search values, although the values can be in any of the event's fields. The search can be made case-sensitive or can look for data that is not displayed in columns.

Select display options from the Options menu to the right of the Search field.
Grouping Events

One of the most powerful ways to analyze event data is by grouping the data based on the specific columns using the Group By button on the toolbar. Here you can group the events by one or more columns and the Event Log shows the number of matching events in those groups, presented in descending order.

You can also specify the default grouping that a query should use by marking fields as Grouped in the Events Query Properties (“Customizing Query Filters” on page 17) window.

The top line of each group in the Event Log shows a summary of the events that it contains. If you hover over a field in the top line, you can see details of what data that field contains in all of the events in the group.

To group events by one or more fields, perform one of the following:
1. Click on Group By in the toolbar and select the field to use for grouping events.
2. Click on Group By in the toolbar and select More Fields. Then in the Group By window select one or more field to use for grouping events.
3. Right-click on the column in the Event Log you want to use for grouping events and select Group By This Column.

Once you have already grouped by a column, you can add another column to use for grouping by right-clicking on the column in the Event Log you want to use for grouping events and select Add this Column to the Group.

To remove fields from the grouping, perform one of the following:
1. Click on Ungroup in the toolbar to remove all grouping.
2. Click on Group By in the toolbar and select More Fields. Then in the Group By window remove one or more field from grouping.
3. Right-click on the column in the Event Log you want to remove from the grouping and select Remove Column from Group.

Sending an Event

In some circumstances, event information can be used to show evidence of a security attack or vulnerability that needs to be resolved. For example, you may decide that another member of your security team should review an event as evidence of an attack. Also, reporting events to Check Point can help Check Point improve the IPS technology to detect new threats in an ever-changing security environment. From the Event Log, you can choose to send event details as an email using your default email client, or you can choose to send the event details to Check Point over a secure SSL connection.

To send an event using email:
1. Select the event in the Event Log.
2. Right-click on the event and select Send event by Email.

A new email opens using your default email client and the event information is included in the body of the email.

To report an event to Check Point:
1. Select the event in the Event Log.
2. Right-click on the event, select Report Event to Check Point and choose whether you want to include just the Event Details or to also include the Packet Capture associated with the event.

Only the event information will be sent to Check Point over a secure SSL connection. The data is kept confidential and Check Point only uses the information to improve IPS.
Exporting Events to a File

The Event Log can contain thousands of events. You can export the events from the SmartEvent client into a text file to allow you to review or manipulate the data using external applications, such as a spreadsheet or text editor.

You can export events from the Overview tab, Events tab or Events window. When exported, the list of events will be saved exactly as it appears in the Event Log, including the visible columns and any sorting, filtering or grouping that is applied to the events.

To export events to a comma-delimited (csv) file:
1. In the Overview tab, Events tab or Events window, organize the events as you would like them to be saved.
   - Hide/show columns to display the information you want to save.
   - Apply sorting, filtering and grouping to produce a list of events in the format you want.
2. From the File menu, select Export Events to csv File.
3. Name the file, navigate to the location where you want the file saved and click Save.

Checking Client Vulnerability

To maintain a high level of security, organizations must install the latest security patches on network computers. Many of the security patches are designed to prevent threats from exploiting known vulnerabilities. If you are consistent with implementing software patches, your network computers will not be vulnerable to some of the attacks that are identified by SmartEvent. SmartEvent ClientInfo helps you determine whether an attack related to Microsoft software is likely to affect the target machine. If the target machine is patched, you can stop the events from being generated by choosing to exclude the target machine from the event definition or from the specific IPS protection.

SmartEvent ClientInfo connects to the computer whose IP address is listed in the event. After you enter credentials with administrator privileges on the target computer, SmartEvent ClientInfo reads the list of Microsoft patches installed on the computer as well as other information about the installed hardware and software. SmartEvent ClientInfo also retrieves the Microsoft Knowledge Base article related to the vulnerability reported in the event and checks to see if the patches listed in the article are installed on the target computer. If SmartEvent ClientInfo finds that the matching patch is installed, it is likely that the attack will have no affect on the target computer and you can choose to create an exception so that IPS or SmartEvent stops recognizing the attack as a threat.

Once the computer information is loaded in SmartEvent ClientInfo, you can perform the following functions:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Folder]</td>
<td>Save the information in the active tab to a .csv file</td>
</tr>
<tr>
<td>![Credential]</td>
<td>Enter new credentials for accessing the computer information</td>
</tr>
<tr>
<td>![Copy]</td>
<td>Copy the contents of the selected cell</td>
</tr>
<tr>
<td>![Search]</td>
<td>Run Google.com search using the contents of the selected cell</td>
</tr>
<tr>
<td>![Filter]</td>
<td>Filter the contents of the active tab for rows containing the search text</td>
</tr>
<tr>
<td>![Filter KB]</td>
<td>Filter the contents of the active tab for rows containing the KB number</td>
</tr>
<tr>
<td>![Connect]</td>
<td>Connect to the specified IP address to gather the computer's information</td>
</tr>
</tbody>
</table>

To check that a computer is not vulnerable to an attack:
1. In the Events tab, right-click on the event you want to investigate and select SmartEvent ClientInfo.
2. Enter user credentials that allow administrator privileges on the target computer or select Use Windows Logon Account to login with your current credentials. You can also save your credentials to avoid having to enter them again.
SmartEvent ClientInfo retrieves the software and hardware information from the target computer, as well as the details of the Knowledge Base article associated with the vulnerability identified in the event.

3. Check the result. SmartEvent ClientInfo returns one of the following results:

- **Installed fix / Computer is not vulnerable** - In this instance, SmartEvent ClientInfo found that the patch recommended by Microsoft for protecting against the vulnerability is installed on the target computer.
  
  Based on this, you can decide to modify the associated IPS protection or event definitions to prevent these events from displaying in the future.

- **Unfound fix / Derived fixes exist** - In this instance, SmartEvent ClientInfo found that a patch is installed that is related to the Security Bulletin, but found that the main patch that is recommended by Microsoft for protecting against the vulnerability is not installed on the target computer. The installed fix may not cover all of the affected software.
  
  Click on the KB numbers specified to open the associated Knowledge Base articles. Review the recommended remediation steps, which may include installing a patch on the target computer.

- **Missing Fix / Computer may be vulnerable** - In this instance, SmartEvent ClientInfo found that the patch recommended by Microsoft for protecting against the vulnerability is not installed on the target computer.
  
  Click on the KB number specified to open the associated Knowledge Base article. Review the recommended remediation steps, which may include installing a patch on the target computer.

  **Note** - If SmartEvent ClientInfo finds that the patch in the KB article is not installed on the remote computer, it may indicate one of the following:

  - The vulnerability does not affect or is not relevant to the target computer’s Operating System OR Service Pack version. If so, the computer is not vulnerable.
  - The article is relatively old and you may have installed Service Pack that includes the patch for the vulnerability. If so, you should check the installed Service Pack to see if it was released after KB article and may include the associated patch.

### Event Statistics Pane

The Event Log is accompanied by charts displaying the Top Events, Top Sources, Top Destinations and Top Users for the active query. These statistics are automatically updated as filters are applied to the Event Log.

You can toggle between viewing the statistics as a chart or a list by clicking on the arrow in the top-right corner of each of the boxes and selecting Show Pie Chart.

You can filter in or out any value in the Event Statistics Pane to focus the query results on the data that is most important to you. Filtering in the Event Statistics Pane is also reflected in the Event Log, and clearing filters from the Event Statistics Pane clears all filters that have been applied to the query.

- To remove events that have any specific field value, right-click on the value and select Filter out.
- To include only events that have a specific field value, right-click on the value and select Follow.
- To remove the extra conditions you have applied, click on the Clear Filter icon.

### Event Details

See the details of an event from the Preview Pane in the Events tab or by double-clicking on the event in the Event Log. The Event Details window has two tabs with different data:

- **Summary tab** - Shows a brief summary of the event in a user-friendly format.
- **Details tab** - Shows the full, technical details of the event.

These options are available from the Event Details window:

- **Copy** - Copies the event's details to the Windows Clipboard.
• **Actions** - Actions that you can do that are related to this log. They include:
  • **Event Raw Logs** - Launches SmartView Tracker and displays the log entries upon which the event is based.
  • **Edit Ticket** - Lets you set the state of the event, assign an owner, and add a comment.
  • **Add Comment** - Lets you add a quick comment about the event without changing the state or owner.
  • **View History** - Lets you view the ticket activity on the event, including changes to the state, owner, or comments.
• **Blade Specific Menu** - For example, IPS or Application Control. This menu has different options depending on the Software Blade that is related to the event.
• **Previous** displays the event that appears before the current event in the Event Log.
• **Next** displays the event that appears after the current event in the Event Log.

**Summary Tab**

The **Summary** tab includes:

• The source of the activity. If Identity Awareness is enabled, this can be the user's name.
• A brief description of the event.
• The action taken on the event.
• The time of the event.
• Other important data related to the event.

**Details Tab**

The **Details** tab includes:

• Details about the Software Blade and rule that caused the event.
• Ticketing information for the event - Use this to track activity related to the event.
• General Event Information - Includes the severity for the event and a unique ID.
• Traffic Information - Where the event originated, its destination, and the size of the data in bytes.
• Event Detection - How and when the event was detected and by which gateway.
More - Additional information related to the connections involved in the event and the source.

Presenting Event Data

SmartEvent provides a wide-variety of methods for graphically presenting event data so that you can find the events and the event patterns that are most important to maintaining a high level of security in your environment.

Overview Tab

The SmartEvent Overview tab combines the most critical information for monitoring security in your environment. Its main focus is presenting a quick view of the recent events data using the Timeline View, Recent Critical Events, and Top tables and chart. These interactive sections report on the events based on the Time Frame setting to allow you to display event data from a specific latest period of time.
Double-click on data in any of the sections in the Overview tab to open the associated list of events so that you can continue investigating issues all the way down to the individual event level.

The Overview tab sections include:

1. **Timeline View** - Timelines allow you to graphically view the most important queries of recent events grouped together according to a configured time interval. Each timeline displays up to one million events for a particular query over the specified **Time Frame**. The events are grouped as a chart according to the selected **Time Resolution**. You can add, modify or remove timelines from this view just as you would in the **Timeline Tab** (on page 28).

2. **Security Events Section** - This section shows events from a user-selected query. This is useful for examining important events that occurred during the specified **Time Frame**. To select a query to show in this pane:
   a) Click the icon in the upper right-hand corner of the pane.
   b) Select one of these options from the menu:
      - **Set Query** - Select a predefined query from **Set Query** window.
      - **Show Newly Detected Applications table** - Show applications seen for the first time during the specified **Time Frame**.

   You can search, sort, filter and group events using the same methods as in the **Events tab** ("Event Query Results" on page 19). Click the arrow to select a different query to show here.

3. **Security Center** - When connected to the Internet, the Security Center displays a dynamic ticker tape of available protections against new vulnerabilities. The **Open** link of a Security Center item takes you to the Check Point Advisories.

4. **Top 10 Panes** - These two panes show the top ten events during the specified **Time Frame** and according to user-selected categories. You can show events according to traffic volume or the quantity of events. To show the top ten events:
   a) Click the icon in the upper right-hand corner of the pane.
b) Select one of these criteria:

- Sources
- Destinations
- Users
- Events
- Applications
- Application Type

c) Select a metric:

- **Show Data by Event Count** - Quantity of events during the specified **Time Frame**
- **Show Data by Traffic** - Traffic volume in MBs

5. **Status** - The Status section contains system information including:

- **Status** - This indicator reports the current status of the Event Analysis system (see "The SmartEvent Architecture" on page 7), including problems connectivity to Correlation Units and Log servers and when the allocated disk space is full. Click on the link for more information.

- **Object Sync** - This indicator reports on the synchronization of objects between the management servers (either Security Management or Domain Management Server) and the SmartEvent server (see "Interoperability with Security Management" on page 9). Click on the link for more information.

- **Config** - This indicator will appear if components are not configured, including Internal Network settings (see "Defining the Internal Network" on page 61) and Correlation Units. Click on the link for more information.

- **Events received in the** - These statistics show the number of events received by the SmartEvent server in the last minute, hour and 24-hour period. This information gives a quick glance at the traffic load on the SmartEvent server. Unusual data in these fields may indicate connectivity problems between the components of the Event Analysis system (see "The SmartEvent Architecture" on page 7).

---

**Reports Tab**

Daily and weekly reports of the events recorded by SmartEvent are configured and stored on the **Reports** tab. SmartEvent Reports provide a high-level summary of the event patterns occurring on your network. Upon creation, reports can be automatically emailed to predefined addresses, eliminating the need to open SmartEvent to learn of the system’s status.

SmartReporter can create the following SmartEvent reports:

- **SmartEvent** displays events in the following categories:
  - Top Sources and their Top Events
  - Top Destination and their Top Events
  - Top Events
  - Events by Date
  - Events by Date and Top Events per Date
  - Events by Day of the Week
  - Events by Day of the Week and Top Events per Day
  - Events by Hour of the Day
  - Top Products and their Top Events
  - Events by Severity and Top Events per Severity
  - Top Services and their Top Events

- **List of All Events**
  The **SmartReporter > Reports > Definitions > Filter tab** contains the following filters for the two SmartEvent reports:

- **Source** indicates the source of a particular event (that is, its IP address of the DNS name of the machine).

- **Destination** indicates the destination of a particular event (that is, its IP address of the DNS name of the machine).
• **Event** indicates the name of the specific event.

• **Category** indicates the type of event (for example, **Policy > Event Policy > Denial of Service**).

• **Severity** indicates the seriousness of a particular event. There are five severity values (Critical, High, Medium, Low, Informational). The severity of each event is determined by the administrator.

• **Service** indicates the IP Service used in a particular event. For example, combination protocol and port (tcp/80).

• **Product** indicates the product for which logs were generated. For example, UTM-1 Edge, 3Com Firewall, Cisco Router, etc.

  **Note** - Some Internet browsers may block the ActiveX component of the report.

### Timeline Tab

Timelines allow you to graphically view the most important queries of recent events grouped together according to a configured time interval. Each timeline displays up to one million events for a particular query over the specified **Time Frame**. The events are grouped as a chart according to the selected **Time Resolution**.

**Figure 3-2**  
SmartEvent Timeline Tab

**Note** - Because the timeline wheels are displayed by severity, timelines for queries without filters (such as a query by source IP address), will be identical to the timeline of the All Events query.

You can either modify these timelines or add new timelines with pre-defined query definitions or your own. Timelines can also be removed, renamed and moved up or down in the view from the **Manage** menu.
To add a new timeline:
1. Select Manage > Add Line.
2. In the Add Line window, do one of the following:
   a) *Use a Predefined Query:* Choose one of the queries that exists and click OK.
   b) *Modify a Predefined Query:*
      (i) Select an existing query and click Configure.
      (ii) In the Events Query properties window, configure the query to filter for the events that you want to track and click OK.
      (iii) Enter a name for the new custom query. You can choose to save the time frame for the query.
      (iv) Click Save.
   c) *Create a new Custom Query:*
      (i) Click New to create a custom query which you can use for the new timeline.
      (ii) In the Events Query properties window, configure the query to filter for the events that you want to track and click OK.
      (iii) In the Add Line window, enter a name for the custom query.
3. In the Add Line window, click OK.

You can now see the configured timelines and you can modify the Time Frame and Time Line Resolution to help you analyze the event data.

To modify an existing timeline:
1. Select a timeline and select Manage > Configure.
2. In the Events Query properties window, configure the query to filter for the events that you want to track.
3. Click OK.

The selected timeline now displays the event data based on the modified query.

**Charts Tab**

Charts display query results in a graphical format which you can configure to divide the events data based in any event characteristic. You can then drill down into any segment of the chart to display a list of those events in a new Events window.

Event queries can be shown with a Time Axis or as a Pie Chart. The query’s chart properties define which type of chart will be shown by default but you can change the chart type to display at any time by selecting from the options in the upper-left corner.
• The **Time Axis** display shows the query results over time based on a configured **Time Resolution**. This method focuses attention on how the event data differs over time.

**Figure 3-3** SmartEvent Graphs Tab

![Time Axis Display](image)

• The **Pie Chart** is the best way to show Top N data such as By Source (top sources), By Destination (top destinations), and By Service (top services). This method focuses attention on the number of events with specific properties.

**Figure 3-4** SmartEvent Graphs Tab

![Pie Chart](image)

**Event Data Options**

The following are settings that can be set from the Toolbar to change the event data that is displayed in the chart:
• **Time frame** - Click on the **Change time frame** menu, to choose a specific time frame for which events are displayed. For example, you can choose to show only events during the last 24 hours, the last 30 days, or a custom time frame.

• **Time Resolution** - This field determines how events are grouped in charts and timelines. For example, when the time frame is set to one hour, all events that match the query's filter properties and occurred within the period of one hour will be displayed together. The colors of the time wheel indicate the breakdown of events by category within the selected period of time.

• **Split By** - This field determines which dimension will be used to analyze the events. In the query's Chart Properties, you can choose which dimensions to make available for displaying in the charts.

• **Show Top** - This field determines how many of dimensions results will be displayed in the chart. In the query's Chart Properties, you can set the default number.

You can also set a particular chart to be displayed by default in the Charts tab by right-clicking on the query and selecting **Run on Start**.

**Display Options**

The following are options that can be changed from the Toolbar to present the chart data in a more informative and appealing manner:

• **Fixed Scale** - By default, the scale of the number of events will change based on the results displayed in the chart. By selecting **Fixed Scale**, you can choose for the scale of the number of events to remain constant as you scroll through the chart.

• **Data Grid** - You can choose to show a data grid next to the chart. The data grid provides a table which shows a summary of all of the data points in the query. When you move the cursor over any part of the chart grid, the associated data will be highlighted in the other area.

• **Copying Data** - Click on the **Copy** icon to access the options for copying the event statistics to your computer's Clipboard for external use. You can copy the image itself, or you can copy raw event counts represented by the image that is currently displayed and then paste that data into another application.
  
  • Copying the image - Click the **As a Bitmap** icon to copy the image that is currently displayed.
  
  • Copying the event count data - Click the **As Text (data only)** icon to copy the raw event counts represented by the image that is currently displayed.

• **Printing** - Click on the **Print** icon to print the image that is currently displayed.

• **3D/2D Display** - Click on the **3D/2D** icon to choose whether to display the chart as flat (2D) or with depth (3D).

The following are elements of the chart display that can be changed by right-clicking on the chart to customize the presentation of the chart:

• **Toolbar** - The Toolbar can be hidden, which is particularly useful before copying or printing a chart.

• **Legend Box** - You can choose to show or hide the Legend Box. The Legend Box is a key which indicates what the colors of the chart represent. Change the location and font of the Legend Box by right-clicking on it.

• **Background Color** - You can select a background color for the chart.

You can modify the display options for the data grid, legend box, axis labels or axis scales. Right-clicking any of the elements allows you to change the font, text color, display location and other graphical options.

**To view a chart:**

1. Run a query by double-clicking the query in the Query Tree.
   
   You can also open your chart in a new window by right-clicking the query and selecting **Run in New Window**. This allows you to keep multiple charts open at the same time.

2. Decide whether you want the chart to be based on time (**Time Axis**) or based on other event properties (**Pie Chart**).
   
   • When using **Time Axis**, choose a **Chart Time Resolution** to group the events by a specific time range.

3. The chart will display all events. You can choose to show only a number of the top query results by selecting a number from the **Show Top** menu.
Maps Tab

Source and Destination information are frequently critical when determining the potential threat of traffic. Some companies need to block traffic from certain countries based on security, political, or legal reasons whereas other companies may see identifying traffic by country of origin or destination simply as a way to limit the traffic passing through the network.

In the Maps tab, SmartEvent presents source and destination countries for the active query on an interactive world map. Countries are color-coded to indicate levels of event activity. You can define the number of countries to include in the top tier of countries (Top N) and in the second tier of countries (Next Top N) to change how countries are grouped in the map.

Figure 3-5  Maps Tab

By double-clicking on a country, you can drill-down to see a detailed list of events for that country. By default the map shows the results of the All Events query; however, you can populate the map with information from any of the available queries by double-clicking on a query in the Query Tree. You can also choose to view continents individually in order to see countries more clearly.

Statistics information about the active query is displayed below the interactive map. The five countries with the highest number of events matching the query filter are shown with the number of events for each, as well as the total number of countries matching the query.

Interact with the map using the following actions:

- To see the number of events that correspond to a country, move the mouse over that country.
- To view query results for a country in an Events window, double-click on the country.
- To change between viewing the entire world map and viewing maps for individual continents, choose from the Map menu.
- Activity Level - In the bottom right corner of the map is the Activity Level key. Countries are colored according to four tiers:
  - Top - By default, the Top 3 countries are colored Red. Choose the number of countries to include in the top tier by changing this setting.
  - Next Top - By default, the Next Top 5 countries are colored Yellow. Choose the number of countries to include in the second tier by changing this setting.
  - Others - All countries with events, but are not included in the Top or Next Top tiers, are colored Blue.
  - No Activity - All countries without events are colored White.

Moving the mouse over a tier in the Activity Level key will highlight the Countries in that tier. In addition, in the bottom left corner of the map is a summary of event statistics which includes the number of events for the top 5 countries and the total number of countries with events.
Administrator Permission Profiles - Events and Reports

SmartEvent enables you to provide an administrator with a Permission Profile for the SmartEvent database. A Permission Profile is a permission ID card that is assigned to administrators or administrator groups.

The administrator and his Permission Profile are verified during login. When an administrator logs into SmartEvent his user name and password are verified by the SmartEvent server. If the administrator is not defined on the SmartEvent server, the server will attempt the login process with the credentials that are defined on the Security Management server or Multi-Domain Server connected with SIC to the SmartEvent server.

**Note** - If you do not want to centrally manage administrators, and you only use the local administrator defined for the SmartEvent server:

From the SmartEvent server command line, invoke:
```
cpprod_util CPPROD_SetValue FW1 REMOTE_LOGIN 4 1 1
```

The Permission Profile types for the SmartEvent Events tab are set in the SmartDashboard or SmartDomain Manager (SmartDashboard > Manage > Permissions Profiles > New / Edit) connected to the Security Management server or Multi-Domain Server with the following option:

- **Events Database** enables an administrator to receive permissions for the SmartEvent events that are found on the SmartEvent server.

The following are the three types of Permission Profiles:

- **No Access** indicates that the administrator cannot view the SmartEvent Events and Reports tabs.
- **Read Only** enables the administrator to view SmartEvent Events and Reports tabs.
- **Read/Write** enables the administrator to modify the SmartEvent Events and Reports tabs using the Change State option.

### Multi-Domain Security Management

When working with Multi-Domain Security Management, SmartEvent is Domain oriented. That is, each Event and Report is associated with a Domain.

The administrator can view Events and Reports about Domains to which he has permissions. Only locally defined administrators on the SmartEvent server or the Multi-Domain Server Super User can view all events including cross-Domain events.
Chapter 4

Investigating Events

Once you have arranged the events as you like in the Event Log, you can begin to investigate their details and evaluate whether they represent a threat.

In This Chapter

- Tracking Event Resolution using Tickets 34
- Editing IPS Protection Details 34
- Displaying an Event's Original Log Information 34
- Packet Capture 35
- Using Custom Commands 35

Tracking Event Resolution using Tickets

Events can be categorized and assigned to administrators to track their path through the workflow of resolving threats. Once administrators review an event, they can assign it a status, such as Investigation in Progress, Resolved, or False Alarm; add comments that detail the actions that have been taken with respect to the event; and assign an administrator as the owner of the event. This process is called Ticketing.

After editing the ticket, administrators can use queries to track the actions taken to mitigate security threats and produce statistics based on those actions.

- To edit an Event Ticket, open the event and click Edit Ticket.
- To add a quick comment about the event without changing the state or owner, open the event and click Add Comment.
- To view the history of actions that have been taken on an event, open the event and click View History.

Editing IPS Protection Details

When reviewing events generated from the IPS blade, you may want to review the IPS protections and profiles to understand why an event was generated or attempt to change the way the traffic is handled by the IPS blade.

The IPS menu presents actions that are specific to IPS events. These actions include:

- Go to Protection which opens the SmartDashboard to the IPS protection which triggered the event.
- Go to Advisory which opens the Check Point Advisory article which provides background information about the IPS protection.
- Protection description which opens a detailed description of the IPS protection.

Displaying an Event's Original Log Information

To see log entries for an event, right-click the event and select Additional Information > View Event Raw Logs. SmartView Tracker displays the log entries that comprise the event.
Packet Capture

If any logs have related packet captures, you can open a packet viewer to see the contents of the captured packet. You can also save the packet capture to a file for further investigation.

To use the Packet Capture feature, you must activate these blades and plug-ins:

- In a Security Management server deployment, you must activate the Logging and Status Software Blades on the Security Management Server.
- In a Multi-Domain Security Management deployment, you must activate the SmartEvent plug-in in the specified Domain Management Server.

**To view a packet capture:**

1. In the Events tab, right-click the event in the Event Log pane.
2. Select **Additional Information > View packet capture** from the options menu. The Packet Capture Viewer Output window opens.
3. Optionally, click **Save** to save the packet capture data as a text file.

You can select **Actions > Packet Capture Configuration** to define an application in which to view packet capture information. The options are:

- The SmartEvent **Internal Viewer**
- Any windows program associated with this file type
- Select a program by entering the program executable file name and any required arguments.

Using Custom Commands

The SmartEvent client provides a convenient way to run common command line executables that can assist you in investigating events. By right-clicking on cells in the Event Log that refer to an IP address, the default list of commands appears in the context-sensitive menu.

The following commands are available by default: ping, whois, nslookup and Telnet. They appear by design only on cells that refer to IP addresses, because the IP address of the active cell is used as the destination of the command when run.

For example, if you right-click a cell containing an IP address and select the default ping command, a window opens and three ICMP packets are sent to that address. This behavior is configurable, and other commands can be added as well. To add your own custom commands, see Configuring Custom Commands (on page 62).
Chapter 5

Configuring Event Definitions

Most of the configuration of SmartEvent takes place in the Policy tab. System components such as Correlation Units are defined here, as well as lists of blocked IP addresses and other general settings.

But the main attraction of the Policy tab is the configuration of each type of event. Each type of event that SmartEvent can detect is listed here, and sorted into a number of main categories. Each event can be customized by altering the default thresholds and setting Automated Responses. Events can also be disabled by removing the check mark. The settings made here are what determine SmartEvent's Event Policy.

As illustrated in the figure below, the Policy tab is composed of the Selector Tree, which is the navigation pane on the left, the Detail pane, which contains the various settings of each item in the Selector Tree, and the Description pane, which provides a description of the selected item.

Figure 5-6 Policy Tab Components

Once the SmartEvent client begins displaying events, the following tasks should be performed:

- Fine-tune the Event Policy (see "Tuning SmartEvent Using Learning Mode" on page 37)
- Modify the existing Event Definition to focus on the events that you want to see (see "Modifying Event Definitions" on page 37)
- Create new Event Definitions to capture the events that are not covered by the existing definitions (see "Creating Event Definitions (User Defined Events)" on page 42)

Modifications to the Event Policy do not take effect until saved on the SmartEvent server and installed to the Correlation Units.

To enable changes made to the Event Policy, proceed as follows:

1. Select File > Save.
2. Select Actions > Install Event Policy.

Changes made to the Event Policy can be undone if the changes have not been saved first. To undo changes made to the policy, select File > Revert Changes.
Tuning SmartEvent Using Learning Mode

While SmartEvent is ready "out-of-the-box" with an Event Policy based on real-world expectations, in most cases further fine-tuning is required. SmartEvent's Learning Mode analyzes the Event Log and generates a report with suggestions as to what modifications you should make to your system's Event Policy. It should be run a day or so after installing SmartEvent, and whenever you want to further refine the events detected.

Running Learning Mode

To run Learning Mode, proceed as follows:
1. From the Actions menu, select Learning Mode.
2. Select Advanced analysis method, and then select Advanced.
3. Choose from which date you would like to analyze events. If this is the first time you are running Learning Mode, it is recommended to select Analyze entire database.
4. Select OK to close the Learning mode advanced options window, and OK again to begin the analysis. This may take some time.

Working with Learning Mode Results

When the analysis is complete, a browser window will open with SmartEvent's recommendations for fine-tuning your Event Policy. Once Learning Mode presents its results, proceed as follows:
1. Review the Learning Mode results.
2. If you do not want to accept SmartEvent's recommendation on any particular adjustment, remove the check mark from that recommendation.
3. To apply the suggestions, select Apply.
4. Select the Policy tab to confirm that the changes have been applied to specific Event Definitions. Specifically review per event what exceptions have been added to the section Apply the following exceptions.
5. To save and implement these changes to the Event Policy, select File > Save, and Actions > Install Event Policy.

Modifying Event Definitions

SmartEvent is constantly culling data from your Log servers, and searching for patterns within all the network chatter that enters your system.

Depending on the levels set within each Event Definition, the number of events detected can be quite high. Yet only a portion of those events may be meaningful. By modifying the thresholds and other criteria that make up an event, you can reduce the number of false alarms.
Note - It is recommended to run Learning Mode before beginning to manually change Event Definitions. See Using Learning Mode (see "Tuning SmartEvent Using Learning Mode" on page 37) for details.

These modifications are done in the Event Definitions. A high-level view of the process of modifying Event Definitions is as follows:

1. Select a type of event from one of the Event Policy categories.
2. Adjust the Event Definitions as desired. The elements that can be modified vary per Event Definition. Some event types will include all; others will have just one or two of these configurable elements.
3. When you have finished making changes to the Event Definitions, save the Event Policy by selecting File > Save.
4. From the Actions menu, select Install Event Policy.

Event Definitions and General Settings

The Selector tree is divided into two branches: Event Policy and General Settings. All of the events detectable by SmartEvent are organized by category in the Event Policy branch. Selecting an event's definition displays its configurable properties in the Detail pane, and a description of the event in the Description pane. Clearing the property removes this type of event from SmartEvent's Event Policy the next time the Event Policy is installed.

The General Settings branch contains Initial Settings, such as defining Correlation Units, which are typically used for initial configuration. Clicking on a General Settings item displays its configurable properties in the Detail pane.

For details on specific attacks/events, refer to the Event Definition's Detail pane.

Event Definition Parameters

When an event's definition is selected, its configurable elements appear in the Detail pane, and a description of the event is displayed in the Description pane. There are generally six types of configurable elements:

- Thresholds, such as Detect the event when more than x connections were detected over y seconds
- Severity, such as Critical, Medium, Informational, etc.
- Automatic Reactions, such as Block Source or run External Script
- Exclusions, such as Exclude the following sources and destinations
- Exceptions, such as Apply the following exceptions
- Time Object, such as to issue an event if the following occurs outside the following Working Hours

Not all of these elements appear for every Event Definition. After installing and running SmartEvent for a short time, you will discover which of these elements need to be fine-tuned per Event Definition. For more about fine-tuning Event Definitions, see Configurable Elements of Event Definitions.

The configurable settings are straight-forward for the General Settings items. Adding a Time Object opens a window to set the appropriate hours and days of the week. For configuration information regarding most objects in General Settings, see System Administration (on page 59).

Event Threshold

The Event Threshold allows you to modify the limits that, when exceeded, indicates that an event has occurred. The limits typically are the number of connections, logs, or failures, and the period of time in which they occurred. It appears thus:

Detect the event when more than x connections/logs/failures (etc.) were detected over a period of y seconds.

One way of decreasing the number of false alarms based on a particular event is to increase the number of connections, logs or failures and/or the period of time for them to occur.
**Severity**

An event’s severity affects in which queries (among those that filter for severity) this type of event will appear.

To modify the severity of an event, select a severity level from the drop-down list.

**Automatic Reactions**

Upon detection, an event can activate an Automatic Reaction. The SmartEvent administrator can create and configure a single Automatic Reaction, or many, according to the needs of the system. For example, a single Mail Reaction can be defined to inform the administrator of any event to which it is applied, or multiple Automatic Mail Reactions can be created in order to inform a different responsible party for each type of event.

There are five kinds of Automatic Reactions:

- **Mail** - alert an administrator by email that the event has occurred
- **SNMP Trap** - generate an SNMP Trap
  
  It is possible to send event fields in the SNMP Trap message. The format for such an event field is `[seam_event_table_field]`. The following list represents the possible `seam_event` table fields:

  - `AdditionalInfo` varchar(1024)
  - `AutoReactionStatus` varchar(1024)
  - `Category` varchar(1024)
  - `DetectedBy` integer
  - `DetectionTime` integer
  - `Direction` integer
  - `DueDate` integer
  - `EndTime` integer
  - `EventNumber` integer
  - `FollowUp` integer
  - `IsLast` integer
  - `LastUpdateTime` integer
  - `MaxNumOfConnections` integer
  - `Name` varchar(1024), `NumOfAcceptedConnections` integer
  - `NumOfRejectedConnections` integer
  - `NumOfUpdates` integer
  - `ProductCategory` varchar(1024)
  - `ProductName` varchar(1024)
  - `Remarks` varchar(1024)
  - `RuleID` varchar(48)
  - `Severity` integer
  - `StartTime` integer
  - `State` integer
  - `TimeInterval` integer
  - `TotalNumOfConnections` varchar(20)
  - `User` varchar(1024)
  - `Uuid` varchar(48)
  - `aba_customer` varchar(1024),
  - `jobID` varchar(48)
  - `policyRuleID` varchar(48)
- **Block Source** - instruct the Security Gateway to block the source IP address(es) from which this event was detected for a configurable period of time (choose any period of time from one minute to over three weeks).
• **Block Event activity** - instruct the Security Gateway to block a distributed attack emanating from multiple sources or attacking multiple destinations for a configurable period of time (choose any period of time from one minute to over three weeks).

• **External Script** - run a script that you provide. See Creating an External Script (on page 62) for help in writing a script that can exploit SmartEvent's data.

Each Automatic Reaction must be defined, and that can be done either from within an Event Definition, or from General Settings > Objects > Automatic Reactions.

The following sections describe how to add an Automatic Reaction to an event, and how to create

Adding an Automatic Reaction to an Event

To add an Automatic Reaction for SmartEvent to execute when this type of event is detected, proceed as follows:

1. Select the icon 
2. Either select an Automatic Reaction that you have created from the list, or select Add new…. (See section below for details on creating each type of Automatic Reaction.)
3. Configure the Automatic Reaction, and then select Save.
4. Click OK.

Creating Automatic Reactions

Automatic Reactions can be created either from:

• within an Event Definition, by selecting the icon [...] and clicking Add new…
• the Policy tab, by selecting General Settings > Objects > Automatic Reactions

The first step for each of the following procedures assumes that you are at one of these two starting points.

Create a Mail Reaction

1. Select Add > Mail.
2. Give the automatic reaction a significant Name.
3. Fill out the Mail Parameters of From, To and cc. To add multiple recipients, separate each email address with a semi-colon. Note that the Subject field has the default variables of [EventNumber] - [Severity] - [Name], which automatically adds to the mail's subject the event number, severity and name of the event that triggered this reaction. These variables can be removed at your discretion. You can also include your own standard text per mail reaction.
4. Enter the domain name of the SMTP server.
5. Select Save.

Create an SNMP Trap Reaction

1. Select Add > SNMP Trap.
2. Give the automatic reaction a significant Name.
3. Fill out the SNMP Trap parameters of Host, Message, OID and Community name. The command send_snmp uses values that are found in the file chkpnnt.mib, in the directory $CPDIR/lib/snmp/. Any OID value used in the SNMP Trap parameters window must be defined in chkpnnt.mib, or in a file that is referenced by it. If the OID field is left blank, then the value is determined from iso.org.dod.internet.private.enterprises.checkpoint.products.fw.fwEvent = 1.3.6.1.4.1.2620.1.1.11. When the automatic reaction occurs, the SNMP Trap is sent as a 256 byte DisplayString text. However, if the OID type is not text, the message is not sent.
4. Select Save.

Create a Block Source Reaction

1. Select Add > Block Source.
2. Give the automatic reaction a significant Name.
3. Select from the drop-down list or enter the number of minutes to block this source.
4. Select Save.

Create a Block Event Activity Reaction

1. Select Add > Block Event Activity.
2. Give the automatic reaction a significant **Name**.
3. Select from the drop-down list or enter the number of minutes to block this source.
4. Select **Save**.

**Create an External Script Reaction**
1. Select **Add > External Script**.
2. Give the automatic reaction a significant **Name**.
3. Either provide the full path and file extension of the script to be run, or be sure that the executable resides on the SmartEvent server in the directory `$FWDIR/bin`. The path and script name must not contain any spaces.
4. Select **Save**.

*Note* - The script must run no longer than 10 minutes, otherwise it will be terminated by the SmartEvent Server.

**Working Hours**

Working Hours are used to detect unauthorized attempts to access protected systems and other forbidden operations after-hours. To set the **Regular Working Hours** for an event, select a **Time Object** that you have configured from the drop-down list.

**To create a Time Object:**
1. From the **Policy** tab, select **General Settings > Objects > Time Objects**.
2. Click **Add**. Enter a **Name** and **Description**.
3. Select the days and times that are considered **Regular Working Hours**.
4. Click **OK**.

**To assign a Time Object to an event:**
1. From the **Policy** tab, select an event that requires a **Time Object** (for example, **User Login at irregular hours** in the **Unauthorized Entry** event category).
2. Select the **Time Object** you created from the drop-down list.
3. Select **File > Save** to save the configuration.

**Adding Exclusions**

Exclusions remove log entries from query results according to defined criteria (query properties). For example, if source `10.10.10.1` is defined as an exclusion for an event, all events with source `10.10.10.1` do not show in the query result. Global Exclusions work in the same way, except they apply to all events.

You can add exclusions in one of these ways:

- Manually using this window
- By accepting Learning Mode recommendations
- By right-clicking an event and selecting **Exclude from event definition**.

**To manually add an exclusion:**
1. Click **Add**.
2. In the **Exclusion** window, select the **Source** and/or destination **Server** object you want to exclude from the query results.
3. Configure any other filter criteria that is available for the specified event.
4. Optionally, click **Apply and delete existing events** to remove the excluded events from the existing query results.

*Note* - If you do not see the host object listed, you may need to create it in SmartEvent (see "Adding Network and Host Objects" on page 60).

Existing exclusions can be modified or deleted by selecting **Edit** or **Remove**, respectively.
Exceptions

Exceptions allow an event to be independently configured for the sources or destinations that appear here. For example, if the event *Port Scan from Internal Network* is set to detect an event when 30 port scans have occurred within 60 seconds, you can also define that two port scans detected from host *A* within 10 seconds of each other is also an event.

To manually add an exception, under the heading *Apply the following exceptions*, click *Add* and select either the *Source* and/or *Destination* of the object to which you want to apply different criteria for this event.

Note - If you do not see the host object listed, you may need to create it in SmartEvent (see "Adding Network and Host Objects" on page 60).

Existing exceptions can be modified or deleted by selecting *Edit* or *Remove*, respectively.

Creating Event Definitions (User Defined Events)

Creating a user-defined event requires knowledge of the method by which SmartEvent identifies events. The following section begins with a high level overview of how logs are analyzed to determine if an event is occurring or has occurred.

High Level Overview of Event Identification

Events are detected by SmartEvent's Correlation Unit. The Correlation Unit's task is to scan logs for criteria that match an Event Definition. SmartEvent employs a four step process to identify an event:

- Step 1: Matching a Log Against Global Exclusions (on page 42)
- Step 2: Matching a Log Against Each Event Definition (on page 43)
- Step 3: Creating an Event Candidate (on page 44)
- Step 4: When a Candidate Becomes an Event (on page 46)

**Step 1: Matching a Log Against Global Exclusions**

When the Correlation Unit reads a log, it first checks whether the log matches any defined *Global Exclusions*. Global Exclusions (defined on the *Policy* tab > *Event policy* > *Global Exclusions*) direct SmartEvent to ignore logs that are not expected to contribute to an event. If the log matches a Global Exclusion, it is discarded by the system. If not, the Correlation Unit begins matching it against each Event Definition.

[Figure 5-7] Checking for Global Exclusions
Step 2: Matching a Log Against Each Event Definition

Each Event Definition contains a filter which is comprised of a number of criteria that must be found in any matching log. The criteria are divided by product; that is, the Event Definition may include a number of different products, but each product has its own criteria.

Figure 5-8 Event Definition Example

<table>
<thead>
<tr>
<th>Product</th>
<th>Endpoint Security</th>
<th>Security Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action Type</td>
<td>firewall</td>
<td>drop, reject</td>
</tr>
<tr>
<td>Port Protocol</td>
<td>80 – 84</td>
<td>80 – 84</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
<td>TCP</td>
</tr>
</tbody>
</table>

For a log from Endpoint Security to match on Event Definition "A", it must match the Action, Event Type, Port, and Protocol values listed in the Endpoint Security column. A log from a Security Gateway must match the values listed in its column.

SmartEvent divides this process into two steps. The Correlation Unit first checks whether the Product value in the log matches one of the acceptable Product values of an Event Definition.

Figure 5-9 Comparing Log "Product" value with Event Definition

If Log 1 did not contain an acceptable Product value, the Correlation Unit would then compare the log against Event Definition "B", and so on. If the log fails to match against any Event Definition, it is discarded.

After checking the "Product" criterion, the Correlation Unit checks whether the log contains the Product-specific criteria to match the Event Definition. For instance, the product Endpoint Security generates logs that involve the Firewall, Spyware, Malicious Code Protection, and others, and the log contains this information in the field "Event Type". If an event is defined to match on Endpoint Security logs with the Event Type "Firewall", then an Endpoint Security log with Event Type "Spyware" will fail against the Event Definition's filter. Other criteria may be specific to the Product as well.

Returning to our example, Log 1 has matched Event Definition "A" with an acceptable Product value. The Correlation Unit now examines whether the log contains the necessary criteria for an Endpoint Security log to match.

Figure 5-10 Comparing Log Details with Event Definition

If the criteria did not match, the Correlation Unit would continue comparing the log's criteria to other Event Definitions, until discarding it.
Step 3: Creating an Event Candidate

Once a log matches the Event Definition's criteria, it becomes or is added to an Event Candidate. Event Candidates are SmartEvent's way of tracking logs until an event threshold has been crossed, at which point an event is generated.

Figure 5-11  Event Candidate

<table>
<thead>
<tr>
<th>Product</th>
<th>Security Gateway</th>
<th>Product</th>
<th>Security Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>reject</td>
<td>Action</td>
<td>block</td>
</tr>
<tr>
<td>Port</td>
<td>83</td>
<td>Type</td>
<td>firewall</td>
</tr>
<tr>
<td>Protocol</td>
<td>TCP</td>
<td>Port</td>
<td>84</td>
</tr>
<tr>
<td>Source</td>
<td>1.1.1.5</td>
<td>Protocol</td>
<td>TCP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source</td>
<td>1.1.1.5</td>
</tr>
</tbody>
</table>

Note that:

- the Event Candidate can track logs from multiple products
- the logs must originate from the same source
- the Event Candidate tracks logs even before all of the criteria have been matched

Each Event Definition may have multiple Event Candidates existing simultaneously, each of which is keeping track of logs grouped by similar properties, such as by host, service, destination, or any combination of these or others. In the figure above the logs that form the Event Candidate have a common Source value, and have been dropped, blocked or rejected by a firewall. They are grouped together because the Event Definition is designed to detect this type of activity originating from a single source.
Whenever a log matches the Event Definition but has properties different than those of the existing Event Candidates, a new Event Candidate is created and added to what can be thought of as the Event Candidate Pool.

**Figure 5-12** New Event Candidate Added to the Pool

Note that SmartEvent creates a new Event Candidate for a log with a different source.
To illustrate further, consider an event defined to detect a high rate of blocked connections. SmartEvent tracks the number of blocked connections for each firewall, and the logs of the blocked traffic at each firewall forms an event candidate. When the threshold of blocked connection logs from any firewall is surpassed, that firewall's event candidate becomes an event. While this Event Definition creates one event candidate for each firewall monitored, other Event Definitions may create many more.

Figure 5-13  A New Log Added to the Event Candidate

The Event Candidate Pool is a dynamic environment, with new logs being added and older logs being discarded when they have exceeded an Event Definition's time threshold.

**Step 4: When a Candidate Becomes an Event**

When a candidate becomes an event, the Correlation Unit forwards the event to the Event Database. But discovering an event does not mean that SmartEvent stops tracking logs related to it. The Correlation Unit will keep adding matching logs to the event as long as they continue to arrive during the event threshold. Keeping the event "open" condenses what might otherwise appear as many instances of the same event to one, and provides accurate, up-to-date information as to the beginning and end time of the event.

**Creating a User-Defined Event**

New Event Definitions can be created by right clicking an existing Event Definition or via the Actions menu:
Right Click | Actions Menu | Description
--- | --- | ---
New | New Custom Event | Launches the Event Definition Wizard, which allows you to choose whether to base the event on an existing Event Definition, or from scratch.
Save As | Save Event As | Creates an Event Definition based on the properties of the highlighted Event Definition. When selecting Save As, the system prompts you to save the selected Event Definition with a new name for later editing. Save As can also be accessed from the Properties window.

All User Defined Events are saved at Policy tab > Event policy > User Defined Events. Once an Event Definition exists here, it can be modified via the Properties window, available by right click and from the Actions menu.

**Creating a New Event Definition**

**To create a User Defined Event based on an existing event:**

1. From the Actions menu, select New Custom Event. The Event Definition Wizard opens.
2. For Create an event, select that is based on an existing event and select an event that has similar properties to the event you want to create. Click Next.
3. Give the Event Definition a name, enter a Description and select a Severity level. Click Next.
4. Set whether the event is generated by:
   - a single log — In many cases, a single log can depict an event, such as a log from a virus scanner that reports that a virus has been found.
   - multiple logs — Multiple logs are required if the event can only be identified as a result of a combination of multiple logs, such as a High Connection Rate.
   Click Next.
5. Check the products that can trigger this event and select Next.
6. Choose whether to edit the product filters.
   - If you added an additional product you can choose whether you want to edit the filters for each product (Edit all product filters), or only those of new products you have added (Edit only newly selected product filters).
   - If you did not add any additional products, you can choose to edit the filters of existing products (Yes) or you can skip the step and leave the product filters unchanged (No, Leave the original files).
   Click Next.
7. Edit or add product filters for each product by For each log field that you want in the Event Definition filter:
   a) Select the Log field from the available Log Field list.
   b) Click Add to edit the filter.
   c) Select whether the filter matches on All Conditions or Any Conditions.
   d) Double-click on the Log field and select the values to use in the filter.
   Click Next.
8. Once you have defined the filters for each product, define how to process logs by selecting values for the following options:
   - **Detect the event when at least ___ logs occurred over a period of ___ seconds** contains the event thresholds that define the event. You can modify the event thresholds by altering the number of logs and/or the period of time that define the event.
   - **Each event definition may have multiple Event Candidates existing simultaneously** allows you to set whether SmartEvent creates distinct Event Candidates based on a field (or set of fields) that you select below.
Select the field(s) by which distinct Event Candidates will be created allows you to set the field (or set of fields) that are used to differentiate between Event Candidates.

- Use unique values of the __ field when counting logs directs SmartEvent to count unique values of the specified field when determining whether the Event Threshold has been surpassed. When this property is not selected, SmartEvent counts the total number of logs received.

9. Click Finish.

Editing a User-Defined Event

1. From the Policy tab > Event policy > User Defined Events, right click a User-Defined Event and select Properties.
2. In the tabs provided make the necessary changes:
   - **Name**
     
     Give the Event Definition a name, enter a Description and select a Severity level. The text you enter in the Description field appears in the Event Description area (under the event's configurable properties).
   - **Filter**
     
     To edit a product filter select the product and do the following:
     
a) Select the Log field from the available Log Fields list.

     If the field you want is not displayed select Show more fields... to add another field to the Log Fields list.

b) Click Add to edit the filter.

c) Select whether the filter matches on All Conditions or Any Conditions.
   - **Count logs**
     
     This screen defines how SmartEvent counts logs associated with this event.

- **a single log** — In many cases, a single log can depict an event, such as a log from a virus scanner that reports that a virus has been found.

    With this option you can set the fields that are used to group events into Event Candidates. Logs with matching values for these fields are added to the same event. For example, multiple logs reporting a virus detected on the same source with the same virus name will be combined into the same event.

- **multiple logs** — Multiple logs are required for events that identify a certain level of activity, such as a High Connection Rate.

    When the event is triggered by multiple logs, set the behavior of Event Candidates:

    **Detect the event when at least...** — Set the Event Threshold that, when exceeded, indicates that an event has occurred.

    **Select the field(s) by which distinct event candidates will be created** — An event is generated by logs with the same values in the fields specified here. Define how logs are grouped into Event Candidates by selecting the relevant fields here.

    **Use unique values of the ...** — Only logs with unique values for the fields specified here are counted in the event candidate. For example, a port scan event might count logs that include unique ports scanned, and do not increment the log count for logs that contain ports already encountered in the event candidate.

    **Advanced** — enables you to define the keep-alive time for the event, as well as how often the Correlation Unit updates the SmartEvent server with new logs for the created event.

   - **Event Format**
     
     When an event is generated, information about the event is presented in the Event Detail pane.

     This screen lets you specify whether the information will be added to the detailed pane and from which Log Field the information is taken.

     If you do not want to populate an Event Field clear it in the Display column.
All events can be configured and this screen allows you to determine the configuration parameters that are displayed.

The **Threshold section** will display the number of logs that need to be matched to create the event. This is usually not displayed for single log events and displayed for multiple log events.

The **Exclude section** lets you specify the log fields that will be displayed when adding an event exclusion.

The **Exception section** lets you specify the log fields that will be displayed when adding an event exception.

3. Click **Ok** to save your changes.
Chapter 6

Eliminating False Positives

The purpose of this chapter is to provide additional assistance in reducing false positives.

In This Chapter

Services that Generate Events 50
Common Events by Service 50

Services that Generate Events

Certain types of services are characterized by a high amount of traffic that could be misidentified as events. The following are examples of services and protocols that could potentially generate events:

- Software that performs a routine scan of the network to make sure that everything is running properly. Configuring SmartEvent to exclude this source from a scan event will eliminate a source of false positive events.
- High connection rate on a web server. SmartEvent should be set to allow a higher connection rate per minute on a busy web server, or to exclude this source from a scan event.

Common Events by Service

The information in the table below provides a list of server types where high activity is common. Modify the Event Policy by adjusting event thresholds and adding Exclusions for servers and services in order to further reduce the amount of false positives detected.

Table 6-1 Common events by service

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Category</th>
<th>Event Name</th>
<th>Source</th>
<th>Dest</th>
<th>Service</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP</td>
<td>Scans</td>
<td>IP sweep from internal network</td>
<td>Any</td>
<td>Any</td>
<td>SNMP-read</td>
<td>Hosts querying other hosts</td>
</tr>
<tr>
<td>DNS Servers</td>
<td>Scans</td>
<td>IP sweep from internal network</td>
<td>DNS servers</td>
<td>-</td>
<td>DNS</td>
<td>Inter-DNS servers updates</td>
</tr>
<tr>
<td>Denial of Service (DoS)</td>
<td></td>
<td>High connection rate on internal host on service</td>
<td>Any</td>
<td>DNS servers</td>
<td>DNS</td>
<td>DNS requests and inter-DNS servers updates</td>
</tr>
<tr>
<td>Anomalies</td>
<td></td>
<td>High connection rate from internal network</td>
<td>Any</td>
<td>Any</td>
<td>DNS</td>
<td>DNS requests and inter-DNS servers updates</td>
</tr>
<tr>
<td>Server Type</td>
<td>Category</td>
<td>Event Name</td>
<td>Source</td>
<td>Dest</td>
<td>Service</td>
<td>Reason</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
<td>-------</td>
<td>---------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal network on service</td>
<td>Any</td>
<td>Any</td>
<td>DNS</td>
<td>DNS requests and inter-DNS servers updates</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>Abnormal activity on service</td>
<td>Any</td>
<td>Any</td>
<td>DNS</td>
<td>DNS requests and inter-DNS servers updates</td>
</tr>
<tr>
<td>NIS Servers</td>
<td>Scans</td>
<td>Port scan from internal network</td>
<td>NIS servers</td>
<td>Any</td>
<td>-</td>
<td>Multiple NIS queries</td>
</tr>
<tr>
<td></td>
<td>Denial of Service (DoS)</td>
<td>High connection rate on internal host on service</td>
<td>Any</td>
<td>NIS servers</td>
<td>NIS</td>
<td>NIS queries</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal network</td>
<td>Any</td>
<td>Any</td>
<td>NIS</td>
<td>NIS queries</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal network on service</td>
<td>Any</td>
<td>Any</td>
<td>NIS</td>
<td>NIS queries</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>Abnormal activity on service</td>
<td>Any</td>
<td>Any</td>
<td>NIS</td>
<td>NIS queries</td>
</tr>
<tr>
<td>LDAP Servers</td>
<td>Denial of Service (DoS)</td>
<td>High connection rate on internal host on service</td>
<td>Any</td>
<td>LDAP servers</td>
<td>LDAP</td>
<td>LDAP requests</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal network</td>
<td>Any</td>
<td>LDAP servers</td>
<td>LDAP</td>
<td>LDAP requests</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal network on service</td>
<td>Any</td>
<td>LDAP servers</td>
<td>LDAP</td>
<td>LDAP requests</td>
</tr>
<tr>
<td>Server Type</td>
<td>Category</td>
<td>Event Name</td>
<td>Source</td>
<td>Dest</td>
<td>Service</td>
<td>Reason</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------</td>
<td>---------</td>
<td>---------------</td>
<td>-------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>Abnormal activity on service</td>
<td>Any</td>
<td>LDAP servers</td>
<td>LDAP</td>
<td>LDAP requests</td>
</tr>
<tr>
<td>HTTP Proxy Servers - Hosts To Proxy Server</td>
<td>Denial of Service (DoS)</td>
<td>High connection rate on internal host on service</td>
<td>Any</td>
<td>Proxy servers</td>
<td>HTTP:8080</td>
<td>Hosts connections to Proxy servers</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal network</td>
<td>Any</td>
<td>Proxy servers</td>
<td>HTTP:8080</td>
<td>Hosts connections to Proxy servers</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal hosts on service</td>
<td>Any</td>
<td>Proxy servers</td>
<td>HTTP:8080</td>
<td>Hosts connections to Proxy servers</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>Abnormal activity on service</td>
<td>Any</td>
<td>Proxy servers</td>
<td>HTTP:8080</td>
<td>Hosts connections to Proxy servers</td>
</tr>
<tr>
<td>HTTP Proxy Servers - Out to the Web</td>
<td>Scans</td>
<td>IP sweep from internal network</td>
<td>Proxy servers</td>
<td>Any</td>
<td>HTTP/HTTPS</td>
<td>Proxy servers connections out to various sites</td>
</tr>
<tr>
<td></td>
<td>Denial of Service (DoS)</td>
<td>High connection rate on internal host on service</td>
<td>Proxy servers</td>
<td>Any</td>
<td>HTTP/HTTPS</td>
<td>Proxy servers connections out to various sites</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal network</td>
<td>Proxy servers</td>
<td>Any</td>
<td>HTTP/HTTPS</td>
<td>Proxy servers connections out to various sites</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High connection rate from internal hosts on service</td>
<td>Proxy servers</td>
<td>Any</td>
<td>HTTP/HTTPS</td>
<td>Proxy servers connections out to various sites</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>Abnormal activity on service</td>
<td>Proxy servers</td>
<td>Any</td>
<td>HTTP/HTTPS</td>
<td>Proxy servers connections out to various sites</td>
</tr>
<tr>
<td></td>
<td>UFP Servers</td>
<td>Denial of Service (DoS)</td>
<td>Any</td>
<td>UFP servers</td>
<td>Any/UFP by vendor</td>
<td>firewall connections to UFP servers</td>
</tr>
<tr>
<td>Server Type</td>
<td>Category</td>
<td>Event Name</td>
<td>Source</td>
<td>Dest</td>
<td>Service</td>
<td>Reason</td>
</tr>
<tr>
<td>-------------</td>
<td>------------</td>
<td>-------------------------------------------------</td>
<td>--------</td>
<td>----------</td>
<td>---------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal network</td>
<td>Any</td>
<td>UFP</td>
<td>Any/UFP by vendor</td>
<td>firewall connections to UFP servers</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal hosts on service</td>
<td>Any</td>
<td>UFP</td>
<td>Any/UFP by vendor</td>
<td>firewall connections to UFP servers</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>Abnormal activity on service</td>
<td>Any</td>
<td>UFP</td>
<td>Any/UFP by vendor</td>
<td>firewall connections to UFP servers</td>
</tr>
<tr>
<td></td>
<td>CVP Servers Request</td>
<td>High connection rate on internal host on service</td>
<td>Any</td>
<td>CVP</td>
<td>Any/CVP by vendor</td>
<td>firewall connections to CVP servers</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal network</td>
<td>Any</td>
<td>CVP</td>
<td>Any/CVP by vendor</td>
<td>firewall connections to CVP servers</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal hosts on service</td>
<td>Any</td>
<td>CVP</td>
<td>Any/CVP by vendor</td>
<td>firewall connections to CVP servers</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>Abnormal activity on service</td>
<td>Any</td>
<td>CVP</td>
<td>Any/CVP by vendor</td>
<td>firewall connections to CVP servers</td>
</tr>
<tr>
<td></td>
<td>CVP Servers Replies</td>
<td>Port scans from internal network</td>
<td>CVP</td>
<td>-</td>
<td>CVP</td>
<td>multiple CVP replies to same GW</td>
</tr>
<tr>
<td></td>
<td>Scans</td>
<td>IP sweep from internal network</td>
<td>CVP</td>
<td>-</td>
<td>CVP</td>
<td>CVP replies to multiple GWs</td>
</tr>
<tr>
<td></td>
<td>Denial of Service (DoS)</td>
<td>High connection rate on internal host on service</td>
<td>CVP servers</td>
<td>Any</td>
<td>Any/CVP by vendor</td>
<td>CVP replies</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal network</td>
<td>CVP</td>
<td>Any</td>
<td>Any/CVP by vendor</td>
<td>CVP replies</td>
</tr>
<tr>
<td>Server Type</td>
<td>Category</td>
<td>Event Name</td>
<td>Source</td>
<td>Dest</td>
<td>Service</td>
<td>Reason</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------------</td>
<td>--------------</td>
<td>--------------</td>
<td>--------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal hosts on service</td>
<td>CVP servers</td>
<td>Any</td>
<td>Any/CVP by vendor</td>
<td>CVP replies</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>Abnormal activity on service</td>
<td>CVP servers</td>
<td>Any</td>
<td>Any/CVP by vendor</td>
<td>CVP replies</td>
</tr>
<tr>
<td>UA Servers</td>
<td>Denial of</td>
<td>High connection rate on internal host on service</td>
<td>Any</td>
<td>UA servers</td>
<td>uas-port (TCP:19191 TCP:19194)</td>
<td>connections to UA servers</td>
</tr>
<tr>
<td>Request (DoS)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal network</td>
<td>Any</td>
<td>UA servers</td>
<td>uas-port (TCP:19191 TCP:19194)</td>
<td>connections to UA servers</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal hosts on service</td>
<td>Any</td>
<td>UA servers</td>
<td>uas-port (TCP:19191 TCP:19194)</td>
<td>connections to UA servers</td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>Abnormal activity on service</td>
<td>Any</td>
<td>UA servers</td>
<td>uas-port (TCP:19191 TCP:19194)</td>
<td>connections to UA servers</td>
</tr>
<tr>
<td>UA Servers</td>
<td>Scans</td>
<td>Port scans from internal network</td>
<td>UA servers</td>
<td>Any</td>
<td>-</td>
<td>multiple UA replies to the same machine</td>
</tr>
<tr>
<td>Reponses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scans</td>
<td></td>
<td>IP sweep from internal network</td>
<td>UA servers</td>
<td>Any</td>
<td>uas-port (TCP:19191 TCP:19194)</td>
<td>multiple UA replies to multiple machines</td>
</tr>
<tr>
<td></td>
<td>Denial of</td>
<td>High connection rate on internal host on service</td>
<td>UA servers</td>
<td>Any</td>
<td>uas-port (TCP:19191 TCP:19194)</td>
<td>UA replies</td>
</tr>
<tr>
<td>Service (DoS)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anomalies</td>
<td>High connection rate from internal network</td>
<td>UA servers</td>
<td>Any</td>
<td>uas-port (TCP:19191 TCP:19194)</td>
<td>UA replies</td>
</tr>
</tbody>
</table>

**Notes:**
- UA: UA Server
- CVP: CVP Server
- uas-port: UA port
- TCP: Transmission Control Protocol
<table>
<thead>
<tr>
<th>Server Type</th>
<th>Category</th>
<th>Event Name</th>
<th>Source</th>
<th>Dest</th>
<th>Service</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anomalies</td>
<td></td>
<td>High connection rate from internal hosts on service</td>
<td>UA servers</td>
<td>Any</td>
<td>uas-port (TCP:19191 TCP:19194)</td>
<td>UA replies</td>
</tr>
<tr>
<td>Anomalies</td>
<td></td>
<td>Abnormal activity on service</td>
<td>UA servers</td>
<td>Any</td>
<td>uas-port (TCP:19191 TCP:19194)</td>
<td>UA replies</td>
</tr>
<tr>
<td>SMTP Servers</td>
<td>Scans</td>
<td>IP sweep from internal network</td>
<td>SMTP servers</td>
<td>-</td>
<td>SMTP</td>
<td>SMTP servers connections out to various SMTP servers</td>
</tr>
<tr>
<td></td>
<td>Denial of Service (DoS)</td>
<td>High connection rate on internal host on service</td>
<td>SMTP servers</td>
<td>Any</td>
<td>SMTP</td>
<td>SMTP servers connections out to various SMTP servers</td>
</tr>
<tr>
<td>Anomalies</td>
<td></td>
<td>High connection rate from internal network</td>
<td>SMTP servers</td>
<td>Any</td>
<td>SMTP</td>
<td>SMTP servers connections out to various SMTP servers</td>
</tr>
<tr>
<td>Anomalies</td>
<td></td>
<td>High connection rate from internal hosts on service</td>
<td>SMTP servers</td>
<td>Any</td>
<td>SMTP</td>
<td>SMTP servers connections out to various SMTP servers</td>
</tr>
<tr>
<td>Anomalies</td>
<td></td>
<td>Abnormal activity on service</td>
<td>SMTP servers</td>
<td>Any</td>
<td>SMTP</td>
<td>SMTP servers connections out to various SMTP servers</td>
</tr>
<tr>
<td>Anti-virus</td>
<td>Scans</td>
<td>IP sweep from internal network</td>
<td>AVDefs servers</td>
<td>-</td>
<td>Any/AV by vendor</td>
<td>Anti-Virus definitions updates deployment</td>
</tr>
<tr>
<td>Definition Servers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Denial of Service (DoS)</td>
<td>High connection rate on internal host on service</td>
<td>AVDefs servers</td>
<td>-</td>
<td>Any/AV by vendor</td>
<td>Anti-Virus definitions updates deployment</td>
</tr>
<tr>
<td>Anomalies</td>
<td></td>
<td>High connection rate from internal network</td>
<td>AVDefs servers</td>
<td>-</td>
<td>Any/AV by vendor</td>
<td>Anti-Virus definitions updates deployment</td>
</tr>
</tbody>
</table>
Dynamic Updates

SmartEvent provides you with the ability to download updates from the Check Point User Center. These updates are referred to as Dynamic Updates and they include Check Point Event Definitions and third party product parsing. For additional information on Event Definitions refer to Modifying Event Definitions (on page 37) and Creating Event Definitions (User Defined Events). (see "Creating Event Definitions (User Defined Events)" on page 42)

The update process connects to the User Center and verifies whether or not updates of new event definitions, expanded existing event definitions and/or third party product parsings exist. The administrator has the option of downloading the updates and incorporating them into the Event Policy (a policy that includes events to be detected when connections are made to specific Security Rule Base rules at high rates). Once the Event Policy is installed the administrator must perform an Install Policy in order for the updates to take effect. For additional information about Event Policy refer to Policy Tab.

In the same respect, if the administrator is unsatisfied with the update, it is possible to revert to a revision of the configuration files that is created before the update is executed. There is always only one previous version of the Event Policy since the revision is overwritten each time an update is performed.

Data received as a result of the Dynamic Update process may contain third party syslog and snmpTrap parsing for firewall and SmartEvent parsing. SmartEvent can parse and process third-party syslog and snmpTrap messages. This parsing process extracts relevant log fields from the data and creates a normalized Check Point log which is available for further analysis. The syslog and snmpTrap data is kept in the following directory:

$FWDIR/conf/syslog/CPdefined syslog files

If the administrator wants to modify a file defined by Check Point, the specific file must be copied from the CPdefined Syslog directory and placed in the User Defined Syslog directory ($FWDIR/conf/syslog/UserDefined syslog files).

For additional information about new devices and syslog and snmpTrap parsing please refer to Third-Party Device Support (on page 64).

Perform a Dynamic Update

1. Open SmartEvent.
2. Select Actions > Dynamic Update.
   The Enter Network Password window appears.
3. Enter your User Center password and user name and click OK.
   A window opens and displays the Available Updates List.
4. Select one or more updates.
5. Click Update Now.
   At this point the relevant files are fetched from the User Center and the Event Policy and third party product parsing files are updated in SmartEvent and all Log servers installed on SmartEvent and SmartReporter.
Note - If you have an external log server that parses the third party product data manually copy the fwdir/conf/syslog directory from the SmartEvent Server to the same directory on the log server and invoke cpstop and cpstart.

View Updated Events

1. Open SmartEvent.
2. Select the Policy tab.
3. Select View > View Updated Events.
   The updated events appear in blue in the Event tree.

Revert the Dynamic Update to a Previous Version

1. Open SmartEvent.
2. Select Actions > Undo last policy update.
   If you select Yes, the process updates the Event Policy to its prior definition.

Undo last policy update only applies to Policy Updates and not all updates.

Administrator Permissions Profile - Policy

SmartEvent enables you to provide an administrator with a Permission Profile for the SmartEvent database. A Permission Profile is a permission ID card that is assigned to administrators or administrator groups.

The administrator and his Permission Profile are verified during login. When an administrator logs into SmartEvent his user name and password are verified by the SmartEvent server. If the administrator is not defined on the SmartEvent server, the server will attempt the login process with the credentials that are defined on the Security Management server or Multi-Domain Server connected with SIC to the SmartEvent server.

The Permission Profile types for the SmartEvent Events tab are set in the SmartDashboard or SmartDomain Manager (SmartDashboard > Manage > Permissions Profiles > New / Edit) connected to the Security Management server or Multi-Domain Server with this option:

The following are the four types of Permission Profiles:

- **None** indicates that the administrator cannot view the SmartEvent Policy tab.
- **Read Only** enables the administrator to view SmartEvent Policy tab.
- **Read/Write** enables the administrator to perform Install Policy and modify the SmartEvent Policy tab.
  With Read/Write permissions the administrator can also configure one or both of the following from within the Events tab:
  - **Exclude from Event Definition**
  - **Add Exception to Event Definition**
- **Customized** allows user-defined access to the selected Check Point products and select permissions per application.

Multi-Domain Security Management

When using Multi-Domain Security Management, SmartEvent works with specified Domains. In the Policy tab, administrator can see events, exceptions and exclusions for Domains according to administrator permissions.

A Multi-Domain Security Management Policy administrator can be one of the following:

- Locally defined administrator on the SmartEvent Server
• Multi-Domain Server Super User defined on the Multi-Domain Server.
• An administrator with permissions to all Domains selected in SmartEvent (Policy > General Settings > Objects > Domains). Unlike the two above, this type of administrator can install a policy and can view events that are cross-Domain (an event created from logs that come from multiple Domains).
Chapter 7

System Administration

The following tasks help you maintain your SmartEvent system properly:

- Creating objects for use in filters (see "Adding Network and Host Objects" on page 60)
- Adding additional IPS Event Correlation Units and Log servers (see "Defining Correlation Units and Log Servers" on page 60)
- Adding objects to the Internal Network (see "Defining the Internal Network" on page 61)
- Creating or modifying custom commands that can be run from the SmartEvent client (see "Configuring Custom Commands" on page 62)
- Creating scripts to run as Automatic Reactions for certain events (see "Creating an External Script" on page 62)
- Modify the database settings to fit your disk space and requirements (see "Managing the Event Database" on page 63)

These tasks can be performed from the Policy tab.

Modifications to the Event Policy do not take effect until saved on the SmartEvent server and installed to the Correlation Units.

To enable changes made to the Event Policy, proceed as follows:

1. Select File > Save.
2. Select Actions > Install Event Policy.

Changes made to the Event Policy can be undone if the changes have not been saved first. To undo changes made to the policy, select File > Revert Changes.

In This Chapter

- Modifying the System's General Settings
- Managing the Event Database
- SmartEvent High Availability Environment
- Third-Party Device Support

Modifying the System's General Settings

The following tasks help you maintain your SmartEvent system:

- Creating objects for use in filters, as described in Adding Network and Host Objects (on page 60).
- Adding additional IPS Event Correlation Units and Log servers, as detailed in Defining Correlation Units and Log servers (on page 60)
- Adding objects to the Internal Network, as described in Defining the Internal Network (on page 61)
- Creating or modifying custom commands that can be run from the SmartEvent client, as explained in Configuring Custom Commands (on page 62)
- Creating scripts to run as Automatic Reactions for certain events, as detailed in Creating an External Script (on page 62).

These tasks can be performed from the Policy tab. The Policy tab is hidden by default, but can be revealed by selecting Policy Tab from the View menu.
Modifying the System's General Settings

Adding Network and Host Objects

Certain objects from the Management server are added during the initial sync with the SmartEvent server and updated at a set interval. However, it may be necessary or useful to add other Network or Host objects, for the following reasons:

- If you have devices or networks not represented on the Management server that are important for the purpose of defining your internal network
- When adding sources or destinations to exclusions or exceptions in Event Definitions
- When selecting sources or destinations in a filter

The following screens are locked until initial sync is complete:

- Network Objects
- Internal Network
- Correlation Units

To make these devices available for use in SmartEvent, proceed as follows:

For a Host object:
1. From the Policy tab, select General Settings > Objects > Network Objects > Add > Host.
2. Give the device a significant Name.
3. Enter its IP Address or select Get Address.
4. Select OK.

For a Network object:
1. From the Policy tab, select General Settings > Objects > Network Objects > Add > Network.
2. Give the network a significant Name.
3. Enter the Network Address and Net Mask.
4. Select OK.

See Defining the Internal Network (on page 61) for information on adding objects to the Internal Network definition.

Defining Correlation Units and Log Servers

The SmartEvent system works with correlation units that compile event information from log servers. Additional Correlation Units and their corresponding Log servers should be configured during the initial system setup.

To define Correlation Units or Log servers in SmartEvent:
1. From the Policy tab, select General Settings > Initial Settings > Correlation Units.
2. Select Add.
3. Select the [...] symbol and select a Correlation Unit from the pop-up window.
4. Select OK.
5. Select Add and select a Log server available to the Correlation Unit from the pop-up window.
6. Select Save.
7. From the Actions menu, select Install Event Policy.

Note - The following screens are locked until sync is complete:
- Network Objects
- Internal Network
- Correlation Units

To define Correlation Units in SmartEvent Intro:
- In a Security Management Server environment: correlation is defined automatically.
- In a Multi-Domain Security Management environment: do the previous procedure on the Multi-Domain Server.
Defining the Internal Network

To help SmartEvent determine whether events have originated internally or externally, the Internal Network must be defined. The direction is calculated as follows:

1. **Incoming** – all the sources are outside the network and all destinations are inside
2. **Outgoing** – all sources are inside the network and all destinations are outside
3. **Internal** – sources and destinations are all inside the network
4. **Other** – a mixture of internal and external values makes the result indeterminate

**To define the Internal Network:**
1. From the Policy tab, select General Settings > Initial Settings > Internal Network.
2. Add internal objects.

   ![Note](image) - It is recommended to add all internal Network objects, and not Host objects

Certain network objects are copied from the Management server to the SmartEvent server during the initial sync and updated afterwards periodically.

The following screens are locked until initial sync is complete:

- Network Objects
- Internal Network
- Correlation Units

Offline Log Files

SmartEvent enables an administrator to view existing logs from a previously generated log file. This feature is designed to enable an administrator to review security threats and pattern anomalies that appeared in the past. As a result, an administrator can investigate threats (for example, unauthorized scans targeting vulnerable hosts, unauthorized legions, denial of service attacks, network anomalies, and other host-based activity) before SmartEvent was installed.

In the same respect, an administrator can review logs from a specific time period in the past and focus on deploying resources on threats that have been active for a period of time but may have been missed (for example, new events which may have been dynamically updated can now be processed over the previous period).

The generation of Offline logs are set in the SmartEvent > Policy tab > General Settings > Initial Settings > Offline Jobs, connected to the Security Management server or Multi-Domain Server with the following options:

- **Add** enables you to configure an Offline Log File process.
  - **Name** acts as a label that enables you to recognize the specific Offline Log file for future processing. For example, you can create a query according to the Offline Job's name. This name is used in Event tab queries to search events that have been generated by this job.
  - **Comment** contains a description of the Offline Job for edification.
  - **Offline Job Parameters**:
    - **Correlation Unit** the machine that reads and processes the Offline Logs.
    - **Log Server** the machine that contains the Offline Log files. SmartEvent will query this log server to see which log files are available.
    - **Log File** contains a list of available log files found on the selected Log server to be processed by the correlation unit. In this window you select the log file from which you would like to retrieve historical information.

- **Edit** enables you to modify the parameters of an Offline Log File process.

- **Remove** enables you to delete an Offline Log File process.

Once you **Start** an Offline Log File process you cannot remove it.

- **Start** runs the Offline Log File process.
The results of this process appear in the **Events** tab and are accessible by the **By Job Name** query or filter.

- **Stop** ends the Offline Log Files process.
- **Stop** does not delete the entire process, it only stops the process at the specific point at which it is selected. The information collected up until the process is stopped will appear in the **Events** tab.

With the SmartEvent **Events Tab** you can add offline jobs to query events generated by offline jobs. To do this perform the following:

1. Select the **Events** Tab.
2. Go to **Predefined > By Job Name**.
3. Double-click **By Job Name**.
   - Every job that appears in this window is an offline job except for **All online jobs**.
4. Select the job you want the **By Job Name** to query.
5. Click **OK**.

### Configuring Custom Commands

**To add (or edit) custom commands:**

1. Select **Actions > Configure Custom Commands**.
2. To add a command, select **Add…**. (To edit an existing command, highlight the command and select **Edit**.)
3. Enter the text to appear in the right-click context menu.
4. Enter the command to run, and any arguments.
5. Select whether the command should be run in a SmartEvent window or a separate Windows command window.
6. Select whether the command should appear in the context menu only when right-clicking in cells with IP address data.
7. Select **OK**.

### Creating an External Script

An external script can be written to receive an Event Definition via standard input. The format of the event content is a name-value set – a structured set of fields that have the form:

```
(name: value ;*
```

where **name** is a string and **value** is either free text until a semicolon, or a nested name-value set. The script will be reported as successful if it completes within 10 minutes and its exit status is zero.

The following is a sample event as it is received by an external script:

```
(Name: Check Point administrator credential guessing; RuleID: {F182D68C-A0AA-444a-9F31-C0C22ACA2114}; Uuid: <42135c9c,00000000,2e1510ac,131c07b6>; NumOfUpdates: 0; IsLast: 0; StartTime: 16Feb2005 16:45:45; EndTime: Not Completed; DetectionTime: 16Feb2005 16:45:48; LastUpdateTime: 0; TimeInterval: 600; MaxNumOfConnections: 3; TotalNumOfConnections: 3; DetectedBy: 2886735150; Origin: (IP: 1.2.3.4; repetitions: 3; countryname: United States; hostname: theHost) ; ProductName: SmartDashboard; User: XYZ; Source: (hostname: theHost; repetitions: 3; IP: 1.2.3.4; countryname: United States) ; Severity: Critical; EventNumber: EN00000184; State: 0; NumOfRejectedConnections: 0; NumOfAcceptedConnections: 0) ;
```

**To add an External Script, proceed as follows:**

1. From the **Policy** tab, select **General Settings > Initial Settings > Automatic Reactions > Add > External Script**.
2. Give the script a name.
3. In the field Action, enter the name of the file containing the script. The script must be placed in the directory $RTDIR/bin/ext_commands, and must have execute privileges.

Managing the Event Database

The Event Database uses a file-switching scheme, where after the database file grows to a set size, it is closed, compacted, and moved to a separate directory, and a new file is opened in its place. After a number of files have been closed, the earliest file is automatically deleted from the disk. For this reason it is a good idea to back up these files to a backup location. It is also therefore important to be able to restore this data, if necessary.

Backup and Restore of the Database

The evs_backup utility backs up the SmartEvent configuration files and places them in a compressed tar file. In addition, it backs up data files based upon the options selected. The files can be restored using the evs_backup_extractor script. Enclosed are two script versions, one for Windows that has a .bat suffix and one for Solaris, Linux and SecurePlatform that does not have a suffix but should have the executable permissions set.

Usage:

Additional options are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvaDb</td>
<td>Copy the SmartEvent events database</td>
</tr>
<tr>
<td>EvrDb</td>
<td>Copy the SmartReporter consolidation database</td>
</tr>
<tr>
<td>Results</td>
<td>Copy the SmartReporter results</td>
</tr>
<tr>
<td>Logs</td>
<td>Copy the SmartEvent error logs</td>
</tr>
<tr>
<td>LogoAndScripts</td>
<td>Copy the logo file and the distribution script</td>
</tr>
<tr>
<td>export</td>
<td>Runs a evr_addon_export, for a different file name use -filename</td>
</tr>
<tr>
<td>All</td>
<td>Select all options</td>
</tr>
</tbody>
</table>

Adjusting the Database Size

The size of the Event Database should be set according to the available disk space on your system. The database size is determined by the number of days that records are kept and the number of records.

To adjust the database size, from the Policy tab, select General Settings > Database Maintenance, and adjust the settings for the fields Number of days to keep records in the database and Number of records to keep in the database.

Backing Up Events

To back up all events, do the following from the command line of the SmartEvent server:

1. Enter the command cpstop to stop the SmartEvent server.
2. Locate the folder $RTDIR/distrib and move its contents to a backup location.
3. Do the same for the folder $RTDIR/events_db.
4. Enter the command cpstart to restart the SmartEvent server.
Deleting Events

To clean the system of all events, do the following on the SmartEvent server:
1. Enter the command `cpstop` to stop the SmartEvent server.
2. Locate the folder `$RTDIR/distrib` and delete all files there.
3. Do the same for the folder `$RTDIR/events_db`.
4. Enter the command `cpstart` to restart the SmartEvent server.

SmartEvent High Availability Environment

The SmartEvent database keeps a synchronized copy of management objects locally on the SmartEvent server. This process, `dbsync`, allows SmartEvent to work independently of different management versions and different management servers in a High Availability environment.


How it works

`Dbsync` initially connects to the management server with which SIC is established. It retrieves all the objects and after the initial synchronization it gets updates whenever an object is saved. At this point, `dbsync` registers all the High Availability management machines and periodically tests the connectivity with the current management server. If connectivity is lost, it attempts to connect to the other High Availability management servers until it finds an active one and connects to it.

If two management servers are active concurrently, `dbsync` will remain connected to one management server and will not receive any changes made on the other management server until a synchronization operation is performed.

Log Server High Availability

In SmartDashboard, it is possible to configure a Security Gateway such that when it fails to send its logs to one log server, it will send its logs to a secondary logs server. In order to support this configuration, it is possible to add both log servers to a single Correlation Unit. In this way, the Correlation Unit will get an uninterrupted stream of logs from both servers and will continue to correlate all firewall logs.

Correlation Unit High Availability

Multiple Correlation Units can read logs from the same log servers and in this way provide redundancy in case one of them fails. The events that the Correlation Units detect will be duplicated in the SmartEvent database; however these events can be disambiguated by filtering with the Detected By field in the Event Query definition. The Detected By field specifies which Correlation Unit detected the event.

In case the SmartEvent server becomes unavailable, the Correlation units retain the events until it can reconnect with the SmartEvent server and will then forward the events.

Third-Party Device Support

New Device Support

Adding support for a log-generating device (e.g., router, firewall, IDS, anti-virus, OS) to SmartEvent involves one or both of the following:

- Adding the data necessary to translate the device's logs to a format that a Check Point Log server can read. This translation is called parsing, and it involves extracting the relevant log fields from the log data to create a normalized Check Point log available for further analysis.
• Adding the device's logs to Event Definitions.

SmartEvent currently supports the following log formats:
• Check Point / OPSEC ELA
• Microsoft Windows Events
• Syslog messages
• SNMP traps

Devices using Check Point, ELA, or Windows Events do not require special parsing configuration. If you are adding a device using one of these formats, skip to the section Adding New Devices to Event Definitions (on page 67). For details on support for Windows logs, see the section Windows Events (on page 14).

Devices using the syslog or SNMP format require parsing configuration. Continue to Planning and Considerations (on page 65) and the parsing section relevant for your device.

### Parsing Log Files

#### Planning and Considerations

1. Learn the exact structure of the logs the device generates with the following
   a) The vendor's logging guide (if it exists), or any other documentation that specifies the different logs the device can generate and their exact structure. Documentation is important to verify that you have found all possible logs and is usually enough to start writing the parsing file.
   b) Log samples, as many as possible. It is recommended to use real logs generated from the actual devices to be used with SmartEvent. Samples are important for testing the parsing file and tuning it accordingly.

2. Consult the Syslog Parsing guide to become familiar with the Free Text Parsing Language. The document also specifies the relevant parsing files and their location on the Log server.

3. Decide which fields to extract from the log. While the fields you want to extract differ from one device to another, devices of the same category would usually have similar log fields. For example:

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Typical Log Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall, router and other devices that send connection based logs</td>
<td>source IP address, destination IP address, source port, destination port, protocol, accept/reject indication</td>
</tr>
<tr>
<td>IDS/IPS, application firewall and other devices that send attack logs</td>
<td>attack name/ID</td>
</tr>
</tbody>
</table>

4. It may also be useful to compare existing parsing files of another similar product.

#### Syslog Parsing

To parse a syslog file:


2. On the Log server, edit the file `$FWDIR/conf/syslog/UserDefined/UserDefinedSyslogDevices.C` to add a line that includes the new parsing file. For example:
Third-Party Device Support

System Administration

Page 66

: ( 
  :command { 
    :cmd_name (include) 
    :file_name ("snortPolicy.C") 
  } 
)

3. If needed, create a new dictionary file called <device product name>_dict.ini (see "Dictionary" on page 78), and place it in the directory $FWDIR/conf/syslog/UserDefined on the Log server. A dictionary translates values with the same meaning from logs from different devices into a common value. This common value is then used in the Event Definitions.

4. If you have added a new dictionary file, edit the file $FWDIR/conf/syslog/UserDefined/UserDefinedSyslogDictionaries.C on the Log server and add a line to include the dictionary file. For example:

:filename ("snort_dict.ini")

To test the parsing, send syslog samples to a Check Point Log server:

1. Configure the Log server to accept syslogs by doing one of the following:
   - Using SmartDashboard, connect to the Security Management server and edit the SmartEvent server network object: Go to Logs and Masters > Additional Logging Configuration and enable the property Accept Syslog messages.
   - On the Log server, run syslog -r to register the syslog daemon.

2. After making any change in the parsing file, restart the fwd process on the Log server (either run the commands cpstop & cpstart, or fw kill fwd & fwd -n)

3. Send syslogs from the device itself, or from a syslog generator, such as Kiwi Syslog Message Generator, available at http://www.kiwisyslog.com/software_downloads.htm#sysloggen, or Adiscon logger, available at http://www.monitorware.com/logger/.

Troubleshooting:

If SmartView Tracker does not display the logs as expected, there may be specific problems with the parsing files:

- If there is a syntax error in the parsing files, an error message will report a failure to read the parsing files. To read a specific error message, set the environment variable TERROR_ALL_FTPARSER value to 5 before running the process fwd -n.
- If the syslogs are displayed in SmartView Tracker with Product 'Syslog', this means the log was not parsed properly, and was parsed as a general syslog.
- If the Product field contains another product (not the one you have just added) this means there is a problem with the other product parsing file. Report this to the Check Point SmartEvent team.
- If the product is reporting correctly in the log, look for all the fields you have extracted. Some of them will be in the Information section. Some fields may only be visible when selecting More Columns.

SNMP Parsing

1. Create a new parsing file called <device product name>.C as specified in the Syslog Parsing guide, and place it in the directory $FWDIR/conf/snmpTrap/UserDefined on the Log server. In the file, use a switch command for the snmp_trap_to_cp_log_param_id field, so that each case contains OID for a specific log field (OID information may be extracted from the device MIB files, if available)

To view an example, see the file $FWDIR/conf/snmpTrap/CPdefined/realSecure.C.

2. Edit the file $FWDIR/conf/snmpTrap/UserDefined/UserDefinedSnmpDevices.C to add lines to include the new parsing file. The value of the attribute case should be the appropriate OID for the product. Note that the product OID should contain exactly seven numeric values, separated by decimal points. For example:

: ( 
  :case ("1.3.6.1.4.1.2499") 
  :command { 
    :cmd_name (include) 
    :file_name ("realSecure.C") 
  } 
)

3. To test the parsing, send SNMP trap samples to a Check Point Log server:
1. Configure the Log server to accept SNMP traps, as follows:
   a) On the Log server, run the command `snmpTrapToCPLog -r` to register the SNMP trap daemon.
   b) On the Log server, run the command `snmpTrapToCPLog -a [ip_addr]` to add the SNMP trap sender.

2. Restart the `snmpTrapToCPLog` process on the Log server after any change in the parsing file (using `cpstop & cpstart` or by terminating the `snmpTrapToCPLog` process and running `snmpTrapToCPLog` again from the command line)


4. If SmartView Tracker does not display the logs as expected, there may be specific problems with your parsing files:
   a) If there is a syntax error in the parsing files, an error message will report a failure to read the parsing files. To read a specific error message, set the environment variable `TDERROR_ALL_SNMP` value to 5 before running the process `snmpTrapToCPLog`.
   b) If the SNMP traps are displayed in SmartView Tracker with Product 'Snmp Trap', this means the log was not parsed properly, and was parsed as a general SNMP trap.
   c) If the Product field contains another product (not the one you have just added) this means there is a problem with the other product parsing file. Report this to the Check Point SmartEvent team.
   d) If the product is reporting correctly in the log, look for all the fields you have extracted. Some of them will be in the Information section. Some fields may only be visible when selecting More Columns.

**Adding New Devices to Event Definitions**

After creating the appropriate parsing file for the new product, the next step is to include the product in the SmartEvent Event Policy by adding it to the Product filters of new and existing events. This involves making changes to the SmartEvent server database. Some of the changes are accomplished using SmartEvent client, while others require using a CPMI client (such as GuiDBedit or dbedit, or a specific client you can write for your own use).

**Note** - Manually editing the files in `$FWDIR/conf` is not recommended and should be done with extreme care.

**Step 1: Create an object to represent the new device in one of the following ways:**

- Using the SmartEvent client:
  a) Right click any of the Event Definitions on the Policy tab and select Properties > Filter tab.
  b) From the Product list section, select Add > Add Product.
  c) Enter the product name as it appears in the Product field of the log.
  d) Select OK.
  e) Select OK again.
  f) Select Cancel to exit the dialog.

- Using another CPMI client:
  a) Enter the class name: `eventia_product_object` and the table: `eventia_products`.
  a) Set the name and the product_displayed_name & product_name fields, for example:

```
: (Snort_IDS
 :product_displayed_name ("Snort IDS")
 :product_name ("Snort IDS")
)
```

The resulting object is added to the file `$FWDIR/conf/sem_products.C`. 
Step 2: Add the device to the relevant Event Definitions:

For example, if this is an IDS/IPS reporting a 'Ping of Death' attack, use the Event Definition Wizard to add a filter for the new product in the 'Ping of Death' Event Definition. You may also add existing or new fields to the product filter by selecting the property Show more fields.

1. Note that Event Definitions cannot be modified, so adding a new filter requires doing one of the following:
   - Saving the relevant Event Definitions as User Defined Events.
   - Overriding this restriction by making a change to the file $FWDIR/conf/sem_detection_policies.C. Use an editor to open the file, search for the line `abacus_detection_policy_object`, and set the value :user_defined to false.

2. Create new Event Definitions where needed if the requested event is not covered by existing Event Definitions. As in step 2, this is accomplished via the Event Definition Wizard. New Event Definitions appear in the User Defined Events section of the Event policy tree.

To move the Event Definition to another section of the tree, do the following:

   a) Use a CPMI client to edit the `abacus_detection_policy_object` in the table `abacus_detection_policies`.
   b) Edit the category field.
   c) To verify that the change has been made, view the object `abacus_detection_policy_object` in the file $FWDIR/conf/sem_detection_policies.C.

3. Consider adding a generic event for the new product (as in the Third Party Devices - User Configured Events section of the Event policy tree).

   a) Create a new Event Definition based on the new product using the Event Definition Wizard.
   b) Use a CPMI client to edit the `abacus_detection_policy_object` in the table `abacus_detection_policies`.
   c) Set the property :create_exception_only for this event to true.
   d) Modify the values of the following fields as desired:
      - exception_rule_static_string_1
      - exception_rule_static_string_2
      - exception_rule_static_string_3
      - static_description_string
      - exception_list_def
      - exception_columns

To test the changes in the Event Definition:

1. Copy the modified files to the directory $FWDIR/conf on the SmartEvent Server.
2. Run cpstop & cpstart on the SmartEvent server.
3. Close and reopen the SmartEvent client.
4. Assuming the Event Definitions are configured as expected, install Event policy.
5. Send logs as described in the testing for parsing above, and see the generated events.

Syslog Parsing

Various third-party devices use the syslog format for logging. SmartEvent can parse and process third-party syslog messages by reformatting the raw data. This parsing process extracts relevant log fields from the syslog data and creates a normalized Check Point log which is available for further analysis.

⚠️ Warning - Manual modifications to out-of-the-box parsing files will not be preserved automatically during the upgrade process. Mark your modifications with comments so you can remember what changed.
**The Parsing Process**

The process takes place on the Log server and begins with the syslog daemon. The syslog daemon running on the Log server receives the syslogs and calls for their parsing. The parsing itself involves various parsing files, which contain the different parsing definitions and specifications and can be found in $FWDIR/conf/syslog. Among these files, are the device-specific parsing files, which define the actual parsing and extraction of fields, according to each device's specific syslog format.

The parsing starts with the `syslog_free_text_parser.C` file. This file defines the different dictionaries (see Dictionary (on page 78)) and performs a preliminary parsing of the syslog, extracting fields which are common to all syslog messages such as PRI, date and time, and the machine and application that generated the syslog. `syslog_free_text_parser.C` then uses the `allDevices.C` file (which includes reference to two files: `UserDefined/UserDefinedSyslogDevices.C` and `CPdefined/CPdefinedSyslogDevices.C`). The first (`UserDefined/UserDefinedSyslogDevices.C`) contains the names of all the devices' parsing files that were defined by the user while the second (`CPdefined/CPdefinedSyslogDevices.C`) contains all devices' parsing files that were defined by Check Point. The `allDevices.C` file starts by going over the user device's parsing files, and tries to match the incoming syslog with the syslog format parsed in that particular file. Once a device parsing-file succeeds in the preliminary parsing of the syslog (that is, it matches the syslog's format and is therefore the syslog's origin), the rest of the syslog is parsed in that file. If a match is not found, the file will continue going over the Check Point device's parsing files until it finds a match.

**The Free Text Parsing Language**

The free text parsing language enables us to parse an input string, extract information and define log fields which appear as part of the Check Point log in the Log server which are then used in the definition of events. Each parsing file contains a tree of commands. Each command tries to check/parse part of the input string (sometimes adding fields to the log as a result) and decides whether to continue parsing the string (according to the success/failure of its execution).

**The Commands**

Each command consists of the following parts:

1. **cmd_name** - the name of the command.
2. **command arguments** - arguments that define the behavior of the command.
3. **on_success** (optional) - the next command executed if the current command's execution succeeds.
4. **on_fail** (optional) - the next command executed if the current command's execution fails.

**Table 7-3 Sample**

```plaintext
:command {
  :cmd_name (try)
  :try_arguments
    ,
  ,
  :on_success (command())
  :on_fail (command())
})
```

**Try**

The **try** command matches a regular expression against the input string.
**Table 7-4 Try Command Parameters**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
</table>
| parse_from | - **start_position** - run the regular expression from the beginning of the input string.  
|            | - **last_position** - run the regular expression from the last position (of the previous successful command). |
| regexp     | The regular expression to match.                                            |
| add_field  | One or more fields to add to the result (only if the regular expression is successful). See Adding a Field (on page 74). |

**Table 7-5 Try Command Sample**

```
:cmd_name (try)
:parse_from (start_position)
:add_field {
   :type (index)
   :field_name (Src)
   :field_type (ipaddr)
   :field_index (1)
}
```

In the above example, we try to match the regular expression `([0-9]+\.[0-9]+\.[0-9]+\.[0-9]+)` looking at the entire log (parse_from (start_position) - parse from the beginning of the log). If the regular expression is matched, we add a source field (See Adding a Field (on page 74)).

**Group_try**

The command **group_try** can executes one or more commands in one of the following four modes:

1. **try_all** tries all the commands in the group and ignores the return code of the commands.
2. **try_all_successively** tries all the commands in the group one after the other and ignores the return code of the commands. Each command tries to execute from the last position of the previous successful command.
3. **try_until_success** tries all the commands until one succeeds.
4. **try_until_fail** tries all the commands until one fails.

The command **group_try** is commonly used when parsing a "free-text" portion of a log, which contains a number of fields we wish to extract. For example:

```
%PIX-6-605004: Login denied from 194.29.40.24/4813 to outside:192.168.35.15/ssh for user 'root'
```

When looking at this section of the log, we can use the following structure:
Table 7-6  Group_try Command Sample 1

```plaintext
:command (
  :cmd_name (group_try)
  :mode (try_all_successively)
  :
    # A "try" command for the source.
    :command ()
  )
  :
    # A "try" command for the destination.
    :command ()
  )
  :
    # A "try" command for the user.
    :command ()
  )
).
.
.
.
```

In this example, the first try command in the group_try block (for the source) is executed. If the source, destination and user appear in no particular order in the syslog, the try_all mode should be used instead of try_all_successively.

Table 7-7  Group_try Command Sample 2

```plaintext
:command (
  :cmd_name (group_try)
  :mode (try_until_success)
  :
    :command (  
      .
      .
      .
      .:regexp ("((\|)(login|su)(\|)\|).* session (opened|closed) for user ([a-z,A-Z,0-9]*)")
    )
  )
  :
    :command (  
      .
      .
      .
      .:regexp ("((\|)su(\|)\|).* authentication failure; logname=([a-zA-Z0-9]*)\| user=([a-zA-Z0-9]*)")
    )
  )
).
.
.
.
```

In the above example, the regular expressions in the different commands try matching more specific logs. At most, one command in the group_try block will be successful and once it is found, there will be no need to check the others.
Note - Note that when adding a new device, the first try command in the parsing file must be from try until success mode as follows:

```
:cmd_name (group_try)
:mode (try_until_success)
:
    ....
)
```

Switch

This command enables the ability to compare the result of a specific field against a list of predefined constant values.

**Table 7-8 Switch Command Parameters**

<table>
<thead>
<tr>
<th>field_name</th>
<th>The field name whose value is being checked.</th>
</tr>
</thead>
<tbody>
<tr>
<td>case</td>
<td>One or more case attributes followed by the value with which to compare.</td>
</tr>
<tr>
<td>default</td>
<td>Execute only if no relevant case is available. The default value is optional.</td>
</tr>
</tbody>
</table>

**Table 7-9 Switch Command Sample**

```
:command (  
    :cmd_name (switch)  
    :field_name (msgID)  
    :  
        :case (302005)  
        :command ()  
    )  
    :  
        :case (302001)  
        :case (302002)  
        :command ()  
    )  
    :default (  
        :command()  
    )  
)
```

Unconditional _try

This command is an "empty" command that allows adding fields to the result without any conditions.
Table 7-10 Unconditional _try Command Sample 1

```plaintext
:command (
    :cmd_name (unconditional_try)
    :add_field (    
        :type (const)
        :field_name (product)
        :field_type (string)
        :field_value ("Antivirus")
    )
)
```

A common usage of unconditional_try is with the switch command. In the following example, each message ID is attached with its corresponding "message" field (denoting its meaning).

Table 7-11 Unconditional _try Command Sample 2

```plaintext
:command (    
    :cmd_name (switch)
    :field_name (msgID)
)
:case (106017)
:command (    
    :cmd_name (unconditional_try)
    :add_field (        
        :type (const)
        :field_name (message)
        :field_type (string_id)
        :field_value ("LAND Attack")
    )
)
:case (106020)
:command (    
    :cmd_name (unconditional_try)
    :add_field (        
        :type (const)
        :field_name (message)
        :field_type (string_id)
        :field_value ("Teardrop Attack")
    )
)
```

Include

This command enables the inclusion of a new parsing file.

<table>
<thead>
<tr>
<th>file_name</th>
<th>The full path plus the file name of the file to be included.</th>
</tr>
</thead>
</table>

Table 7-12 Include Command Sample

```plaintext
:command (    
    :cmd_name (include)
    :file_name ("c:\freeTextParser\device\antivirusPolicy.C")
)
```
Adding a Field

add_field

Each add_field has several arguments:

- **Type** - The type of the add_field command. This argument has two possible values:
  - **Index** - Part of the regular expression will be extracted as the field. The field_index value denotes which part will be extracted (see field_index bullet).
  - **Const** - adding a constant field whose value doesn't depend on information extracted from the regular expression (see field_value bullet).

**Field name** - the name of the new field. There are a number of common fields, which have corresponding columns in SmartView Tracker. Following is a table with the field names that need to be given in order for these fields to appear in their column in SmartView Tracker (and not in the Information field, where other added fields will appear):

<table>
<thead>
<tr>
<th>Field Name to be Given</th>
<th>Column in SmartView Tracker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src</td>
<td>Source</td>
</tr>
<tr>
<td>Dst</td>
<td>Destination</td>
</tr>
<tr>
<td>proto</td>
<td>Protocol</td>
</tr>
<tr>
<td>s_port</td>
<td>Source Port</td>
</tr>
<tr>
<td>product</td>
<td>Product</td>
</tr>
<tr>
<td>service</td>
<td>Service (when resolved includes the port and protocol.)</td>
</tr>
<tr>
<td>Action</td>
<td>Action</td>
</tr>
<tr>
<td>iface</td>
<td>Interface</td>
</tr>
<tr>
<td>User</td>
<td>User</td>
</tr>
</tbody>
</table>

Naming the above fields accordingly places them in their correct column in SmartView Tracker and thus enables them to participate in any filtering done on these columns. These fields will automatically take part in existing event definitions with these field names.

**Field_type** - the type of the field in the log. Following is a table with the possible field types:

<table>
<thead>
<tr>
<th>Field Type</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>int</td>
<td></td>
</tr>
<tr>
<td>uint</td>
<td></td>
</tr>
<tr>
<td>string</td>
<td></td>
</tr>
<tr>
<td>ipaddr</td>
<td>For IP addresses used with the Src and Dst fields.</td>
</tr>
<tr>
<td>pri</td>
<td>Includes the facility and severity of a syslog.</td>
</tr>
<tr>
<td>timestamp</td>
<td>Includes the date and time of the syslog. Supports the format 'Oct 10 2004 15:05:00'.</td>
</tr>
<tr>
<td>time</td>
<td>Supports the format '15:05:00'.</td>
</tr>
<tr>
<td>string_id</td>
<td>For a more efficient usage of strings. Used when there is a finite number of possible values for this field.</td>
</tr>
</tbody>
</table>
### Field Name | Field Type
--- | ---
Src | ipaddr
Dst | ipaddr
proto | protocol
s_port | port
service | port
Action | action
ifname | ifname

- **field_index** or **field_value** - The argument used depends on the value of the "type" field. If it is "index", "field_index" appears and if it is "const", "field_value" appears.
- **field_index** - denotes which part of the regular expression will be extracted, according to the grouping of the patterns (the grouping is done by writing a certain expression in brackets so basically the number in "field_index" denotes the bracket number whose pattern will be taken into account).
Table 7-13 Add_field Command Sample

```plaintext
:command (  
  :cmd_name (try)  
  :parse_from (last_position)  
  :add_field (  
    :type (index)  
    :field_name (User)  
    :field_type (string)  
    :field_index (1)  
  )  
  :add_field (  
    :type (index)  
    :field_name (Src)  
    :field_type (ipaddr)  
    :field_index (2)  
  )  
  :add_field (  
    :type (index)  
    :field_name (port)  
    :field_type (port)  
    :field_index (3)  
  )  
)```

The pattern for the User, [a-zA-Z0-9]+, is located in the first pair of brackets (and therefore the field_index is 1), the pattern for the Source address, [0-9]+\.[0-9]+\.[0-9]+\.[0-9]+, is located in the second pair of brackets (hence the index 2) and the pattern for the port is in the third pair of brackets.

In each parsed regular expression the maximum number of brackets is limited to 9. If you wish to extract more that 9 elements from the regular expression, "break" the expression into 2 pieces. The first regular expression will contain the first 9 brackets and the rest of the regular expression will be in the on_success command.
:command {
  :cmd_name (try)
  :parse_from (start_position)
    :add_field (  
      :type (index)  
      :field_name (listID)  
      :field_type (string)  
      :field_index (1)  
    )
    :add_field (  
      :type (index)  
      :field_name (action)  
      :field_type (action)  
      :field_index (2)  
    )
    :add_field (  
      :type (index)  
      :field_name (proto)  
      :field_type (protocol)  
      :field_index (3)  
    )
    :add_field (  
      :type (index)  
      :field_name (ifname)  
      :field_type (ifname)  
      :field_index (4)  
    )
    :add_field (  
      :type (index)  
      :field_name (Src)  
      :field_type (ipaddr)  
      :field_index (5)  
    )
    :on_success (  
      :command (  
        :cmd_name (try)  
        :parse_from (last_position)
        :add_field (  
          :type (index)  
          :field_name (destination_interface)
          :field_type (string)  
          :field_index (1)  
        )
      )
    )
  )
}

- **field_value** is the constant value to be added.
Dict_name is the name of the dictionary to use to convert the value (if the value is not found in the dictionary the real value will be the result). See Dictionary (on page 78).

**Dictionary**

The free text parser enables us to use dictionaries to convert values from the log. These conversions are used in order to “translate” values from logs from different devices, with the same meaning, into a common value, which is used in the events’ definitions.

Each dictionary file is defined as a .ini file, in which the section name is the dictionary name and the values are the dictionary values (each dictionary can include one or more sections).

<table>
<thead>
<tr>
<th>dictionary_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name1 = val1</td>
</tr>
<tr>
<td>Name2 = val2</td>
</tr>
</tbody>
</table>

[cisco_action]

permitted = accept  Permit = accept

denied = reject     Deny = reject

**Dictionary Sample**

The reference to a dictionary in the parsing file is shown in the following table:

**Dictionary Command Sample 2**

:command (  
   :cmd_name (try)  
   :parse_from (start_position)  
   :regexp ("list (.*) (permitted|denied) (icmp) 
   :add_field (  
      :type (index)  
      :field_name (action)  
      :field_type (action)  
      :field_index (2)  
      :dict_name (cisco_action)  
   )
   )

):command (  
   :cmd_name (try)  
   :parse_from (last_position)  
   :regexp ("%PIX-([0-9])-( [0-9]*)")  
   :add_field (  
      :type (const)  
      :field_name (product)  
      :field_type (string_id)  
      :field_value ("CISCO PIX")  
   )
   )

)
Administrator Support for WinEventToCPLog

WinEventToCPLog uses Microsoft APIs to read events from Windows operating system event files. These files can be viewed using the Windows Event Viewer.

WinEventToCPLog can read all event files on the local machine and it can read log files from remote machines with the right privileges. This is useful for making a central WinEventToCPLog server that forwards multiple Windows hosts events to a Check Point Log server.

The privileges are set by invoking WinEventToCPLog -s to specify an administrator login and password. There are two ways to access the files on a remote machine. The first is to define a local administrator on the remote machine whose name matches the name registered with WinEventToCPLog. The second way is to define the administrator registered with WinEventToCPLog as an administrator in the domain and then this administrator can access all the machines in the domain.