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=22930
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the R76 home page (http://supportcontent.checkpoint.com/solutions?id=sk91140).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 February 2013</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on SmartView Tracker R76 Administration Guide).
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>SmartView Tracker Overview</td>
<td>6</td>
</tr>
<tr>
<td>Tracking Network Traffic</td>
<td>7</td>
</tr>
<tr>
<td>Log Suppression</td>
<td>7</td>
</tr>
<tr>
<td>SmartView Tracker GUI</td>
<td>7</td>
</tr>
<tr>
<td>SmartView Tracker Toolbar</td>
<td>8</td>
</tr>
<tr>
<td>SmartView Tracker Query Toolbar</td>
<td>9</td>
</tr>
<tr>
<td>SmartView Tracker Actions</td>
<td>10</td>
</tr>
<tr>
<td>DLP Actions</td>
<td>11</td>
</tr>
<tr>
<td>DLP General Columns</td>
<td>11</td>
</tr>
<tr>
<td>DLP Restricted Columns</td>
<td>12</td>
</tr>
<tr>
<td>Identity Awareness Columns</td>
<td>12</td>
</tr>
<tr>
<td>IPS Columns</td>
<td>12</td>
</tr>
<tr>
<td>IPS-1 Columns</td>
<td>13</td>
</tr>
<tr>
<td>SmartView Tracker Modes</td>
<td>14</td>
</tr>
<tr>
<td>Using SmartView Tracker</td>
<td>15</td>
</tr>
<tr>
<td>Viewing Log Files</td>
<td>15</td>
</tr>
<tr>
<td>Filters</td>
<td>15</td>
</tr>
<tr>
<td>Queries</td>
<td>15</td>
</tr>
<tr>
<td>Matching Rules</td>
<td>16</td>
</tr>
<tr>
<td>Maintaining Log Files with Log Switch</td>
<td>17</td>
</tr>
<tr>
<td>Managing Disk Space with Cyclic Logging</td>
<td>17</td>
</tr>
<tr>
<td>Exporting Logs</td>
<td>17</td>
</tr>
<tr>
<td>Saving Logs on Security Gateways</td>
<td>17</td>
</tr>
<tr>
<td>Logging Behavior during Downtime</td>
<td>17</td>
</tr>
<tr>
<td>Logging Using Log Servers</td>
<td>17</td>
</tr>
<tr>
<td>Setting Up Security Management Server for Log Server</td>
<td>18</td>
</tr>
<tr>
<td>Maintaining a Secure Network</td>
<td>18</td>
</tr>
<tr>
<td>Using Check Point Advisories</td>
<td>18</td>
</tr>
<tr>
<td>Blocking Intruders</td>
<td>18</td>
</tr>
<tr>
<td>Running Custom Commands</td>
<td>18</td>
</tr>
<tr>
<td>Viewing Packet Capture</td>
<td>19</td>
</tr>
<tr>
<td>Configuring SmartView Tracker</td>
<td>20</td>
</tr>
<tr>
<td>Overview</td>
<td>20</td>
</tr>
<tr>
<td>Choosing which Rules to Track</td>
<td>20</td>
</tr>
<tr>
<td>Choosing the Appropriate Tracking Option</td>
<td>20</td>
</tr>
<tr>
<td>Forwarding Online or Forwarding on Schedule</td>
<td>21</td>
</tr>
<tr>
<td>Modifying the Log Forwarding Process</td>
<td>21</td>
</tr>
<tr>
<td>Basic Tracking Configuration</td>
<td>21</td>
</tr>
<tr>
<td>Configuring SmartView Tracker Views</td>
<td>21</td>
</tr>
<tr>
<td>Query Pane</td>
<td>21</td>
</tr>
<tr>
<td>Resolving IP Addresses</td>
<td>22</td>
</tr>
<tr>
<td>Resolving Services</td>
<td>22</td>
</tr>
<tr>
<td>Showing Null Matches</td>
<td>22</td>
</tr>
<tr>
<td>Configuring a Filter</td>
<td>23</td>
</tr>
<tr>
<td>Configuring the Current Rule Number Filter</td>
<td>23</td>
</tr>
<tr>
<td>Using Follow Commands</td>
<td>23</td>
</tr>
<tr>
<td>Viewing the Logs of a Rule from the Rule Base</td>
<td>23</td>
</tr>
<tr>
<td>Configuring Queries</td>
<td>24</td>
</tr>
<tr>
<td>Opening an Existing Query</td>
<td>24</td>
</tr>
<tr>
<td>Creating a Customized Entry</td>
<td>24</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

In This Chapter

- SmartView Tracker Overview
- Tracking Network Traffic
- Log Suppression
- SmartView Tracker GUI

SmartView Tracker Overview

You need different levels of tracking, depending on the data's importance. For example, while you may choose to track standard network patterns (e.g., your users' surfing patterns), this information is not urgent and you can inspect it at your convenience. If your network is being attacked, you must be alerted immediately.

Check Point products provide you with the ability to collect comprehensive information on your network activity in the form of logs. You can then audit these logs at any given time, analyze your traffic patterns and troubleshoot networking and security issues. The figure below illustrates the log collection and tracking process:

The SmartDashboard allows you to customize your tracking settings for each Rule Base, by specifying per-rule whether or not to track the events that match it.

If you decide to track the events that match a certain rule, you can choose from a variety of tracking options, based on the information's urgency. For example, you can choose a standard Log for allowed http connections; opt for an Account log when you wish to save byte data; or issue an Alert (in addition to the log) when a connection's destination is your gateway. For a list of the available tracking options, right-click the relevant rule's Track column.

The gateways on which this Policy is installed collect data as specified in the Policy, and forward the logs to the Security Management server (and/or to Log Servers, depending on their settings). The logs are organized in files according to the order in which they arrived to the Security Management server. All new logs are saved to the fw.log file, except for audit (management-related) logs, which are saved to the fw.adtlog file.

The Security Management server makes these logs available for inspection via SmartView Tracker - a comprehensive auditing solution, enabling central management of both active and old logs of all Check Point products. You can conveniently customize searches to address your specific tracking needs; integrate the logs with the Check Point SmartReporter; or export them to text files or to an external Oracle database.
The Security Management server also performs the operations specified in the Policy for events matching certain rules (e.g., issuing an alert, sending email, running a user-defined script etc.).

In addition to the above solutions, you can benefit from the tracking and auditing capabilities of the following Check Point SmartConsole:

- SmartView Monitor allows you to manage, view and test the status of various Check Point components throughout the system, as well as to generate reports on traffic on interfaces, specific Check Point products, and other Check Point system counters.
- SmartReporter allows you to save consolidated records (as opposed to "raw" logs) and conveniently focus on events of interest.

### Tracking Network Traffic

The SmartView Tracker can be used to track all daily network traffic and activity logged by any Check Point and OPSEC Partners log-generating product. It can also be used to give an indication of certain problems. Network administrators can use the log information for:

- Detecting and monitoring security-related events. For example, alerts, repeated rejected connections or failed authentication attempts, might point to possible intrusion attempts.
- Collection information about problematic issues. For example, a client has been authorized to establish a connection but the attempts to connect have failed. The SmartView Tracker might indicate that the Rule Base has been erroneously defined to block the client's connection attempts.
- Statistical purposes such as analyzing network traffic patterns. For example, how many HTTP services were used during peak activity as opposed to Telnet services.

### Log Suppression

The SmartView Tracker is designed to efficiently present the logs that are generated from Check Point products. To avoid displaying log entries for a frequently repeating event, SmartView Tracker displays the first instance of the event and then counts subsequent instances which occur in the next two minutes. For as long as the event continues to occur, every two minutes SmartView Tracker shows a Log Suppression Report which contains the details of the event as well as the number of times the event occurred.

### SmartView Tracker GUI

In the main window of SmartView Tracker, an entry in the Records pane is a record of an event that was logged according to a specific rule in the Rule Base. New records that are added to the fw.log file are automatically added to the Records pane as well.

To understand the figure, refer to the numbers in the figure and the following list.

1. The **Network & Endpoint, Active and Management** modes display different types of logs.
2. The **Query Tree** pane displays the Predefined and Custom queries.
3. The **Query Properties** pane displays the properties of the fields in the Records pane.
4. The **Records** pane displays the fields of each record in the log file.
The log fields displayed are a function of the following factors:

- The software blade that generated the log, such as Firewall, VPN or IPS.
- The type of operation performed, such as installation or opening a connection.

For example, when NAT is used, the address translation fields (with the ‘Xlate’ prefix, e.g., XlateSrc, XlateDst etc.) are displayed. When Firewall is used, IKE-related fields (e.g., IKE CookieL, IKE CookieR etc.) are displayed.

### SmartView Tracker Toolbar

<table>
<thead>
<tr>
<th>Icon</th>
<th>Menu Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📈</td>
<td>File &gt; Open</td>
<td>Open an existing Log File.</td>
</tr>
<tr>
<td>📂</td>
<td>File &gt; Save As</td>
<td>Save the Log File under a new name in a new location.</td>
</tr>
<tr>
<td>🔄</td>
<td>File &gt; Switch Active File</td>
<td>Open a new active Log File.</td>
</tr>
<tr>
<td>🛠️</td>
<td>Tools &gt; Remote Files Management</td>
<td>Remote log files management</td>
</tr>
<tr>
<td>⌚️</td>
<td>View &gt; Files Fetch Progress</td>
<td>Hide or show the Files Fetch Progress Window.</td>
</tr>
<tr>
<td>📜</td>
<td>View &gt; Query Tree</td>
<td>Hide or show the Query Tree on the left side of the window.</td>
</tr>
</tbody>
</table>
### Query Toolbar

**Icon** | **Menu Command** | **Description**
--- | --- | ---
| | **Query > Hide Identities** | Hide or show user identities. Only users with relevant permissions can view identities. |
| | Select a query > **Query > Open** | Open an existing Query. |
| | **Query > Save Query** | Save the modifications you made to the custom Query. |
| | **Query > Save Query As** | Save the Query under a new name in the **Custom** folder. |
| | F1 | Online Help |

**SmartView Tracker Query Toolbar**

**Note** - Some of the toolbar buttons are shortcuts for menu commands. Some toolbar buttons do not have corresponding menu commands.

The following table describes the toolbar buttons for the **Query Properties** pane.

<table>
<thead>
<tr>
<th>Icon</th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Show or hide query properties.</td>
</tr>
<tr>
<td></td>
<td>Apply all filtering criteria.</td>
</tr>
<tr>
<td></td>
<td>Display the name of the host and the domain.</td>
</tr>
<tr>
<td></td>
<td>Display the type of service the port uses.</td>
</tr>
<tr>
<td></td>
<td>Show all null matches.</td>
</tr>
<tr>
<td></td>
<td>The Autoscroll button enables you to update the Log File to display all new log entries and place them at the end of the Log File.</td>
</tr>
<tr>
<td></td>
<td>Delete all filtering criteria in the Log File.</td>
</tr>
<tr>
<td></td>
<td>Find the specified text string in all fields.</td>
</tr>
<tr>
<td></td>
<td>Go to the top of the Log File.</td>
</tr>
<tr>
<td></td>
<td>Go to the bottom of the Log File.</td>
</tr>
<tr>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td><img src="image1.png" alt="Icon" /></td>
<td>Shows the total number of filtered records.</td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon" /></td>
<td>The Abort button enables you to stop loading Log data from the server or abort any action which is in progress or on queue to begin.</td>
</tr>
</tbody>
</table>

### SmartView Tracker Actions

The following table gives a description of the different types of actions recorded by SmartView Tracker.

<table>
<thead>
<tr>
<th>Action Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept</td>
<td>The connection was allowed to proceed.</td>
</tr>
<tr>
<td>Reject</td>
<td>The connection was blocked.</td>
</tr>
<tr>
<td>Drop</td>
<td>The connection was dropped without notifying the source.</td>
</tr>
<tr>
<td>Detect</td>
<td>The connection was monitored without enforcing IPS protections.</td>
</tr>
<tr>
<td>Encrypt</td>
<td>The connection was encrypted.</td>
</tr>
<tr>
<td>Authcrypt</td>
<td>SecuRemote user logon.</td>
</tr>
<tr>
<td>Bypass</td>
<td>The connection passed transparently through InterSpect.</td>
</tr>
<tr>
<td>Flag</td>
<td>Flags the connection.</td>
</tr>
<tr>
<td>Login</td>
<td>A user logged into the system.</td>
</tr>
<tr>
<td>Reject</td>
<td>The connection was rejected.</td>
</tr>
<tr>
<td>VPN routing</td>
<td>The connection was routed through the gateway acting as a central hub.</td>
</tr>
<tr>
<td>Decrypt</td>
<td>The connection was decrypted.</td>
</tr>
<tr>
<td>Key Install</td>
<td>Encryption keys were created.</td>
</tr>
<tr>
<td>Authorize</td>
<td>Client Authentication logon.</td>
</tr>
<tr>
<td>Deauthorize</td>
<td>Client Authentication logoff.</td>
</tr>
<tr>
<td>Block</td>
<td>Connection blocked by Interspect.</td>
</tr>
<tr>
<td>Detect</td>
<td>Connection was detected by Interspect.</td>
</tr>
<tr>
<td>Inspect</td>
<td>Connection was subject to InterSpect configured protections.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>The IP source address of the connection was quarantined by InterSpect.</td>
</tr>
<tr>
<td>Replace Malicious code</td>
<td>Malicious code in the connection was replaced.</td>
</tr>
</tbody>
</table>
**DLP Actions**

Specific actions for DLP incidents include:

<table>
<thead>
<tr>
<th>DLP Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ask User</td>
<td>DLP incident captured and put in Quarantine, user asked to decide what to do.</td>
</tr>
<tr>
<td>Do not Send</td>
<td>User decided to drop transmission that was captured by DLP.</td>
</tr>
<tr>
<td>Send</td>
<td>User decided to continue transmission after DLP notified that it may contain sensitive data.</td>
</tr>
<tr>
<td>Quarantine Expired</td>
<td>DLP captured data transmission cannot be sent because the user did not make a decision in time. Expired incidents may still be viewed, until they are deleted (routine cleanup process).</td>
</tr>
<tr>
<td>Prevent</td>
<td>DLP transmission was blocked.</td>
</tr>
<tr>
<td>Allow</td>
<td>DLP transmission was allowed; usually by exception to rule.</td>
</tr>
<tr>
<td>Inform User</td>
<td>DLP transmission was detected and allowed, and user notified.</td>
</tr>
<tr>
<td>Deleted Due To Quota</td>
<td>DLP incidents are deleted from gateway for disk space.</td>
</tr>
</tbody>
</table>

**DLP General Columns**

DLP incidents may show any of these columns and are available to all administrators.

<table>
<thead>
<tr>
<th>DLP Columns</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident UID</td>
<td>Unique ID of the incident.</td>
</tr>
<tr>
<td>DLP Action Reason</td>
<td>Reason for the action. Possible values: Rulebase, Internal Error, Prior User Decision</td>
</tr>
<tr>
<td>Related Incident</td>
<td>Internal incident ID related to the current log.</td>
</tr>
<tr>
<td>DLP Transport</td>
<td>Protocol of the traffic of the incident: HTTP, FTP, SMTP.</td>
</tr>
</tbody>
</table>

**Using the Incident UID as a key between multiple logs:**

Each DLP incident has a unique ID included in the log and sent to the user as part of an email notification. User actions (Send, Do not Send) are assigned the same Incident UID that was assigned to the original DLP incident log.

If a user sends an email with a DLP violation and then decides to discard it, two logs are generated. The first log is a DLP incident log with **Ask User** action and is assigned an Incident UID. On the user action, the second log is generated with the same UID, with the **Do not Send** action.

Each matched data type generates its own log. The gateway makes sure that all the data type logs of one incident indicate the same unique Incident UID and rule action (Prevent, Ask, Inform, or Detect), even if data types were matched on different rules. The common action for an incident is the most restrictive.

For example, assume a transmission matches two data types. Each data type is used in a different rule. The action of one rule is Prevent. The action of another rule is Detect. The two logs that are generated will indicate Prevent as the action. (The action implemented will be Prevent.) The log of the Detect rule will show **Rule Base (Action set by different rule)** in the DLP Action Reason column.
**DLP Restricted Columns**

These columns are restricted to administrators with permissions.

<table>
<thead>
<tr>
<th>Restricted Filters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP Rule Name</td>
<td>Name of the DLP rule on which the incident was matched.</td>
</tr>
<tr>
<td>DLP Rule UID</td>
<td>Internal rule ID of the DLP rule on which the incident was matched.</td>
</tr>
<tr>
<td>Data Type UID</td>
<td>Internal ID of the data type on which the incident was matched.</td>
</tr>
<tr>
<td>Data Type Name</td>
<td>Name of the matched data type.</td>
</tr>
<tr>
<td>User Action Comment</td>
<td>Comment given by user when releasing the incident from the Portal.</td>
</tr>
<tr>
<td>DLP Recipients</td>
<td>For SMTP traffic, list of recipients of captured email.</td>
</tr>
<tr>
<td>Scanned Data Fragment</td>
<td>Captured data itself: email and attachment of SMTP, file of FTP, or HTTP traffic.</td>
</tr>
<tr>
<td>Message to User</td>
<td>Message sent, as configured by administrator, for the rule on which the incident was matched.</td>
</tr>
<tr>
<td>DLP Categories</td>
<td>Category of data type on which the incident was matched.</td>
</tr>
<tr>
<td>DLP Words List</td>
<td>If the data type on which the incident was matched included a word list (keywords, dictionary, and so on), the list of matched words.</td>
</tr>
<tr>
<td>Mail Subject</td>
<td>For SMTP traffic, the subject of captured email.</td>
</tr>
</tbody>
</table>

**Identity Awareness Columns**

Incidents for Identity Awareness show information about the AD name and IP address associations.

<table>
<thead>
<tr>
<th>Identity Awareness Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination Machine Name</td>
<td>Resolved AD name of a machine associated with destination IP of a logged traffic.</td>
</tr>
<tr>
<td>Destination User Name</td>
<td>Resolved AD name of a user associated with destination IP of a logged traffic.</td>
</tr>
<tr>
<td>Source Machine Name</td>
<td>Resolved AD name of a machine associated with source IP of a logged traffic.</td>
</tr>
<tr>
<td>Source User Name</td>
<td>Resolved AD name of a user associated with source IP of a logged traffic.</td>
</tr>
</tbody>
</table>

**IPS Columns**

The **Protection Type** column is relevant to IPS protection incidents. You can filter for any of these types:

- Application Control
- Engine Settings
- Geo Protection
- Protocol Anomaly
- Signature

Other columns specific to the IPS Software Blade:
- Protected Server
- Source Reputation
- Destination Reputation
- Client Type
- Server Type

**IPS-1 Columns**

These columns are relevant for IPS-1 appliances.

<table>
<thead>
<tr>
<th>IPS-1 Product Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPC Service Number</td>
<td>Protocol detail.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Internal ID of the VLAN.</td>
</tr>
<tr>
<td>MAC Destination Address MAC</td>
<td>MAC address associated with destination or source machine.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Used in protocol context and is name or identifier of the command used in the traffic of the attack.</td>
</tr>
<tr>
<td>Command</td>
<td>Name of the host associated with source or destination of the logged traffic according to the relevant resolving service. Not all those fields are filled in the same time.</td>
</tr>
<tr>
<td>Destination DHCP Hostname</td>
<td></td>
</tr>
<tr>
<td>Destination DNS Hostname</td>
<td></td>
</tr>
<tr>
<td>NetBIOS Destination</td>
<td></td>
</tr>
<tr>
<td>Hostname</td>
<td></td>
</tr>
<tr>
<td>NetBIOS Source Hostname</td>
<td></td>
</tr>
<tr>
<td>Source DHCP Hostname</td>
<td></td>
</tr>
<tr>
<td>Source DNS Hostname</td>
<td></td>
</tr>
<tr>
<td>Source OS</td>
<td>OS type of source or destination machine.</td>
</tr>
<tr>
<td>Destination OS</td>
<td></td>
</tr>
<tr>
<td>Email Address</td>
<td>Email address fetched from attack traffic.</td>
</tr>
<tr>
<td>Email Subject</td>
<td>Subject of the email caught in attack traffic.</td>
</tr>
<tr>
<td>Hostname</td>
<td>If in attack traffic we find host name that is unrelated to the either source or destination, it is given here.</td>
</tr>
<tr>
<td>HTTP Referer</td>
<td>HTTP protocol elements.</td>
</tr>
<tr>
<td>HTTP Modifier</td>
<td></td>
</tr>
<tr>
<td>Cookie</td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td></td>
</tr>
<tr>
<td>Payload</td>
<td></td>
</tr>
<tr>
<td>Attack Assessment</td>
<td>Possible values: Failed, Successful, Unknown.</td>
</tr>
<tr>
<td>Sensor Mode</td>
<td>Possible values: Invalid, Passive, Inline - Fail-open, Inline - Fail-closed, Inline - Monitor only.</td>
</tr>
<tr>
<td>Activated Quarantine</td>
<td>Whether attack caused quarantine.</td>
</tr>
</tbody>
</table>
**SmartView Tracker Modes**

SmartView Tracker consists of three different modes:

- **Log**, the default mode, displays all logs in the current `fw.log` file. These include entries for security-related events logged by different Check Point software blades, as well as Check Point's OPSEC partners. New logs that are added to the `fw.log` file are added to the bottom of the Records pane.

- **Active** allows you to focus on connections that are currently open through the Security Gateways that are logging to the active Log file.

- **Audit** allows you to focus on management-related records, such as records of changes made to objects in the Rule Base and general SmartDashboard usage. This mode displays audit-specific data, such as the record's Administrator, Application or Operation details, which is read from the `fw.adtlog` file.

You can toggle between modes by clicking the desired tab.
Chapter 2

Using SmartView Tracker

In This Chapter

Viewing Log Files 15
Maintaining Log Files with Log Switch 17
Managing Disk Space with Cyclic Logging 17
Exporting Logs 17
Saving Logs on Security Gateways 17
Maintaining a Secure Network 18
Running Custom Commands 18
Viewing Packet Capture 19

Viewing Log Files

Filters

SmartView Tracker’s filtering mechanism allows you to conveniently focus on log data of interest and hide other data, by defining the appropriate criteria per-log field. Once you have applied the filtering criteria, only entries matching the selected criteria are displayed.

The filtering options available are a function of the log field in question. For example, while the Date field is filtered to show data that is after, before or in the range of the specified date, the Source, Destination and Origin fields are filtered to match (or differ from) the specified machines.

It is very useful to filter the Product field and focus on a specific Check Point product. SmartView Tracker features these filters as predefined queries.

Queries

SmartView Tracker gives you control over the Log file information displayed. You can either display all records in the Log file, or filter the display to focus on a limited set of records matching one or more conditions you are interested in. This filtering is achieved by running a query.

A query consists of the following components:

- Condition(s) applied to one or more log fields (record columns) — for example, to investigate all HTTP requests arriving from a specific source, you can run a query specifying HTTP as the Service column’s filter and the machine in question as the Source column’s filter.
- A selection of the columns you wish to show — for example, when investigating HTTP requests it is relevant to show the URL log field.

Each of the SmartDashboard modes (Log, Active and Audit) has its own Query Tree, with these folders:

- Predefined: contains the default queries that cannot be directly modified or saved.
  The predefined queries available depend on the mode you are in. The default query of all three modes is All Records. In addition, the Log mode includes predefined per product or feature.
- Custom: allows you to customize your own Query based on a predefined one, to better address your needs. Customized queries are the main querying tool, allowing you to pinpoint the data you are interested in. An existing query that is copied or saved under a new name is automatically added to the Custom folder.

The attributes of the selected query are displayed in the Query Properties pane.
Matching Rules

SmartView Tracker records the Firewall Rule Base rule to which a connection was matched. The matching rule is recorded in four columns in SmartView Tracker, as depicted in the figure below:

- The Rule column, which records the number of the rule in the Rule Base at the time the log entry was recorded. Like other properties in SmartView Tracker, logs can be sorted and queried by rule number.

- The Current Rule Number column, which is a dynamic field that reflects the current placement of the rule in the Rule Base and displays the current policy package name. As the Rule Base is typically subject to change, this column makes it possible to locate the rules that have changed their relative positions in the Rule Base since the log was recorded, and to create filters for log entries that match the rule, not just the rule number. By way of example, note the log entry in the figure. When this log was first recorded, it recorded the matching rule as Rule 1. Since then the rule's position in the Rule Base has changed, and so the Current Rule Number column reports its present position as 2 [Standard], where [Standard] is the name of the policy package in which this rule resides.

- The Rule Name column, which records the short textual description of the rule in the Name column of the Rule Base, when in use.

- The Rule UID column, which records the unique identifying number (UID) that is generated for each rule at the time that it is created. This number serves an internal tracking function, and as such the column is hidden by default. To display this column, click on View > Query Properties and enable the Rule UID property.

Filtering Log Entries by Matching Rule

In order to filter log entries based on a matching rule, right-click on a log entry and choose either Follow Rule or Follow Rule Number.

- Follow Rule generates a filtered view of all logs that matched this rule, and is based on the UID number of the rule.

- Follow Rule Number generates a filtered view of all log files that match the number recorded in the Rule column of the selected log.

These two operations are essentially short-cuts to creating a filter. You can achieve the same results by right-clicking anywhere in a given column and selecting Edit Filter, and then entering the filtering criteria you want to apply.

The Rule and Current Rule Number filters, which provide the same functionality as the Follow Rule and Follow Rule Number commands, can also create filtered views based on multiple matching rules. The figure below shows the Current Rule Number Filter.

Viewing the Matching Rule in Context

From SmartView Tracker, you can launch SmartDashboard to examine the rule within the context of the Firewall Rule Base. By right-clicking on the relevant log and selecting View rule in SmartDashboard, SmartDashboard will open with the rule highlighted in white.

If you are using version control, SmartDashboard opens with the revision that was saved when this record was created. If no revision is available, SmartDashboard uses the unique identifying number to display the relevant rule. If neither version control nor a UID number are available, the View rule in SmartDashboard option is not available.

Viewing the Logs of a Rule from SmartDashboard

From the firewall Rule Base in SmartDashboard, there are two methods by which you can launch SmartView Tracker to view all of the log entries that matched on a particular rule. By right-clicking on the rule, you can choose to either:

- View rule logs in SmartView Tracker, which opens SmartView Tracker to a filtered view of all logs that matched on the rule.

- Copy Rule ID, which copies the unique identifying number of the rule to the clipboard, allowing the user to paste the value into the Rule UID Filter in SmartView Tracker.
Maintaining Log Files with Log Switch

The active Log file’s size is kept below the 2 GB default limit by closing the current file when it approaches this limit and starting a new file. This operation, known as a log switch, is performed either automatically, when the Log file reaches the specified size or according to a log switch schedule; or manually, from SmartView Tracker.

The file that is closed is written to the disk and named according to the current date and time. The new Log file automatically receives the default Log file name ($FWDIR/log/fw.log for log mode and $FWDIR/log/fw.adtlog for audit mode).

Managing Disk Space with Cyclic Logging

When there is a lack of sufficient free disk space, the system stops generating logs. To ensure the logging process continues even when there is not enough disk space, you can set a process known as Cyclic Logging. This process automatically starts deleting old log files when the specified free disk space limit is reached, so that the Security Gateway can continue logging new information. The Cyclic Logging process is controlled by:

- Modifying the amount of required free disk space.
- Setting the Security Gateway to refrain from deleting logs from a specific number of days back.

Exporting Logs

While SmartView Tracker is the standard log tracking solution, you may also wish to use your logs in other ways that are specific to your organization. For that purpose, Check Point products provide you with the option to export log files to the appropriate destination.

A log file can be exported in two different ways:

- As a simple text file
- In a database format, exported to an external Oracle database

SmartView Tracker supports a basic export operation, in which the display is copied as-is into a text file. More advanced export operations (for example, exporting the whole log file or exporting logs online) are performed using the command line (using the fwm logexport, log_export and fw log commands).

With the Export option (File > Export) you can create a comma delimited ASCII file that can be used as input for other applications.

Saving Logs on Security Gateways

By default, Security Gateways forward their log records online to the Security Management server. Alternatively, to improve the gateway's performance, you can free it from constantly sending logs by saving the information to local log files. These files can either be automatically forwarded to the Security Management server or Log Server, according to a specified schedule; or manually imported through SmartView Tracker, using the Remote File Management operation.

Logging Behavior during Downtime

During downtime, when the gateway cannot forward its logs, they are written to a local file. To view these local files, you must manually import them using the Remote File Management operation.

Logging Using Log Servers

To reduce the load on the Security Management server, administrators can install Log Servers and then configure the gateways to forward their logs to these Log Servers. In this case, the logs are viewed by logging with SmartView Tracker into the Log Server machine (instead of the Security Management server machine).
A Log Server behaves just like a Security Management server for all log management purposes: it executes the operation specified in the Policy for events matching certain rules (e.g., issuing an alert or an email); performs an Automatic Log Switch when `fw.log` reaches 2GB, allows you to export files, etc.

**Setting Up Security Management Server for Log Server**

Logs are not automatically forwarded to new log servers. You must manually setup each relevant gateway to send its logs to the new log server. The same plug-ins should be installed on all Security Management servers and log servers involved in order for the install policy procedure to be successful.

To instruct a Security Management server to send logs to a Log server:
1. In SmartDashboard, double-click the gateway object to display its Check Point Gateway window.
2. Select **Logs and Masters > Additional Logging.** Select **Forward log files to Log Server.**
   - The Security Management server drop-down list is enabled.
3. Select the new log server from the Security Managements drop-down list and click **OK.**
4. Select **Policy > Install,** and then select the gateways and log servers on which the Policy should be installed.

**Maintaining a Secure Network**

**Using Check Point Advisories**

Check Point Advisory are detailed descriptions and step-by-step instructions on how to activate and configure relevant defenses provided by Check Point and IPS Updates.

The ability to view a Check Point Advisory in SmartView Tracker provides information about the IPS protection that is directly related to the selected IPS log. This information can help you analyze your configuration choices and better understand why the specific SmartView Tracker log appeared.

In addition, Check Point Advisory supplies all of your IPS configuration choices so that you can learn why the specific log appeared. To view Check Point Advisory for a specific IPS log, right-click the log and select **Go to Advisory.**

For more detailed information about the IPS log and associated protection, scroll down to the bottom of the Check Point Advisory window and select **Read the Full ADVISORY and SOLUTION.**

The Check Point Advisory feature will not appear for logs that do not contain an Attack Name and/or Attack Information.

**Blocking Intruders**

The **Active** mode of SmartView Tracker allows you to shut out intruders by selecting the connection you've identified as intrusive and blocking one of the following. **Block Intruder** uses SAM to perform the block action.

- The connection - block the selected connection or any other connection with the same service, source or destination.
- The source of the connection - block access to and from this source. Block all connections that are headed to or coming from the machine specified in the Source field.
- The destination of the connection - block access to and from this destination. Block all connections that are headed to or coming from the machine specified in the Destination field.
- Specify a time frame during which this connection is to be blocked.

**Running Custom Commands**

SmartView Tracker allows you to conveniently run commands from the SmartConsole, instead of working in the command line. The commands available by default are `ping` and `whois`. These commands, along with the ones you add manually, are available through the menu displayed by right-clicking a relevant cell in the **Records** pane.
Viewing Packet Capture

Certain Check Point products include the ability to capture network traffic. After this feature is activated, a packet capture file is sent with a log to the log server. The packet capture can be retrieved at a later time to allow the administrator greater insight into the exact traffic which generated the alert.

The packet capture file can be accessed from the log entry in SmartView Tracker. The file can be saved as a file to a file location, or can be opened in the internal viewer included in the SmartConsole or any packet capture viewer installed on the SmartConsole client.
Chapter 3

Configuring SmartView Tracker

In This Chapter

Overview 20
Basic Tracking Configuration 21
Configuring SmartView Tracker Views 21
Configuring a Filter 23
Configuring the Current Rule Number Filter 23
Using Follow Commands 23
Viewing the Logs of a Rule from the Rule Base 23
Configuring Queries 24
Hiding and Showing the Query Tree Pane 25
Working with the Query Properties Pane 25
Copying Log Record Data 26
Viewing a Record's Details 26
Viewing a Rule 26
Finding an Interface 27

Overview

Choosing which Rules to Track

The extent to which you can benefit from the events log depends on how well they represent the traffic patterns you are interested in. Therefore, you must ensure your Security Policy is indeed tracking all events you may later wish to study. On the other hand, you should keep in mind that tracking multiple events results in an inflated log file, which requires more disk space and management operations.

To balance these conflicting needs, and determine which of your Policy’s rules should be tracked, consider how useful this information is to you. For example, consider whether this information:

- Improves your network’s security
- Enhances your understanding of your users’ behavior
- Is the kind of data you wish to see in reports
- May be useful for future purposes

Choosing the Appropriate Tracking Option

For each rule you track, specify one of the following tracking options:

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

### Forwarding Online or Forwarding on Schedule

By default, Security Gateways forward their log records online, one by one, to the selected destination (the Security Management server or a Log Server). In this case, SmartView Tracker allows you to see new records as they are forwarded to the machine you logged into.

To improve the gateway's performance, you can free it from constantly forwarding logs by configuring a Local Logging system in which the records are saved to a local log file. If you set a log forwarding schedule, you can open this file (instead of the active file) in SmartView Tracker. Otherwise, you can manually import this file from the gateway, using the **Remote File Management** operation.

### Modifying the Log Forwarding Process

Log files can be forwarded without deleting them from the Security Management server, Security Gateway, or Log server that sends them. This is particularly useful in a Multi-Domain Security Management environment.

In a Multi-Domain Security Management environment logs are commonly saved on the customer's Log server, to which the customer connects using SmartView Tracker. However, for analysis and back-up purposes, these logs are soon forwarded to dedicated servers run by the customer's ISP, to which the customer has no access. This enhancement to the scheduled log forwarding process makes the logs available to both the customer and customer's ISP.

By default, this feature is disabled. To enable the feature, use GuiDBEdit to set the `forward_log_without_delete` property to `TRUE`.

**Note** - If cyclical logging has been enabled, the log files maintained on the sender after forwarding will eventually be overwritten.

### Basic Tracking Configuration

**To track connections in your network:**

1. For each of the Security Policy rules you wish to track, right-click in the **Track** column and choose **Log** from the menu.
   
   All events matching these rules are logged.

2. Launch SmartView Tracker through the SmartDashboard's **Window** menu.
   
   The Log mode is displayed, showing the records of all events you have logged.

### Configuring SmartView Tracker Views

The display of SmartView Tracker can be modified to better suit your auditing needs. The following table lists the operations you can perform to adjust the view.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toggling the display of the Query Tree and Query Properties panes</td>
<td>Choose <strong>View &gt; Query Tree</strong> or <strong>Query Properties</strong> (respectively).</td>
</tr>
</tbody>
</table>
Configuring SmartView Tracker

<table>
<thead>
<tr>
<th>Operation</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resizing columns</td>
<td>Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• In the Query Properties pane — enter the appropriate number of characters in the Width column, or</td>
</tr>
<tr>
<td></td>
<td>• In the Records pane — drag the column's right border while clicking on the left mouse button. Release when the column has reached its desired width.</td>
</tr>
<tr>
<td>Sorting columns</td>
<td>Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• In the Query Properties pane — drag the column up or down to the desired position, or</td>
</tr>
<tr>
<td></td>
<td>• In the Records pane — drag the header of the column left or right to the desired position.</td>
</tr>
<tr>
<td>Collapsing/expanding the Query Tree</td>
<td>Selecting (+) or (-), respectively.</td>
</tr>
<tr>
<td>Display a record's details window</td>
<td>Double-click the record in question in the Records pane.</td>
</tr>
</tbody>
</table>

**Query Pane**

The Query Tree pane is the area where the Log Files appear. The SmartView Tracker has a new and improved interface enabling you to open multiple windows.

You can open more than one Log File simultaneously. You can also open more than one window of the same Log File. This may be helpful if you want to get different images of the same Log File. For example, you can open two windows of the same file and use different filtering criteria on each window. You can view both windows simultaneously and compare the different images. You can also resize each window so as to fit in as many windows as possible in the Query pane. The Query pane is divided into two sections:

- **Query Properties pane** shows all the attributes of the fields contained in the Records pane.
- **Records pane** displays the fields of each record in the Log File.

**Resolving IP Addresses**

Since the IP address resolution process consumes time and resources, SmartView Tracker allows you to choose whether or not to display source and destination host names in the Log file.

Click the Resolve IP toolbar button to toggle between:

- Displaying the name of the host and the domain.
- Displaying the addresses in conventional IP dot notation.

**Resolving Services**

With the Resolving Services option you can control the display of the source and destination port in the Log File. Each port number is mapped to the type of service it uses.

This option toggles between:

- Displaying the destination port number.
- Displaying the type of service the port uses.

If you click Resolving Services to see the type of service the port uses, and the port number shows: no service is defined for this port. You can map a port number to a service in the Object Manager, or in the Services Configuration file (/etc/services).

**Showing Null Matches**

This option controls the display of Null Matches, that is, log entries that are neither included nor excluded by the current filtering criteria.
For example, if you choose to display only log entries whose Action is either Reject or Drop, control logs are null matches because Action is not relevant to a control log. They are neither included nor excluded. If the Show Null Matches toolbar button is clicked, the null matches are displayed.

Configuring a Filter

Make sure the Apply Filter toolbar button is activated. Filter criteria is not applied if this button is not active.

To filter a log field and focus on data of interest:
1. Click View > Query Properties.
2. Right-click the log field in the Filter column, and select Edit Filter.
   Each field shows a type-specific Filter window. Configure the window according to the criteria you want.
3. Click OK.

Configuring the Current Rule Number Filter

To launch the Current Rule Number Filter:
1. Right-click anywhere in the column Curr. Rule No. and select Edit Filter.
2. Select the appropriate policy package from the drop-down list.
3. Select the current rule number(s) of the logs you want to display and click OK.

Using Follow Commands

With the Follow commands you can create a filter that matches a specific query to a specific Source, Destination or User.

Right-click the record with the value of interest in the Records pane and select one of the following Follow commands:
- Follow Source enables a search for a log record according to a specific source.
- Follow Destination enables a search for a log record according to a specific destination.
- Follow User enables a search for a log record according to a specific user.
- Follow Rule Number enables a search for a log record according to the rule name.
- Follow Rule enables a search for a log record according to the rule number.

Note - A new window opens, displaying the relevant column (Source, Destination or User) first.

Viewing the Logs of a Rule from the Rule Base

From the Rule Base in SmartDashboard, it is possible to generate a filtered view of logs that match a specific rule. There are two ways of achieving this:
- View rule logs in SmartView Tracker
  Right-click on a rule in the No. column in SmartDashboard and select View rule logs in SmartView Tracker.
  SmartView Tracker opens with a filter applied to the Curr. Rule No. column to display only those logs that match on the selected rule.
- Copy rule ID
  a) Right-click on the rule in the No. column in SmartDashboard and select Copy rule ID.
  b) In SmartView Tracker, click View > Query Properties and enable the Rule UID column.
  c) Right-click on the Rule UID column heading and choose Edit Filter.
  d) Paste the UID in the Value field and click OK.
Configuring SmartView Tracker

A filter is applied to the Curr. Rule No. column to display only those logs that matched on the Rule UID.

Configuring Queries

New queries are created by customizing existing queries and saving them under new names. Proceed as follows:

1. Select an existing query in the Query Tree (either a predefined query or a custom query) and choose Query > Copy from the menu.
   A copy of the query, named New, is added to the Custom folder.
2. Rename the new query.
3. In the Query Properties pane, modify the query as desired by specifying the following for each relevant log field (column):
   - Whether to Show the information available for that column.
   - The Width of the column displaying the information.
   - The Filter (conditions) applied to the column.
4. Double-click the query in order to run it.

Opening an Existing Query

You can open an existing query in an active window by:

- Using the Query menu:
  In the Query Tree pane, select the query you would like to open. Select Query > Open. The desired query appears in the Records pane.
- Right-clicking an existing query.
  Right-click the query you would like to open. Select Open. The desired query appears in the Records pane.
- Double-clicking an existing query.
  Double-click the query you would like to open. The desired query appears in the Records pane.

Creating a Customized Entry

Predefined queries contained in the Predefined folder cannot be modified but they can be saved under a different name.

To save a predefined query under a different name:
1. Open a predefined query.
2. Modify the query as desired.
3. From the Query menu, select Save As.
4. Type the desired query name.
5. Click OK. The modified view is placed in the Custom folder.

Saving a Query under a New Name

You can modify a query and save it under a new name.

To change a predefined query and save it under a new name:
1. Modify the predefined query as desired.
2. Choose Save As from the Query menu, and specify a file name for the modified query.
3. Click OK. The modified query is placed in the Custom folder.

To change a custom query:
1. Modify the query as desired.
2. Choose Save from the Query menu.
Renaming a Customized Query

1. Select the query you want to rename.
   - From the Query menu, select Rename, or
   - Right-click the desired query and select Rename from the displayed menu. The newly-duplicated query is placed in the Custom folder.
2. Enter the desired query name and click Enter.

Deleting a Customized Query

Select the query you want to delete:
   - From the Query menu, select Delete, or
   - Right-click the desired query and select Delete from the displayed menu.
   
   Note - You cannot delete an open or predefined query.

Hiding and Showing the Query Tree Pane

You can choose to hide or display the Query Tree pane. To toggle the display of the Query Tree pane click Query Tree from the View menu.

Working with the Query Properties Pane

The Query Properties pane shows the attributes for the corresponding columns in the Records pane. These attributes include whether the columns are displayed or hidden, the width of the column and the filtering arguments you used to display specific entries.

The Query Properties pane contains four columns.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Column</td>
<td>The name of the column.</td>
</tr>
<tr>
<td>Show</td>
<td>Select to display the corresponding column in the Records pane. Clear to hide the column.</td>
</tr>
<tr>
<td>Width</td>
<td>The specified width of the corresponding column in the Records pane in pixels.</td>
</tr>
<tr>
<td>Filter</td>
<td>The items in this column represent the filtering criteria used to display specific log data.</td>
</tr>
</tbody>
</table>

Showing/Hiding a Column

- Using the Query Properties pane
  In the Query Properties pane, select the column's check box in the Show column to display the column or clear the check box to hide it. The corresponding column in the Records pane is displayed/hidden respectively.
- Using the Records pane
  In the Records pane, right-click the column heading. Select Hide from the displayed menu. The column is hidden and at the same time, the check box in the Show column in the Query Properties pane is automatically cleared.

Changing a Column’s Width

If you change the width of a column in one pane, it is automatically changed in the other. You can change the width of a column either in the:

- Query Properties pane
Double-click the Width field that you would like to edit in the Width column. The Width field becomes an editable field in which you can specify a new width (in pixels). Edit the width value and click Enter. The corresponding column in the Records pane is widened/narrowed accordingly.

- Records pane
  Place the cursor on the column's right border in the header. The cursor changes to the column resize cursor. Click on the left mouse button without releasing it. Move the column border to the desired position while keeping the left mouse button down. Release the left mouse button. The value in the column's corresponding Width field in the Query Properties pane is automatically modified accordingly.

### Rearranging a Column's Position

You can rearrange a column's position in the Query Properties or the Records pane. If you change the position in one pane, it is automatically changed in the other.

- In the Queries Properties pane, drag the column up or down to the desired position.
- In the Records pane, drag the header of the column left or right to the desired position.

### Copying Log Record Data

You can copy a whole log record or only one of its cells to the clipboard:

- Right-click the desired record.
- Select Copy Cell from the displayed menu to copy only the cell on which the cursor is standing or select Copy Line to copy the entire record.

### Viewing a Record's Details

The Record Details window is displayed by double-clicking the desired record in the Records pane.

This window allows you to conveniently view the record's values for all fields included in your query. Fields that have been defined as hidden for that record are not displayed. The fields appear in the same order as they appear in the Records pane, and all field values appear in their entirety, as can be seen in the tooltip.

This window allows you to perform the following operations:

- Display the details of the former or subsequent record by clicking the Previous or Next button respectively. (These buttons correspond to the keyboard arrows.)
- Copy the record details to the clipboard by clicking Copy.
- End operations that take a long time by clicking Abort (this button is enabled only when the server is running).

Note - The Abort option only becomes active when a certain action is being executed, for example, when the Log File is being updated or when a search is taking place.

### Viewing a Rule

You can view the rule that created the log.

**To view a rule:**

1. Open SmartDashboard.
   a) Click the Database Revision Control toolbar button.
   b) Click inside the Create new version upon Install Policy operation check box.
   c) Click Close.
   d) Click Install Policy.
2. Go to SmartView Tracker.
3. Right-click on the desired record.
4. Select **View Rule in SmartDashboard**. The SmartDashboard is opened and the rule appears.

   **Note** - This process only works for logs that have a rule number and were created after the Create a new version upon Install Policy operation is selected. In addition, this option is only available on a Management Station. It is not available on the Domain Log Server.

**Finding an Interface**

To find by interface, add the specific Interface. You can find according to direction forward and back.
Managing the Log Switch Settings

A log switch can be performed in one of the following ways:

- **Automatically**, when the log file’s size is 2 GB.
  You can modify this default size limit, as well as define a log switch schedule, through the SmartDashboard, by editing the properties of the object collecting the logs (the Security Management server, Log Server or the Security Gateway).

- **Manually**, from SmartView Tracker.

**Modifying the Automatic Log Switch Settings**

1. In the SmartDashboard, double-click the gateway in question.
   The gateway’s properties window is displayed.
2. In **Log switch** section of the **Logs and Masters** page, specifies when to perform the log switch:
   - To specify the file size that should trigger a log switch, check **Log switch when file size is x MBytes** and specify the appropriate size.
   - To setup a log switch schedule, check **Schedule log switch to** and choose the appropriate time object from the drop-down list.
   If you specify both options, the log switch is performed when the first criterion is met.
3. Click **OK**.

**Manual Log Switch**

1. In SmartView Tracker, choose **File > Switch Active File** from the menu.
   The **Switch active Log File** window is displayed.
2. By default, the current log file is named based on the current date and time.
   To specify a different name, uncheck **Default** and enter the appropriate name under **Log File Name**.

Managing the Cyclic Logging Settings

**To configure the Cyclic Logging process:**

1. In the SmartDashboard, double-click the gateway in question.
The gateway’s properties window is displayed.

2. In the Disk Space Management section of the Logs and Masters page, specify the following:
   - Whether to Measure free disk space in MBytes or Percent.
   - Check Required Free Disk Space and enter the appropriate value.
   - To refrain from deleting the most recent log files among your old log files, check Do not delete log files from the last and specify the appropriate number of Days.

**Purging a Log File**

To delete all records in the active fw.log log file, display the Log or Audit mode and choose Purge Active File from the File menu.

**Saving Log Files Locally**

To save logs to a local file (instead of forwarding them to the Security Management server or to a Log Server):

1. In the SmartDashboard, double-click the gateway in question to display its properties window.
2. In the Log Servers page (under the Logs and Masters branch), check Define Log Servers and then check Save logs locally, on this machine (<machine hostname>).
3. You can either set a schedule for forwarding the local file to the appropriate machine (the Security Management server or a Log Server), or manually import these files using SmartView Tracker.
   
   **To specify a log file forwarding schedule:**
   - Display the Additional Logging Configuration page (under the Logs and Masters branch).
   - In the Log forwarding settings section, set the following:
     - Check Forward log files to Security Management server and choose the Log Server from the drop-down list.
     - Set a Log forwarding schedule by choosing the appropriate time object from the drop-down list.

**To view the local file using SmartView Tracker:**

1. Select Tools > Remote Files Management.
   
   The Remote Files Management window is displayed, listing all Security Gateways from which you can fetch Log files.
2. Select the desired Security Gateway and click Get File List.
   
   The Files on <Gateway Name> window is displayed, listing all Log files found on the selected Security Gateway.
3. Select one or more files to be fetched.
   
   **Note** - You cannot fetch an active Log File. If you want to fetch the current file, you must first perform a log switch.
4. Click Fetch Files.
   
   The Files Fetch Progress window is displayed, showing the progress of the file transfer operation.

**Working with Log Servers**

To reduce the Security Management server’s load via Log Servers:

1. Install the Log Server software on the machine you wish to dedicate to logging purposes.
   
   **Note** - For proper Log Server operations, the Plug-ins that are installed on the Security Management server should also be installed on the Log Server.
2. Launch the SmartDashboard and add the Log Server you have installed as a Check Point network object:
   - Choose Manage > Network Objects > New > Check Point > Host from the menu.
The Check Point Host window is displayed.

- In the General Properties page, define the standard network object properties, including:
  - Checking Log Server in the Check Point Products list.
  - Setting up Secure Internal Communication between this Log Server and the Security Management server.

- Define additional properties as needed and click OK.

3. Install the Check Point Objects Database on the Log Server object:
   - Choose Policy > Install Database from the menu.
   - The Install Database window is displayed.
   - In the Install Database on list, check the Log Server object and click OK.

4. To setup the gateway to forward its logs to this Log Server, double-click the gateway so that its properties window is displayed.

5. You can either forward the log records online, one by one; or save the records locally, and then forward them in a file according to a specific schedule.

   To forward log records online:
   - Display the Log Servers page (under the Logs and Masters branch).
   - Check Define Log Servers.
   - Add this Log Server to the Always send logs to table (click Add to display the Add Logging Servers window, and move the Log Server from the Available Log Servers list to the Select Log Servers list).

   To specify a log file forwarding schedule:
   - Display the Additional Logging Configuration page (under the Logs and Masters branch).
   - In the Log forwarding settings section, set the following:
     - Check Forward log files to Log Server and choose the Log Server from the drop-down list.
     - Set a Log forwarding schedule by choosing the appropriate time object from the drop-down list.

6. By default, when the selected Log Server is unreachable, the logs are written to a local file. Alternatively, you can select a backup Log Server as follows:
   - Display the Log Servers page (under the Logs and Masters branch).
   - Under When a Log Server is unreachable, send logs to section, click Add to display the Add Logging Servers window.
   - Move the Log Server from the Available Log Servers list to the Select Log Servers list and click OK.

7. Repeat step 4 to step 6 on all relevant gateways.

8. Launch SmartView Tracker and login to this Log Server (instead of the Security Management server).

Using Custom Commands

To configure the commands you can run through SmartView Tracker:

1. Choose Tools > Custom Commands from the menu.
   - The Custom Commands window is displayed.

2. Click Add.
   - The Add New Command window is displayed.

3. Specify the following command properties:
   - Menu Text, defines how this command is to be displayed in the right-click menu (e.g. Ping).
   - Command, specifying the name of the command (e.g. ping.exe).
   - Arguments to be used by the command.
   - IP Columns only, allowing you to apply this command only to columns that have an IP address value (e.g. Origin, Source, Destination etc.).
Note - It is recommended not to use a full path name in the Executable field, since the executable file may be found in different directories of different SmartView Tracker clients. The administrator must ensure that the command can be executed from the SmartView Tracker installation directory. Commands requiring a full path can be executed by a script, which all administrators save in the same directory, but each administrator edits according to his or her needs.

Example:
1. Use the Add New Command window to add the Menu Content TELNET, which runs the command TELNET using <Cell Value> as its Parameter.
2. In the Records pane, right-click a record whose IP address is 192.0.2.2 and select Telnet from the menu.
   The executed command is: telnet 192.0.2.2.

Using Block Intruder
SmartView Tracker allows you to terminate an active connection and block further connections from and to specific IP addresses. The Block Intruder feature only works on UDP and TCP connections. Proceed as follows:
1. Select the connection you wish to block by clicking it in the Active mode’s Records pane.
2. From the Tools menu, select Block Intruder.
   The Block Intruder window is displayed.
3. In Blocking Scope, select the connections that you would like to block:
   - Block all connections with the same source, destination and service - block the selected connection or any other connection with the same service, source or destination.
   - Block access from this source - block access from this source. Block all connections that are coming from the machine specified in the Source field.
   - Block access to this destination - block access to this destination. Block all connections that are headed to the machine specified in the Destination field.
4. In Blocking Timeout, select one of the following:
   - Indefinite blocks all further access
   - For x minutes blocks all further access attempts for the specified number of minutes
5. In Force this blocking, select one of the following:
   - Only on blocks access attempts through the indicated Security Gateway.
   - On any Security Gateway blocks access attempts through all Security Gateways defined as gateways or hosts on the Log Server.
6. Click OK.
   To clear blocked connections from the display, choose Clear Blocking from the Tools menu.

Configuring Alert Commands
When you set a rule's Track column to Alert, SNMP Trap, Mail or UserDefined, a log of the event matching the rule is written to the active log file and the Security Management server executes the appropriate alert script.

Alert scripts are defined through the SmartDashboard, in the Global Properties window's Alert Commands page. You can use the default mail alert and SNMP trap alert scripts, by entering the appropriate IP addresses. Alternatively, define your own alert(s) in the three UserDefined fields.
Enabling Warning Dialogs

When working with SmartView Tracker, messages will appear in a variety of situations. Some of these messages have the option "Don't show this dialog box again". The **Tools > Enable Warning Dialogs** enables you to view all the dialog boxes for which you selected "Don't show this dialog box again".
Index

B
Basic Tracking Configuration • 21
Blocking Intruders • 18

C
Changing a Column's Width • 25
Choosing the Appropriate Tracking Option • 20
Choosing which Rules to Track • 20
Configuring a Filter • 23
Configuring Alert Commands • 31
Configuring Queries • 24
Configuring SmartView Tracker • 20
Configuring SmartView Tracker Views • 21
Configuring the Current Rule Number Filter • 23
Copying Log Record Data • 26
Creating a Customized Entry • 24

D
Deleting a Customized Query • 25
DLP Actions • 10
DLP General Columns • 11
DLP Restricted Columns • 11

E
Enabling Warning Dialogs • 31
Exporting Logs • 17

F
Filtering Log Entries by Matching Rule • 16
Filters • 15
Finding an Interface • 27
Forwarding Online or Forwarding on Schedule • 21

H
Hiding and Showing the Query Tree Pane • 25

I
Identity Awareness Columns • 12
Important Information • 3
Introduction • 6
IPS Columns • 12
IPS-1 Columns • 13

L
Log Suppression • 7
Logging Behavior during Downtime • 17
Logging Using Log Servers • 17

M
Maintaining a Secure Network • 18
Maintaining Log Files with Log Switch • 17
Managing Disk Space with Cyclic Logging • 17
Managing the Cyclic Logging Settings • 28
Managing the Log Switch Settings • 28
Manual Log Switch • 28
Matching Rules • 16
Modifying the Automatic Log Switch Settings • 28
Modifying the Log Forwarding Process • 21

O
Opening an Existing Query • 24
Overview • 20

P
Purging a Log File • 29

Q
Queries • 15
Query Pane • 22

R
Rearranging a Column's Position • 26
Renaming a Customized Query • 25
Resolving IP Addresses • 22
Resolving Services • 22
Running Custom Commands • 18

S
Saving a Query under a New Name • 24
Saving Log Files Locally • 29
Saving Logs on Security Gateways • 17
Setting Up Security Management Server for Log Server • 18
Showing Null Matches • 22
Showing/Hiding a Column • 25
SmartView Tracker Actions • 10
SmartView Tracker GUI • 7
SmartView Tracker Maintenance • 28
SmartView Tracker Modes • 13
SmartView Tracker Overview • 6
SmartView Tracker Query Toolbar • 9
SmartView Tracker Toolbar • 8

T
Tracking Network Traffic • 7

U
Using Block Intruder • 31
Using Check Point Advisories • 18
Using Custom Commands • 30
Using Follow Commands • 23
Using SmartView Tracker • 15

V
Viewing a Record's Details • 26
Viewing a Rule • 26
Viewing Log Files • 15
Viewing Packet Capture • 19
Viewing the Logs of a Rule from SmartDashboard • 16
Viewing the Logs of a Rule from the Rule Base • 23
Viewing the Matching Rule in Context • 16

W
Working with Log Servers • 29
Working with the Query Properties Pane • 25