CHAPTER 5

SmartView Tracker

In This Chapter

The Need for Tracking page 89

The Check Point Solution for Tracking page 90

Tracking Considerations page 96

Tracking Configuration page 97

The Need for Tracking

As a system administrator, you need an advanced tracking tool in order to;

- Ensure your products are operating properly, to confirm that both basic operations such as access control and more advanced operations like IKE are all performed correctly.
- Troubleshoot system and security issues
- Gather information for legal reasons
- Generate reports to analyze your traffic patterns

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. However, if your firewall is being attacked, you must be alerted immediately.

The Check Point Solution for Tracking

In This Section

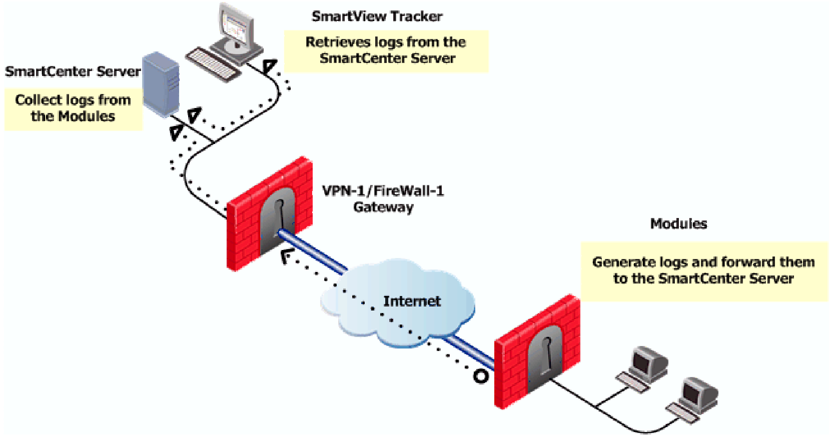
Tracking Overview	page 90
The SmartView Tracker	page 91
Filtering	page 93
Queries	page 93
Log File Maintenance via Log Switch	page 94
Disk Space Management via Cyclic Logging	page 94
Log Export Capabilities	page 94
Local Logging	page 95
Logging using Log Servers	page 95
Advanced Tracking Operations	page 96

Tracking Overview

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.

FIGURE 5-1 illustrates the log collection and tracking process:

FIGURE 5-1 Log Collection and Tracking Process


SmartView Tracker
Retrieves logs from the SmartCenter Server
SmartCenter Server
Collect logs from the Modules
VPN-1/FireWall-1 Gateway
Modules
Generate logs and forward them to the SmartCenter Server
Internet

The *SmartDashboard* allows you 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 firewall machine. For a list of the available tracking options, right-click the relevant rule's **Track** column.

The *modules* on which this Policy is installed collect data as specified in the Policy, and forward the logs to the *SmartCenter 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 SmartCenter 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 SmartCenter Server makes these logs available for inspection via the *SmartView Tracker*: a comprehensive auditing solution, enabling you to centrally manage 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 Check Point's SmartView Reporter; or export them to text files or to an external Oracle database.

The SmartCenter 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.).

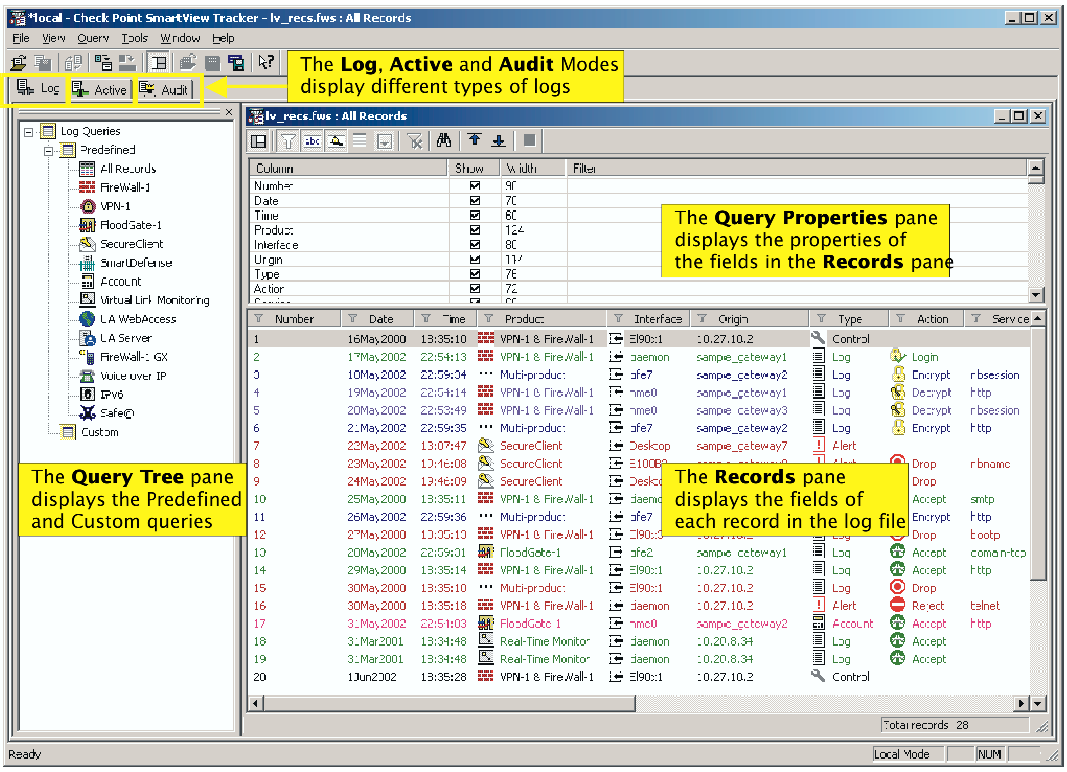
In addition to the above solutions, you can benefit from the tracking and auditing capabilities of the following Check Point SmartConsole:

- The *SmartView Status* allows you to track connections per-module.
- The *SmartView Monitor* offers real-time data with multiple counters.
- The *SmartView Reporter* allows you to save consolidated records (as opposed to "raw" logs) and conveniently focus on events of interest.

The SmartView Tracker

FIGURE 5-2 on page 92 displays the SmartView Tracker's main window. Each 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 at to the records pane as well.

FIGURE 5-2 SmartView Tracker — Main Screen



The **Log**, **Active** and **Audit** Modes display different types of logs

The **Query Tree** pane displays the Predefined and Custom queries

The **Query Properties** pane displays the properties of the fields in the **Records** pane

The **Records** pane displays the fields of each record in the log file

Column	Show	Width	Filter
Number	☑	90	
Date	☑	70	
Time	☑	60	
Product	☑	124	
Interface	☑	80	
Origin	☑	114	
Type	☑	76	
Action	☑	72	

Number	Date	Time	Product	Interface	Origin	Type	Action	Service
1	16May2000	18:35:10	VPN-1 & FireWall-1	El90x1	10.27.10.2	Control		
2	17May2002	22:54:13	VPN-1 & FireWall-1	daemon	sample_gateway1	Log	Login	
3	18May2002	22:59:34	Multi-product	qfe7	sample_gateway2	Log	Encrypt	nbsession
4	19May2002	22:54:14	VPN-1 & FireWall-1	hme0	sample_gateway1	Log	Decrypt	http
5	20May2002	22:53:49	VPN-1 & FireWall-1	hme0	sample_gateway3	Log	Decrypt	nbsession
6	21May2002	22:59:35	Multi-product	qfe7	sample_gateway2	Log	Encrypt	http
7	22May2002	13:07:47	SecureClient	Desktop	sample_gateway7	Alert		
8	23May2002	19:46:08	SecureClient	E100B[illegible]	[illegible]	Alert	Drop	nbname
9	24May2002	19:46:09	SecureClient	Deskt[illegible]	[illegible]	[illegible]	Drop	
10	25May2000	18:35:11	VPN-1 & FireWall-1	daem[illegible]	[illegible]	[illegible]	Accept	smtp
11	26May2002	22:59:36	Multi-product	qfe7	[illegible]	[illegible]	Encrypt	http
12	27May2000	18:35:13	VPN-1 & FireWall-1	El90x3	10.27.10.2	Log	Drop	bootp
13	28May2002	22:59:31	FloodGate-1	qfe2	sample_gateway1	Log	Accept	domain-tcp
14	29May2000	18:35:14	VPN-1 & FireWall-1	El90x1	10.27.10.2	Log	Accept	http
15	30May2000	18:35:10	Multi-product	El90x1	10.27.10.2	Log	Drop	
16	30May2000	18:35:18	VPN-1 & FireWall-1	daemon	10.27.10.2	Alert	Reject	telnet
17	31May2002	22:54:03	FloodGate-1	hme0	sample_gateway2	Account	Accept	http
18	31Mar2001	18:34:48	Real-Time Monitor	daemon	10.20.8.34	Log	Accept	
19	31Mar2001	18:34:48	Real-Time Monitor	daemon	10.20.8.34	Log	Accept	
20	1Jun2002	18:35:28	VPN-1 & FireWall-1	El90x1	10.27.10.2	Control		

Total records: 28

The log fields displayed are a function of the following factors:

- The product that generated the log (e.g. FireWall-1 vs. FloodGate-1)
- The type of operation performed (e.g. installation vs. 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 VPN-1 is used, IKE-related fields (e.g. **IKE CookieI**, **IKE CookieR** etc.) are displayed.

SmartView Tracker Modes

The 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 products, as well as Check Point's OPSEC partners. New logs that are added to the `fw.log` file are added to the bottom or the Records pane.
- **Active** allows you to focus on connections that are currently open through the VPN-1/FireWall-1 modules 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.

Filtering

The 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.

Since it is very useful to filter the **Product** field and focus on a specific Check Point product, the SmartView Tracker features these filters as predefined queries, described in the following section.

Queries

The 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's three modes (**Log**, **Active** and **Audit**) has its own *Query Tree*, consisting of the following folders:

- **Predefined**, containing 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**, allowing 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.

Log File Maintenance via 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 the 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`.

Disk Space Management via 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 module can continue logging new information. The Cyclic Logging process is controlled by;

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

Log Export Capabilities

While the 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

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

Local Logging

By default, modules forward their log records online to the SmartCenter Server. Alternatively, to improve the module'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 SmartCenter Server or Log Server, according to a specified schedule; or manually imported through the SmartView Tracker, using the Remote File Management operation.

If you choose to use a local logging configuration, you need to manually configure the standard log maintenance settings (e.g. log switch, cyclic logging etc.) on the module.

Logging Behavior During Downtime

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

Logging using Log Servers

To reduce the SmartCenter Server's load, administrators can install Log Servers and then configure the modules to forward their logs to these Log Servers. In this case, the logs are viewed by logging with the SmartView Tracker into the Log Server machine (instead of the SmartCenter Server machine).

A Log Server behaves just like a SmartCenter 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.

Advanced Tracking Operations

Block intruder

The **Active** mode of the SmartView Tracker allows you to shut out intruders, by selecting the connection you've identified as intrusive and blocking one of the following:

- 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.

Custom commands

The 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.

Tracking Considerations

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