SmartView Monitor

R75.40

Administration Guide

16 April 2012
Important Information........................................................................................................ v
Introducing SmartView Monitor.......................................................................................... 6
  SmartView Monitor Features.......................................................................................... 6
  SmartView Monitor Considerations............................................................................ 7
  Terminology.................................................................................................................. 7
Understanding the User Interface........................................................................................ 8
  Gateways Status View.................................................................................................. 8
  Traffic View................................................................................................................... 9
  System Counters View................................................................................................ 10
  Tunnels View............................................................................................................... 11
  Users View.................................................................................................................. 12
  Cooperative Enforcement View................................................................................ 13
Monitoring Alerts................................................................................................................. 14
  Alerts.............................................................................................................................. 14
  Interfering Actions........................................................................................................ 14
  Viewing Alerts............................................................................................................... 15
System Alerts..................................................................................................................... 15
  Global versus Customized System Alert Parameters................................................... 15
  Defining Global Properties........................................................................................... 15
  System Alert Monitoring Mechanism......................................................................... 16
Monitoring Gateway Status................................................................................................ 17
  Gateway Status Solution............................................................................................... 17
  How Does it Work?........................................................................................................ 18
  Gateway Status............................................................................................................. 18
  Displaying Gateway Information................................................................................ 19
  Views of a Specified Gateway...................................................................................... 22
  Interfering Actions........................................................................................................ 23
  Thresholds.................................................................................................................... 23
  Alert Dialog................................................................................................................... 23
  SNMP Monitoring Thresholds...................................................................................... 24
Configuring Gateway Views................................................................................................. 27
  Defining Status Fetch Frequency.................................................................................. 28
  Start/Stop Cluster Member ........................................................................................... 28
  Select and Run a Gateways View................................................................................ 28
  Refresh a Gateways Status View................................................................................ 28
  Run a Specific View at Startup..................................................................................... 28
  Monitoring Tunnels....................................................................................................... 29
  View In-Depth Information about a Specific Gateway.................................................. 32
  Create a Custom Gateways Status View....................................................................... 32
  Edit a Gateway View.................................................................................................... 33
  Defining a Threshold...................................................................................................... 33
  Define Global Threshold Settings................................................................................ 33
  Delete a Custom Gateway View................................................................................... 33
  Copy a Gateway View................................................................................................... 33
  Rename a Custom Gateway Status View..................................................................... 34
  Export a Custom Gateway Status View....................................................................... 34
Monitoring Traffic or System Counters.............................................................................. 35
  Traffic or System Counters Solution............................................................................ 35
  Traffic............................................................................................................................ 35
  System Counters.......................................................................................................... 36
  Traffic or System Counters Configuration................................................................... 36
  Select and Run a Traffic or System Counters View.................................................... 37
Run a Specific View at Startup ......................................................... 37
Create a New Traffic or System Counters Results View .................. 37
Create a Real-Time Custom Traffic or Counter View ....................... 38
Create a History Traffic or Counter View ........................................ 38
Edit a System Counter or Traffic View ............................................. 38
Edit a Custom Traffic or System Counter View ............................... 39
Copy a Traffic or System Counter View ........................................... 39
Rename a Custom Traffic or Counter View ....................................... 39
Delete a Custom Traffic or Counter View ........................................ 39
Export a Custom Traffic or Counter View ....................................... 40
Recording a Traffic or Counter View ............................................... 40

**Monitoring Suspicious Activity Rules** ......................................... 41
The Need for Suspicious Activity Rules .......................................... 41
Suspicious Activity Rules Solution .................................................. 41
Configure Suspicious Activity Rules .............................................. 41
Create a Suspicious Activity Rule ................................................... 41
Manage Suspicious Activity Rules .................................................. 43

**Monitoring Users** .................................................................. 44
Users Solution .............................................................................. 44
Users View Configuration .............................................................. 44
Run a Users View .......................................................................... 44
Refresh a Users View ................................................................... 45
Run a Specific View at Startup ....................................................... 45
Create a Custom Users View ......................................................... 45
Edit a Custom Users View ............................................................. 45
Edit a Users View .......................................................................... 46
Delete a Custom Users View .......................................................... 46
Copy a Users View ......................................................................... 46
Rename a Custom Users View ........................................................ 46

**Cooperative Enforcement** .......................................................... 47
Cooperative Enforcement Solution .................................................. 47
Enforcement Mode ......................................................................... 47
Monitor Only Deployment Mode ...................................................... 48
Non-Compliant Hosts by Gateway View ......................................... 48
Configuring a Cooperative Enforcement View ................................. 48

**Index** .................................................................................. 51
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=82734
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more information about this release, see the R75.40 Homepage - R75.40 sk67581 (http://supportcontent.checkpoint.com/solutions?id=sk67581).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 April 2012</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 Monitor R75.40 Administration Guide).
Chapter 1

Introducing SmartView Monitor

Corporate networks in today's dynamic business environment are often comprised of many networks and gateways that support a diverse set of products and user needs. The challenge of managing an increasing array of system traffic can put enormous pressure on IT staffing capacity and network resources. With SmartView Monitor, Check Point offers you a cost effective solution to obtain a complete picture of network and security performance; and to respond quickly and efficiently to changes in gateways, tunnels, remote users and traffic flow patterns or security activities.

SmartView Monitor is a high-performance network and security analysis system that helps you easily administer your network by establishing work habits based on learned system resource patterns. Based on Check Point's Security Management Architecture, SmartView Monitor provides a single, central interface for monitoring network activity and performance of Check Point Software Blades.

In This Chapter

- SmartView Monitor Features 6
- SmartView Monitor Considerations 7
- Terminology 7
- Understanding the User Interface 8

SmartView Monitor Features

SmartView Monitor allows administrators to easily configure and monitor different aspects of network activities. Graphical views can easily be viewed from an integrated, intuitive interface.

Pre-defined views include the most frequently used traffic, counter, tunnel, gateway, and remote user information. For example, Check Point System Counters collect information on the status and activities of Check Point products (for example, VPN or NAT). Using custom or pre-defined views, administrators can drill down on the status of a specific gateway and/or a segment of traffic to identify top bandwidth hosts that may be affecting network performance. If suspicious activity is detected, administrators can immediately apply a Firewall rule to the appropriate Security Gateway to block that activity. These Firewall rules can be created dynamically via the graphical interface and be set to expire within a certain time period.

Real-time and historical reports (that is, flexible, graphical reporting) of monitored events can be generated to provide a comprehensive view of gateways, tunnels, remote users, network, security and gateway performance over time.

The following list describes the key features of SmartView Monitor and how it is employed.

- **Gateways Status**
  SmartView Monitor enables information about the status of all gateways in the system to be collected from these gateways. This information is gathered by the Security Management server and can be viewed in an easy-to-use SmartConsole. The views can be customized so that details about the gateway(s) can be shown in a manner that best meets the administrator's needs.

- **Traffic / System Counters**
  SmartView Monitor delivers a comprehensive solution for monitoring and analyzing network traffic and network usage. You can generate fully detailed or summarized graphs and charts for all connections when monitoring traffic and for numerous rates and figures when counting usage throughout the network. The Traffic view also enables filtering according to categories (for example, services, IP addresses, interfaces or Firewall rules).

- **Tunnels**
Introducing SmartView Monitor

SmartView Monitor enables system administrators to monitor connectivity between gateways. With the information collected by SmartView Monitor system administrators are able to sustain privacy, authentication and integrity. By showing real-time information about active tunnels (for example, information about its state and activities, volume of traffic or which hosts are most active), administrators can verify whether the tunnel(s) is working properly.

- **Users**
  The Remote User Monitor is an administrative feature allowing you to keep track of VPN remote users currently logged on (that is, SecuRemote, Endpoint Security Secure Client and SSL Network Extender, and in general any IPSec client connecting to the VPN gateway). It provides you with a comprehensive set of filters which enables you to navigate easily through the obtained results.
  With information regarding, for example, current open sessions, overlapping sessions, route traffic, connection time, the Remote User Monitor is able to provide detailed information about remote users' connectivity experience. This feature enables you to view real-time and historical statistics about open remote access sessions.

- **Cooperative Enforcement**
  Cooperative Enforcement is a feature that works in conjunction with Endpoint Security client. This feature utilizes Endpoint Security client compliance capability in order to verify connections arriving from the various hosts across the internal network. The firewall generates logs for unauthorized hosts. The logs generated for both authorized and unauthorized hosts can be viewed in SmartView Monitor.

**SmartView Monitor Considerations**

In view of the fact that SmartView Monitor enables graphical views of different types of measurements such as bandwidth, round trip time, packet rate or CPU usage, the most efficient way to yield helpful information is to create a view based on your specific needs.

With SmartView Monitor it is possible to create customized views for view types (for example, status, traffic, system statistics and tunnels). The customization allows control over filtering what to view, and over the values to display (for example, the columns in the Gateway Status view).

The following are just two examples of the numerous scenarios for which SmartView Monitor can offer information:

- If a company’s Internet access is slow, a Traffic view and report can be created to ascertain what may be clogging up the company's gateway interface. The view can be based on a review of, for example, specific Services, Firewall rules or Network Objects, that may be known to impede the flow of Internet traffic. If the SmartView Monitor Traffic view indicates that users are aggressively using such Services or Network Objects (for example, Peer to Peer application or HTTP), the cause of the slow Internet access has been determined. If aggressive use is not the cause, the network administrator will have to look at other avenues (for instance, performance degradation may be the result of memory overload).

- If employees who are working away from the office cannot connect to the network a Counter view and report can be created to determine what may be prohibiting network connections. The view can be based on, for example, CPU Usage %, Total Physical Memory or VPN Tunnels, to collect information about the status, activities hardware and software usage of different Check Point products in real-time. If the SmartView Monitor Counter view indicates that there are more failures than successes, it is possible that the company cannot accommodate the mass number of employees attempting to log on at once.

**Terminology**

These are terms that you should be familiar with, to understand the information that is presented throughout this guide.

- **Views** generate reports about the network according to network targets, filters and specific settings (for example, Monitor Rate).
  - **Custom View** a view generated by the SmartView Monitor user. This type of view is created from scratch or is based on a modified version of an existing out of the box view for common network scenarios.
  - **System Counters** generates reports about the status, activities, hardware and software usage of different Check Point products in real-time or history mode.
• **Traffic** provides transaction information about network sessions in a given time interval.
• **Tunnel** is an encrypted connection between two gateways.
• **Gateways Status** provides information about the status of all Check Point supported hosts.
• **Users** provides information about remote access VPN clients (for example, Endpoint Connect, Mobile Access, and others that are interoperable with VPN clients).

**Cooperative Enforcement** is a feature that works in conjunction with Endpoint Security client. This feature utilizes Endpoint Security client compliance capability in order to verify connections arriving from the various hosts across the internal network. The firewall generates logs for unauthorized hosts. The logs generated for both authorized and unauthorized hosts can be viewed in SmartView Monitor.

• **History** provides information about previous Traffic or System Counters data.
• **Real-Time** provides information about Traffic or System Counters data as it is generated.

**Suspicious Activity Rules** are Firewall rules that are applied immediately. These rules can instantly block suspicious connections that are not restricted by the currently enforced security policy.

• **Threshold** contains actions that are triggered when the status of a blade is changed or when an event has occurred.

• **Cluster** indicates a group of servers and resources that act like a single system. This group enables high availability and in some cases, load balancing and parallel processing.

• **High Availability** is a system or component that is continuously operational for a long length of time. Availability can be measured relative to "100% operational" or "never failing."

### Understanding the User Interface

The SmartView Monitor is divided into a number of features. Refer to the following sections for a visual representation of each SmartView Monitor view.

The type of view results that appear on the screen are directly related to whether a **Traffic**, **Counter**, **Tunnel**, **Gateway** or **Remote User** view is selected.

### Gateways Status View

To understand the following **Gateways Status** view, refer to the numbers in the figure and the list preceding it.

**Figure 1-1**  
[Diagram of Gateways Status View]
Introducing SmartView Monitor

1. **Tree View** lists all the views.
2. **Toolbars** include shortcuts of SmartView Monitor options. The same options can also be accessed from the SmartView Monitor menus. The lower of the two toolbars is view specific and the same options can be found in the **Gateways** menu.
3. **Results View** provides information about all the gateways in the organization as well as pertinent information about the gateway (such as its IP Addresses, the last time it was updated as well as its status). This information is directly linked to the view selected in the **Tree View**. Each row in the table represents a **Gateway**.
4. **Gateway Details** is an HTML view that behaves like a browser and allows the user to hit links associated with a variety of data about the selected gateway.
5. At the bottom of the screen there is a button for every view that is currently running in SmartView Monitor (that is, a minimized view). As the number of running views grows the visibility of these buttons is aided by a tool tip. This tool tip displays the full name of the view on which the cursor is standing.

**Traffic View**

To understand the following **Traffic** view, refer to the numbers in the figure and the list preceding it.

**Figure 1-2** Traffic View

1. **Tree View** lists all the **Custom** and views.
2. **Toolbars** include shortcuts of SmartView Monitor options. The same options can also be accessed from the SmartView Monitor menus. The lower of the two toolbars is view specific and the same options can be found in the **Traffic** menu.
3. **Results View** (that is, bar, line, pie chart) provides information that is directly linked to the view selected and run from the **Tree View**.
4. **Legend** includes a textual view (that is, report) of the **Traffic** view results
5. **Traffic Status Bar** displayed at the bottom of the SmartView Monitor contains system information (for example, system uptime or traffic flow) about the gateway associated with the selected view.
6. At the bottom of the screen there is a button for every view that is currently running in SmartView Monitor (that is, a minimized view). As the number of running views grows the visibility of these buttons is aided by a tool tip. This tool tip displays the full name of the view on which the cursor is standing.
**System Counters View**

To understand the following **System Counters** view, refer to the numbers in the figure and the list preceding it.

**Figure 1-3**  System Counters View

1. **Tree View** lists all the Custom and views.
2. **Toolbars** include shortcuts of SmartView Monitor options. The same options can also be accessed from the SmartView Monitor menus. The lower of the two toolbars is view specific and the same options can be found in the **Counters** menu.
3. **Results View** (that is, bar, line, pie chart) provides information that is directly linked to the view selected and run from the **Tree View**.
4. **Legend** includes a textual view (that is, report) of the **System Counters** view results.
5. **Counter Status Bar** displayed at the bottom of the SmartView Monitor contains system information (for example, system uptime or traffic flow) about the gateway associated with the selected view.
6. At the bottom of the screen there is a button for every view that is currently running in SmartView Monitor (that is, a minimized view). As the number of running views grows the visibility of these buttons is aided by a tool tip. This tool tip displays the full name of the view on which the cursor is standing.
**Tunnels View**

To understand the following Tunnels view, refer to the numbers in the figure and the list preceding it.

**Figure 1-4** Tunnels View

1. **Tree View** lists all the Custom and views.
2. **Toolbars** include shortcuts of SmartView Monitor options. The same options can also be accessed from the SmartView Monitor menus. The lower of the two toolbars is view specific and the same options can be found in the Tunnels menu.
3. **Results View** provides information that is directly linked to the view selected in the Tree View. Each row in the table represents a Tunnel.
4. At the bottom of the screen there is a button for every view that is currently running in SmartView Monitor (that is, a minimized view). As the number of running views grows the visibility of these buttons is aided by a tool tip. This tool tip displays the full name of the view on which the cursor is standing.
**Users View**

To understand the following Users view, refer to the numbers in the figure and the list preceding it.

**Figure 1-5** Users View

1. **Tree View** lists all the Custom and views.

2. **Toolbars** include shortcuts of SmartView Monitor options. The same options can also be accessed from the SmartView Monitor menus. The lower of the two toolbars is view specific and the same options can be found in the Users menu.

3. **Results View** provides information that is directly linked to the view selected in the Tree View. Each row in the table represents a User.

4. At the bottom of the screen there is a button for every view that is currently running in SmartView Monitor (that is, a minimized view). As the number of running views grows the visibility of these buttons is aided by a tool tip. This tool tip displays the full name of the view on which the cursor is standing.
**Cooperative Enforcement View**

To understand the following Cooperative Enforcement view, refer to the numbers in the figure and the list preceding it.

**Figure 1-6** Cooperative Enforcement View

1. **Tree View** lists all the available views.
2. **Toolbars** include shortcuts of SmartView Monitor options. The same options can also be accessed from the SmartView Monitor menus. The lower of the two toolbars is view specific.
3. **Results View** provides information that is directly linked to the view selected in the Tree View.
4. At the bottom of the screen there is a button for every view that is currently running in SmartView Monitor (that is, a minimized view). As the number of running views grows the visibility of these buttons is aided by a tool tip. This tool tip displays the full name of the view on which the cursor is standing.
Chapter 2

Monitoring Alerts

In This Chapter

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alerts</td>
<td>14</td>
</tr>
<tr>
<td>Interfering Actions</td>
<td>14</td>
</tr>
<tr>
<td>Viewing Alerts</td>
<td>15</td>
</tr>
<tr>
<td>System Alerts</td>
<td>15</td>
</tr>
<tr>
<td>System Alert Monitoring Mechanism</td>
<td>16</td>
</tr>
</tbody>
</table>

Alerts

Alerts provide real-time information about vulnerabilities to computer systems and how they can be eliminated.

Check Point alerts users to potential threats to the security of their systems and provides information about how to avoid, minimize, or recover from the damage.

Alerts are sent by the Security Gateways to the Security Management server. The Security Management server then forwards these alerts to the SmartView Monitor client, which is actively connected to the Security Management server.

Alerts are sent in order to draw the administrator's attention to problematic gateways, and are displayed in SmartView Monitor. These alerts are sent:

- If certain rules or attributes, which are set to be tracked as alerts, are matched by a passing connection,
- If system events, also called System Alerts, are configured to trigger an alert when various thresholds are surpassed.

The administrator can define alerts to be sent for different gateways. These alerts are sent under certain conditions, such as if they have been defined for certain policies, or if they have been set for different properties. By default an alert is sent as a pop up message to the administrator's desktop when a new alert arrives to SmartView Monitor. Alerts can also be sent for certain system events. If certain conditions are set, you can get an alert for certain critical situation updates. These are called System Alerts. For example, if free disk space is less than 10%, or if a security policy has been changed. System Alerts are characterized as follows:

- Per product — For instance you may define certain System Alerts for Unified Package and other System Alerts for Check Point QoS.
- Global or per gateway — This means that you can set global alert parameters for all gateways in the system, or you can specify particular action to be taken on alert on the level of every Check Point gateway.
- Display — They are displayed and viewed using the same user-friendly window.

Interfering Actions

After reviewing the status of certain Clients, in SmartView Monitor, you may decide to take decisive action for a particular Client or Cluster Member, for instance:

- Disconnect client - if you have the correct permissions, you can choose to disconnect one or more of the connected SmartConsole clients.
• Start/Stop cluster member - All Cluster Members of a given Gateway Cluster can be viewed via SmartView Monitor. You can start or stop a selected Cluster Member.

**Viewing Alerts**

Alert commands are specified in the **Popup Alert Command** field in the Log and Alert page of the Global Properties window in SmartDashboard and can be viewed in the Alerts window in SmartView Monitor. The Alerts in this window apply only to Security Gateways.

To view the alerts, choose **Alerts** from the Tools menu in SmartView Monitor. The Alerts window is displayed. In this window you can set the alert attributes and delete any number of displayed alerts.

**System Alerts**

System Alerts are defined in the **Network Objects System Alert Definition** pane, in the System Alert tab. The tabs of this pane consist of:

- The **General** tab in which the System Alert parameters are defined
- A tab for each Check Point product in which product-specific attributes can be set

**Global versus Customized System Alert Parameters**

System Alerts can be customized per product or network object, or they can be set to comply with the global System Alert attributes. In order to define the System Alerts options, select the network object in the Modules pane, the details of this module are displayed in the Network Object System Alert Definition pane. In the General tab, define:

- **Same as Global** in order to apply a set of System Alert parameters to all the modules in the Module. If you apply global properties, the System Alert parameters cannot be modified
- **Custom** in order to define object-specific System Alert properties. For each product customize the settings.

Make sure that you click **Apply** button in order to save the option that you have selected.

**Defining Global Properties**

The **Global System Alert Definition** window enables you to define a set of default System Alert parameters (such as CPU utilization) for each installed product and determine the action to be taken (such as log or alert) when that parameter is reached. To open the **Global System Alert Definition** window, select System Alert > Global.
System Alert Monitoring Mechanism

Check Point Security Management server has a System Alert monitoring mechanism that takes the System Alert parameters you defined and checks if that System Alert parameter has been reached. If it is reached, it activates the action defined to be taken.

To activate this mechanism, select Tools > Start System Alert Daemon. To stop the System Alert monitoring mechanism, elect Tools > Stop System Alert Daemon.
Chapter 3

Monitoring Gateway Status

In This Chapter

Gateway Status Solution 17
Configuring Gateway Views 27

Gateway Status Solution

Check Point enables information about the status of all gateways in the system to be collected from these gateways. This information is gathered by the Security Management server and can be viewed in SmartView Monitor. The information gathered includes status information about:

- Check Point gateways
- OPSEC gateways
- Check Point Software Blades

Gateways Status is the SmartView Monitor view which displays all component status information. A Gateways Status view displays a snapshot of all Check Point Software Blades, such as VPN and ClusterXL, as well as third party products (for example, OPSEC-partner gateways).

Gateways Status is very similar in operation to the SNMP daemon that also provides a mechanism to ascertain information about gateways in the system.

Figure 3-7 Gathering Status Information

In the figure above information is retrieved by the Security Management server from all of the available Software Blades, using the AMON protocol, after SIC has been initialized.
**How Does it Work?**

The Security Management server acts as an AMON (Application Monitoring) client. It collects information about specific Check Point Software Blades installed, using the AMON protocol. Each Check Point gateway, or any other OPSEC gateway which runs an AMON server, acts as the AMON server itself. Each gateway makes a status update request, via APIs, from various other components such as:

- The "kernel"
- Security Servers

An alternate source for status collection may be any AMON client, such as an OPSEC partner, which uses the AMON protocol.

The information is fetched at a subscribed interval which is defined by the system administrator. The AMON protocol is SIC-based so information can be retrieved once SIC has been initialized.

**Gateway Status**

General statuses can occur on the Security Gateway or on the server on which a Check Point Software Blade is installed.

**Overall Status**

An Overall status is the result of the blades' statuses. The most serious Software Blades status determines the Overall status. For example, if all the Software Blades statuses are OK except for the SmartReporter blade, which has a Problem status, then the Overall status will be Problem.

- **OK** - indicates that the gateway is working properly.
- **Attention** - at least one of the Software Blades indicates that there is a minor problem but it can still continue to work.
  
  **Attention** can also indicate that, although a Software Blade is not installed, it is selected in the General Properties > Check Point Products associated with a specific gateway.
- **Problem** - indicates that one of the Software Blades reported a specific malfunction. To see details of this malfunction open the gateways status window by double-clicking it in the Gateways view.
  
  **Problem** can also indicate a situation in which the Firewall, VPN and ClusterXL Software Blades are selected in the General Properties > Software Blades but are not installed.
- **Waiting** - from the time that the view starts to run until the time that the first status message is received. This takes no more than thirty seconds.
- **Disconnected** - the Security Gateway cannot be reached.
- **Untrusted** - Secure Internal Communication failed. The gateway is connected, but the Security Management server is not the master of the gateway.

**Software Blade Status**

Software Blades include components such as VPN, SmartReporter, Endpoint Security, and QoS.

- **OK** - indicates that the blade (for example, SmartReporter, VPN, Firewall, etc.) is working properly.
- **Attention** - the blade indicates that there is a minor problem but it can still continue to work.
- **Problem** - indicates that the blade reported a specific malfunction. To see details of this malfunction open the gateways status window associated with the blade by double-clicking it in the Gateways Status view.
- **Waiting** - displayed from the time that the view starts to run until the time that the first status message is received. This takes no more than thirty seconds.
- **Disconnected** - the gateway cannot be reached.
- **Untrusted** - Secure Internal Communication failed. The gateway is connected, but the Security Management server is not the master of the gateway.
Displaying Gateway Information

Gateways Status, information is displayed per Check Point or OPSEC gateway.

To display information about the gateway, click the specific gateway in the Gateway Results view. Details about the gateway will be displayed in the Gateway Details pane.

This information includes general information such as the name, IP Address, version, operating system, and the status of the specified gateway, as well as gateway specific information, such as:

System Information

- **Unified Package** - the version number.
- **SO Information** - the name, the version name/number, the build number, the service pack and any additional information about the Operating System in use.
- **CPU** - the specific CPU parameters (for example, Idle, User, Kernel and Total) for each CPU. Note: In the Gateways Results view the Average CPU indicates the average total CPU usage of all existing CPOS.
- **Memory** - the total amount of virtual memory, what percentage of this total is being used. The total amount of real memory, what percentage of this total is being used and the amount of real memory available for use.
- **Disk** - displays all the disk partitions and their specific details (for example, capacity, used and free). Note: In the Gateways Results view the percentage/total of free space in the hard disk on which the firewall is installed. For example, if there are 2 hard drives C and D and the firewall is on C, the Disk Free percentage represents the free space in C and not D.

Firewall

- **Policy information** - the name of the Security Policy installed on the gateway and the date and time that this policy was installed.
- **Packets** - the number of packets accepted, dropped and logged by the gateway.
- **UFP Cache performance** - the hit ratio percentage as well as the total number of hits handled by the cache, the number of connections inspected by the UFP Server.
- **Hash Kernel Memory** (the memory status) and **System Kernel Memory** (the OS memory) - the total amount of memory allocated and used. The total amount of memory blocks used. The number of memory allocations, as well as those allocation operations which failed. The number of times that the memory allocation has freed up, or has failed to free up. The NAT Cache, including the total amount of hits and misses.

Virtual Private Networks

VPN is divided into three main statuses:

- **Current** represents the current number of active output.
- **High Watermark** represents the maximum number of current output
- **Accumulative** data which represents the total number of the output.

This includes:

- **Active Tunnels** - this includes all types of active VPN peers to which there is currently an open IPsec tunnel. This is useful for tracking the proximity to a VPN Net license and the activity level of the VPN gateway. High Watermark includes the maximum number of VPN peers for which there was an open IPsec tunnel since the gateway was restarted.
- **RemoteAccess** - this includes all types of RemoteAccess VPN users with which there is currently an open IPsec tunnel. This is useful for tracking the activity level and load patterns of VPN gateways serving as a remote access server. High Watermark includes the maximum number of RemoteAccess VPN users with which there was an open IPsec tunnel since the gateway was restarted.
- **Tunnels Establishment Negotiation** - The current rate of successful Phase I IKE Negotiations (measured in Negotiations per second). This is useful for tracking the activity level and load patterns of a VPN gateway serving as a remote access server. High Watermark includes the highest rate of successful Phase I IKE Negotiations since the Policy was installed (measured in Negotiations per second). In addition, accumulative data includes the total number of successful Phase I IKE negotiations since the Policy was installed.

- **Failed** - the current failure rate of Phase I IKE Negotiations can be used for troubleshooting, for instance, denial of service, or for a heavy load of VPN remote access connections. High Watermark includes the highest rate of failed Phase I IKE negotiations since the Policy was installed. And finally, Accumulative is the total number of failed Phase I IKE negotiations since the Policy was installed.

- **Concurrent** - the current number of concurrent IKE negotiations. This is useful for tracking the behavior of VPN connection initiation, especially in large deployments of remote access VPN scenarios. High Watermark includes the maximum number of concurrent IKE negotiations since the Policy was installed.

- **Encrypted and Decrypted throughput** - the current rate of encrypted/decrypted traffic (measured in Mbps). Encrypted/decrypted throughput is useful (in conjunction with encrypted/decrypted packet rate) for tracking VPN usage and VPN performance of the gateway. High Watermark includes the maximum rate of encrypted/decrypted traffic (measured in Mbps) since the gateway was restarted. And finally, Accumulative includes the total encrypted/decrypted traffic since the gateway was restarted (measured in Mbps).

- **Encrypted and Decrypted packets** - the current rate of encrypted/decrypted packets (measured in packets per second). Encrypted/decrypted packet rate is useful (in conjunction with encrypted/decrypted throughput) for tracking VPN usage and VPN performance of the gateway. High Watermark includes the maximum rate of encrypted/decrypted packets since the gateway was restarted. And finally, Accumulative, the total number of encrypted packets since the gateway was restarted.

- **Encryption and Decryption errors** - the current rate at which errors are encountered by the gateway (measured in errors per second). This is useful for troubleshooting VPN connectivity issues. High Watermark includes the maximum rate at which errors are encountered by the gateway (measured in errors per second) since the gateway was restarted. And finally the total number of errors encountered by the gateway since it was restarted.

- **Hardware** - the name of the VPN Accelerator Vendor, and the status of the Accelerator. General errors such as the current rate at which VPN Accelerator general errors are encountered by the gateway (measured in errors per second). The High Watermark includes the maximum rate at which VPN Accelerator general errors are encountered by the gateway (measured in errors per second) since the gateway was restarted. And finally the total number of VPN Accelerator general errors encountered by the gateway since it was restarted.

- **IP Compression** - Compressed/Decompressed packets statistics and errors.

**QoS**

- **Policy information** - the name of the QoS Policy and the date and time that it was installed.

- **Number of interfaces** - the number of interfaces on the Check Point QoS gateway. Information about the interfaces applies to both inbound and outbound traffic. This includes the maximum and average amount of bytes that pass per second, as well as, the total number of conversations, where conversations are active connections and connections that are anticipated as a result of prior inspection. Examples are data connections in FTP, and the "second half" of UDP connections.

- **Packet and Byte information** - the number of packets and bytes in Check Point QoS queues.

**ClusterXL**

- **The gateway’s working mode, whether or not it is active, and its place in the priority sequence.** There are three possible working modes (ClusterXL/Load Sharing or Sync only). There are 4 types of running modes, (Active, standby, ready and down).

- **Interfaces** include the interface(s) recognized by the gateway. The interface information includes the IP Address and status of the specified interface. Whether or not the connection passing through the interface is verified, trusted or shared.

- **Problem Notes** contains descriptions of the problem notification device such as its status, priority and when the status was last verified.
OPSEC

- The version name/number and build number of the Check Point OPSEC SDK and OPSEC product. The amount of time (in seconds) since the OPSEC gateway has been up and running.
- The OPSEC vendor may add additional fields to their OPSEC Application gateway's details.

Check Point Security Management

- The synchronization status indicates the status of the peer Security Management servers in relation to that of the selected Security Management server. This status can be viewed in the Management High Availability Servers window, whether you are connected to the Active or Standby Security Management server. The possible synchronization statuses are:
  - *Never been synchronized* - immediately after the Secondary Security Management server has been installed, it has not yet undergone the first manual synchronization that brings it up to date with the Primary Management.
  - *Synchronized* - the peer is properly synchronized and has the same database information and installed Security Policy.
  - *Advanced* - the Security Management server is more advanced than the standby server, it is more up-to-date.
  - *Lagging* - the Security Management server has not been synchronized properly.
  - *Collision* - the active Security Management server and its peer have different installed policies and databases. The administrator must perform manual synchronization and decide which of the Security Management servers to overwrite.

- **Clients** - the number of connected clients on the Security Management server, the name of the SmartConsole, the administrator responsible for administering the SmartConsole, the name of the SmartConsole host, the name of the locked database and the type of SmartConsole application, such as SmartDashboard, User Monitor etc.

UserAuthority WebAccess

- **Plug-in Performance** - the number of http requests accepted and rejected.
- **Policy info** - the name of the WebAccess policy and the last time that the policy was updated.
- **UAS info** - the name of the UA Server host, the IP Address and port number of the UAG Server. The number of requests sent to the UA Server and the time it took for the request to be handled.
- **Global UA WebAccess** - the number of currently open sessions and the time passed since the last session was opened.

SmartConsole Server

The number of licensed users who are currently connected.

Log Server

Indicates whether or not the Security Management server is active and the number of licensed users who are currently connected. The Log Server includes elaborate details about the named connected client, including, then name of the administrator, managing the selected Log Server, the host of the Log Server and the name of the database if it is locked. The Log Server also indicates the type of application that can be tracked by the Log Server.

Correlation Unit and SmartEvent

SmartView Monitor reads statuses from the SmartEvent Correlation Unit and SmartEvent server.

Correlation Unit status examples:

- is the SmartEvent Correlation Unit active or inactive
- is the SmartEvent Correlation Unit connected to the SmartEvent server
- is the SmartEvent Correlation Unit connected to the log server
Monitoring Gateway Status

- SmartEvent Correlation Unit and log server connection status
- offline job status
- lack of disk space status

SmartEvent Server status examples:
- last handle event time
- is the SmartEvent Server active or inactive
- a list of correlation units the SmartEvent Server is connected to
- how many events arrived in a specific time period.

The SmartEvent Correlation Unit should be connected to the log server(s) so that it can read logs. It also needs to be connected to the SmartEvent Server so that it can send events to it. If problems occur in the SmartEvent Correlation Unit Unit's connection to other components (for example, SIC problems) the problems are reported in the SmartEvent Correlation Unit Unit's status.

For the same reasons, the SmartEvent server contains statuses that provide information about its connect to all the SmartEvent Correlation Unit Unit(s) that it is currently connected to.

Anti-Virus and URL Filtering

SmartView Monitor can now provide statuses and counters for gateways with Anti-Virus and URL Filtering. The statuses are divided into the following two categories:
- Current Status
- Update Status (for example, when was the signature update last checked)

Anti-Virus statuses are associated with signature checks and URL Filtering statuses are associated with URLs and categories.

In addition, SmartView Monitor can now run Anti-Virus and URL Filtering counters. For example:
- Top five attacks in the last hour
- Top 10 attacks since last reset
- Top 10 http attacks in the last hour
- HTTP attacks general info

Multi-Domain Security Management

SmartView Monitor can now be used to monitor Multi-Domain Servers. This information can be viewed in the Gateway Status view. In this view it is now possible to view Multi-Domain Security Management counter information (for example CPU or Overall Status).

Views of a Specified Gateway

Gateways Status allows you to define views for specific gateways. From within a Gateway Status view it is possible to access information about the following:
- **Monitor Tunnels** - provides a list of Tunnels associated with the selected gateway. Tunnels are secure links between gateways that allow secure connections between gateways and remote access clients. The option of viewing a list of tunnels associated with a specific gateway enable you to keep track of the tunnels normal function, so that possible malfunctions and connectivity problems can be accessed and solved as soon as possible.
  
  For additional information about Tunnels refer to the Monitoring Tunnels (on page 29) chapter.

- **Monitor Users** - provides a list of Mobile Access users currently logged on to the specific Security Management servers. On the SmartView Monitor Gateways interface you will be able to view all the remote users currently logged on to specific Security Management servers.
• **Monitor Traffic or System Counters** - provides information about monitored and analyzed network traffic and network usage associated with the selected gateway. You can generate fully detailed or summarized graphs and charts for all connections intercepted and logged when monitoring traffic and for numerous rates and figures when counting usage throughout the network.

For additional information about Traffic or Counter refer to the Monitoring Traffic or System Counters (on page 35) chapter.

**Interfering Actions**

After reviewing the status of certain Clients, in SmartView Monitor, you may decide to take decisive action for a particular Client or Cluster Member, for instance:

- **Disconnect client** - if you have the correct permissions, you can choose to disconnect one or more of the connected SmartConsole clients.

- **Start/Stop Cluster member** - All Cluster Members of a given Gateway Cluster can be viewed via Gateways Status. You can start or stop a selected Cluster Member.

**Thresholds**

For each kind of Check Point Software Blade there is a set of status parameters that can be monitored. When the status of a blade is changed or when an event has occurred, predefined actions can be triggered. This is done by defining Thresholds (that is, limits) and actions to be taken if these Thresholds are reached or exceeded. To Define a Threshold refer to Defining a Threshold (on page 33).

**Alert Dialog**

Alerts provide real-time information about vulnerabilities to computing systems and how they can be eliminated.

Check Point alerts users to potential threats to the security of their systems and provides information about how to avoid, minimize, or recover from the damage.

Alerts are sent by the gateways to the Security Management server. The Security Management server then forwards these alerts to SmartView Monitor, which is actively connected to the Security Management server.

Alerts are sent in order to draw the administrator's attention to problematic gateways, and are displayed in SmartView Monitor. These alerts are sent:

- If certain rules or attributes, which are set to be tracked as alerts, are matched by a passing connection,
- If system events, also called System Alerts, are configured to trigger an alert when various predefined thresholds are surpassed.

The administrator can define alerts to be sent for different gateways. These alerts are sent under certain conditions, for example, if they have been defined for certain policies, or if they have been set for different properties. By default an alert is sent as a pop-up message to the administrator's desktop when a new alert arrives to SmartView Monitor.

Alerts can also be sent for certain predefined system events. If certain predefined conditions are set, you can get an alert for certain critical situation updates. These are called System Alerts. For example, if free disk space is less than 10%, or if a security policy has been changed. System Alerts are characterized as follows:

- Defined per product: For instance, you may define certain System Alerts for Unified Package and other System Alerts for Check Point QoS.
- Global or per gateway: This means that you can set global alert parameters for all gateways in the system, or you can specify a particular action to be taken on alert on the level of every Check Point gateway.
- Displayed and viewed via the same user-friendly window.
SNMP Monitoring Thresholds

This release lets you configure a variety of SNMP Thresholds that generate SNMP traps, or alerts. You can use the thresholds to monitor many system components automatically without requesting information from each object or device. The categories of thresholds that you can configure include:

- Hardware
- High Availability
- Networking
- Resources
- Log Server Connectivity

Some categories apply only to some machines or deployments.

In each category are many individual thresholds that you can set. For example, the hardware category includes alerts for the state of the RAID disk, the state of the temperature sensor, the state of the fan speed sensor, and others. For each individual threshold, you can configure:

- If it is enabled or disabled
- How frequently alerts are sent
- The severity of the alert
- The threshold point (if necessary)
- Where the alerts are sent to

You can also configure some settings globally, such as how often alerts are send and where they are sent to.

Types of Alerts

There are two different types of alerts:

- **Active alerts** are sent when a threshold point is passed or the status of a monitored component is problematic.
- **Clear alerts** are sent when the problem is resolved and the component has returned to its normal value. Clear alerts look like active alerts but the severity is set to 0.

Configuring SNMP Monitoring

Configure the SNMP monitoring thresholds in the command line of the Security Management server. When you install the policy on the gateways the SNMP monitoring thresholds are applied globally to all gateways.

Configuring in Multi-Domain Security Management

In a Multi-Domain Security Management environment, you can configure thresholds on the Multi-Domain Server and on each individual Domain Management Server. Thresholds that you configure on the Multi-Domain Server are for the Multi-Domain Server only. Thresholds that you configure for a Domain Management Server are for that Domain Management Server and its gateways. If a threshold applies to the Multi-Domain Server and the Domain Management Server gateways, set it on the Multi-Domain Server and Domain Management Server. However, in this situation you might only get alerts from the Multi-Domain Server if the threshold is passed.

For example, because the Multi-Domain Server and Domain Management Server are on the same machine, if the CPU threshold is passed, it applies to both of them. However, only the Multi-Domain Server generates alerts.

You can see the **Multi-Domain Security Management level** for each threshold with the `threshold_config` utility.

- If the Multi-Domain Security Management level for a threshold is **Multi-Domain Server**, alerts are generated for the Multi-Domain Server when the threshold point is passed.
• If the Multi-Domain Security Management level for a threshold is **Multi-Domain Server, Domain Management Server**, alerts are generated for the Multi-Domain Server and Domain Management Servers separately when the threshold point is passed.

### Configuring a Local Gateway Policy

You can configure SNMP thresholds locally on a gateway with the same procedure that you do on a Security Management server. However, each time you install a policy on the gateway, the local settings are erased and it reverts to the global SNMP threshold settings.

You can use the `threshold_config` utility to save the configuration file and load it again later. Or you can manually back up the configuration file so that you can copy the configuration to the gateway again after you install the policy.

On SecurePlatform and Linux, the configuration file that you can back up is:

```bash
$FWDIR/conf/thresholds.conf
```

On Windows the configuration file that you can back up is:

```bash
%FWDIR%\conf\thresholds.conf
```

### Configuration Procedures

There is one primary command to configure the thresholds in the command line, `threshold_config`. You must be in expert mode to run it. After you run `threshold_config`, follow the on-screen instructions to make selections and configure the global settings and each threshold.

When you run `threshold_config`, you get these options:

- **Show policy name** - Shows you the name configured for the threshold policy.
- **Set policy name** - Lets you set a name for the threshold policy.
- **Save policy** - Lets you save the policy.
- **Save policy to file** - Lets you export the policy to a file.
- **Load policy from file** - Lets you import a threshold policy from a file.
- **Configure global alert settings** - Lets you configure global settings for how frequently alerts are sent and how many alerts are sent.
- **Configure alert destinations** - Lets you configure a location or locations where the SNMP alerts are sent.
- **View thresholds overview** - Shows a list of all thresholds that you can set including: The category of the threshold, if it is active or disabled, the threshold point (if relevant), and a short description of what it monitors.
- **Configure thresholds** - Open the list of threshold categories to let you select thresholds to configure.

#### Configure Global Alert Settings

If you select **Configure global alert settings**, you can configure global settings for how frequently alerts are sent and how many alerts are sent. You can also configure these settings for each threshold. If a threshold does not have its own alert settings, it uses the global settings by default.

You can configure these options:

- **Enter Alert Repetitions** - How many alerts will be sent when an active alert is triggered. If you enter 0, alerts will be sent until the problem is fixed.
- **Enter Alert Repetitions Delay** - How long the system waits between sending active alerts.
- **Enter Clear Alert Repetitions** - How many clear alerts will be sent after a threshold returns to a normal value.
- **Enter Clear Alert Repetitions Delay** - How long the system waits between sending clear alerts.

#### Configure Alert Destinations

If you select Configure Alert Destinations, you can add and remove destinations for where the alerts are sent. You can also see a list of the configured destinations. A destination is usually an NMS (Network Management System) or a Check Point log server.
After entering the details for a destination, the CLI asks if the destination should apply to all thresholds.

- If you enter **yes**, alerts for all thresholds are sent to that destination, unless you remove the destination from an individual threshold.

- If you enter **no**, no alerts are sent to that destination by default. However, for each individual threshold, you can configure the destinations and you can add destinations that were not applied to all thresholds.

For each threshold, you can choose to which of the alert destinations its alerts are sent. If you do not define alert destination settings for a threshold, it sends alerts to all of the destinations that you applied to all thresholds.

For each alert destination enter:

- **Name** - An identifying name.
- **IP** - The IP address of the destination.
- **Port** - Through which port it is accessed.
- **Ver** - the version on SNMP that it uses
- **Other data** - Some versions of SNMP require more data. Enter the data that is supplied for that SNMP version.

**Configure Thresholds**

If you select Configure thresholds, you see a list of the categories of thresholds, including:

- Hardware
- High Availability
- Networking
- Resources
- Log Server Connectivity

Some categories apply only to some machines or deployments. For example, Hardware applies only to Check Point appliances and High Availability applies only to clusters or high availability deployments.

Select a category to see the thresholds in it. Each threshold can have these options:

- **Enable/Disable Threshold** - If the threshold is enabled, the system sends alerts when there is a problem. If it is disabled it does not generate alerts.

- **Set Severity** - You can give each threshold a severity setting. The options are: Low, Medium, High, and Critical. The severity level shows in the alerts and in SmartView Monitor and lets you know quickly how important the alert is.

- **Set Repetitions** - Set how frequently and how many alerts will be sent when the threshold is passed. If you do not configure this, it uses the global alert settings.

- **Set Threshold Point** - Enter the value that will cause active alerts when it is passed. Enter the number only, without a unit of measurement.

- **Configure Alert Destinations** - See all of the configured alert destinations. By default, active alerts and clear alerts are sent to the destinations. You can change this for each destination. Select the destination and you see these options:
  - **Remove from destinations** - If you select this, alerts for this threshold are not sent to the selected destination.
  - **Add a destination** - If you configured a destination in the global alert destinations but did not apply it to all thresholds, you can add it to the threshold.
  - **Disable clear alerts** - If you select this, clear alerts for this threshold are not sent to the selected destination. Active alerts are sent.

**Completing the Configuration**

To complete threshold configuration and activate the settings:

- On the Security Management server, install the policy on all gateways.
For a local gateway threshold policy or a Multi-Domain Security Management Multi-Domain Server environment, restart the CPD process using the cpwd_admin utility:

a) Run: cpwd_admin stop -name CPD -path "$CPDIR/bin/cpd_admin" -command "cpd_admin stop"

b) Run: cpwd_admin start -name CPD -path "$CPDIR/bin/cpd" -command "cpd"

Monitoring SNMP Thresholds

You can see an overview of the SNMP thresholds that you configure in SmartView Monitor.

To see an overview of the SNMP thresholds:
1. Open SmartView Monitor and select a gateway.
2. In the summary of the gateway data that open in the bottom pane, click System Information.
3. In the new pane that opens, click Thresholds.
4. In the pane that opens, you can see these details:

- **General Info** - A summary of the total SNMP Threshold policy.
  - **Policy name** - The name that you set for the policy in the CLI.
  - **State** - If the policy is enabled or disabled.
  - **Thresholds** - How many thresholds are enabled.
  - **Active events** - How many thresholds are currently sending alerts.
  - **Generated Events** - How many thresholds went from not active to active since the policy was installed.

- **Active Events** - Details for the thresholds that are currently sending alerts.
  - **Name** - The name of the alert (given in the CLI)
  - **Category** - The category of the alert (given in the CLI), for example, Hardware or Resources.
  - **MIB object** - The name of the object as recorded in the .mib file.
  - **MIB object's value** - The value of the object when the threshold became active, as recorded in the .mib file.
  - **State** - The current state of the object, either active or clearing (passed the threshold but is returning to normal value.
  - **Severity** - The severity of that threshold, as you configured for it in the CLI.
  - **Activation time** - When the alert was first sent.

- **Alert Destinations** - A list of the destinations that alerts are sent to.
  - **Name** - The name of the location.
  - **Type** - The type of location, for example, a log server or NMS.
  - **State** - If logs are being sent from the gateway or Security Management server to the destination machine.
  - **Alert Count** - How many alerts were sent to the destination from when the policy was started.

- **Errors** - Shows thresholds that cannot be monitored. For example, the gateway cannot monitor RAID sensors on a machine that does not have RAID sensors. Therefore it will show an error for the RAID Sensor Threshold.
  - **Threshold Name** - The name of the threshold with an error.
  - **Error** - A description of the error.
  - **Time of Error** - When the error first occurred.

Configuring Gateway Views

The following pages contain a number of different sets of steps that will instruct you on how to work with SmartView Monitor Gateway Status views.

To obtain an explicit understanding about the fields, text boxes, drop-down lists, etc., in each window refer to SmartView Monitor Online Help.
Defining Status Fetch Frequency

Define the frequency at which status information will be gathered by the Security Management server from the Check Point gateways and sent to SmartView Monitor. This is referred to as the Status Fetching Interval, and it is defined in SmartDashboard > Global Properties > Log and Alert > Time Settings window. By default a status check takes place every 60 seconds.

Start/Stop Cluster Member

Select a specific Cluster Member of a given Gateway Cluster in the Gateways Status view. Right-click the Cluster Member and select Cluster Member > Start Member or Stop Member respectively.

Select and Run a Gateways View

When a Gateways Status view is run the results appear in the SmartView Monitor client. A Gateways Status view can be run:

- from an existing view
- by creating a new view
- by changing an existing view

In the SmartView Monitor client, click on an existing Gateways Status view. The view results (that is, a list of all the available gateways) appears in the Results View.

Refresh a Gateways Status View

The Gateways Status view is automatically refreshed every 60 seconds. To refresh the view earlier select the specific view in the Tree View, right-click and select Run.

To refresh information about a specific gateway in the currently running Gateways Status view, right-click the specific gateway line and select Refresh.

Run a Specific View at Startup

With SmartView Monitor you can select the view that will first appear when you launch SmartView Monitor.

1. Right-click the view that should be run as soon as SmartView Monitor is launched.
2. Select Run at Startup.
Chapter 4

Monitoring Tunnels

In This Chapter

Tunnels Solution 29
Tunnel View Configuration 30

Tunnels Solution

VPN Tunnels are secure links between Security Gateways and ensure secure connections between an organization’s gateways and remote access clients.

Once Tunnels are created and put to use, you are able to keep track of their normal function, so that possible malfunctions and connectivity problems can be accessed and solved as soon as possible.

To ensure this security level, SmartView Monitor can recognize malfunctions and connectivity problems by constantly monitoring and analyzing the status of an organizations Tunnels. With the use of Tunnel views, you can generate fully detailed reports that include information about all the Tunnels that fulfill the specific Tunnel views conditions. With this information it is possible to monitor Tunnel status, the Community with which a Tunnel is associated, the gateways to which the Tunnel is connected, etc. The following represent the two Tunnel types:

- A Regular tunnel refers to the ability to send encrypted data between two peers. The Regular tunnel is considered "up" if both peers have Phase 1 and Phase 2 keys.
- Permanent tunnels are constantly kept active and as a result it is easier to recognize malfunctions and connectivity problems. With Permanent tunnels administrators can monitor the two sides of a VPN tunnel and identify problems without delay.

Each VPN tunnel in the community can be set as a Permanent tunnel. Since Permanent tunnels are constantly monitored. A log, alert, or user defined action can be issued when the VPN tunnel is down. Permanent tunnels can only be established between Check Point gateways. The configuration of Permanent tunnels takes place on the community level and:

- can be specified for an entire community. This option sets every VPN tunnel in the community as permanent.
- can be specified for a specific gateway. Use this option to configure specific gateways to have Permanent tunnels.
- can be specified for a single VPN tunnel. This feature allows configuring specific tunnels between specific gateways as permanent.

The following table explains the possible Tunnel states and their significance to a Permanent or Regular Tunnel.

Table 4-1 Tunnel Monitoring States

<table>
<thead>
<tr>
<th>State</th>
<th>Permanent Tunnel</th>
<th>Regular Tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up</td>
<td>The tunnel is functioning and the data can flow with no problems.</td>
<td>Both IDE SA (Phase 1) and IPSEC SA (Phase 2) exist with a peer gateway.</td>
</tr>
<tr>
<td>Destroyed</td>
<td>The tunnel is destroyed.</td>
<td>The tunnel is destroyed.</td>
</tr>
<tr>
<td>Up Phase1</td>
<td>Not relevant</td>
<td>Tunnel initialization is in process and Phase 1 is complete (that is, IKE SA exists with cookies), but there is no Phase 2.</td>
</tr>
<tr>
<td>State</td>
<td>Permanent Tunnel</td>
<td>Regular Tunnel</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Down</td>
<td>There is a tunnel failure. You cannot send and receive data to or from a remote peer.</td>
<td>Not relevant.</td>
</tr>
<tr>
<td>Up Init</td>
<td>The tunnel is being initialized.</td>
<td>Not relevant.</td>
</tr>
<tr>
<td>Gateway not Responding</td>
<td>The gateway is not responding.</td>
<td>The gateway is not responding.</td>
</tr>
</tbody>
</table>

### Tunnel View Configuration

The following pages contain a number of different sets of steps that will instruct you on how to work with SmartView Monitor Tunnel views.

**Note** - If a Tunnel is deleted from SmartDashboard, the Tunnel Results View contains the deleted Tunnel for an hour after it was deleted. Likewise, if a community is edited (that is, Tunnels are removed or added), the Results View will contain the deleted communities tunnels for one hour after they were deleted.

To obtain an explicit understanding about the fields, text boxes, drop-down lists, etc., in each window refer to SmartView Monitor Online Help.

**Run a Tunnel View**

When a Tunnel view is run the results appear in the SmartView Monitor client. A Tunnel view can be run:

- from an existing view
- by creating a new view
- by changing an existing view

A Tunnels view can be created and run for

- Down Permanent Tunnels
- Permanent Tunnels
- Tunnels on Community
- Tunnels on Gateway

**Run a Down Tunnel View**

Down Tunnel view results list all the Tunnels that are currently not active.

1. In the SmartView Monitor client, click the Tunnels branch in the Tree View.
2. In the Tunnels branch, (Custom or Predefined) double-click the Down Permanent Tunnel view.
   A list of all the Down Tunnels associated with the selected view's properties appears.

**Run a Permanent Tunnel View**

Permanent Tunnel view results list all the existing Permanent Tunnels and their current status.

A Permanent Tunnel is a Tunnel that is constantly kept active.

1. In the SmartView Monitor client, click the Tunnels branch in the Tree View.
2. In the Tunnels branch, double click the or Custom Permanent Tunnel view that you would like to run.
   A list of all the Permanent Tunnels associated with the selected view's properties appears.

**Run a Tunnels on Community View**

Tunnels on Community view results list all the Tunnels associated with a selected Community.
1. In the SmartView Monitor client, click the **Tunnels** branch in the **Tree View**.
2. In the **Tunnels** branch (Custom or Predefined), double-click the **Tunnels on Community** view.
   A list of all Communities appears.
3. Select the Community whose **Tunnels** you would like to monitor.
4. Select **OK**.
   A list of all the **Tunnels** associated with the selected Community appears.

### Run a Tunnels on Gateway View

**Tunnels on Gateway** view results list all the **Tunnels** associated with a selected Gateway.

1. In the SmartView Monitor client, click the **Tunnels** branch in the **Tree View**.
2. In the **Tunnels** branch (Custom or Predefined) double-click the **Tunnels on Gateway** view.
   A list of all the gateways appears.
3. Select the gateway whose **Tunnels** and their status you would like to see.
4. Select **OK**.
   A list of all the **Tunnels** associated with the selected gateway appears.

### Refresh a Tunnel View

Once a **Tunnel** view is run the information that appears is related to the time at which the view was run. To see current information about the **Tunnel** view running you must refresh the view.

To refresh the entire **Tunnel** view select the specific view in the **Tree View**, right-click and select **Run**.

To refresh information about a specific gateway in the currently running **Tunnel** view, right-click the specific gateway line and select **Refresh**.

### Run a Specific View at Startup

With SmartView Monitor you can select the view that will first appear when you launch SmartView Monitor.

1. Right-click the view that should be run as soon as SmartView Monitor is launched.
2. Select **Run at Startup**.

### Create a Custom Tunnel View

1. In the SmartView Monitor client, select **File > New > Tunnels View**.
   The **Query Properties** window appears.
2. Select **Prompt on** to generate a report about a specific Tunnel, Community or Gateway. Do not select **Prompt on** if your view is not specifically about one these three.
   **Prompt on** signifies that you will be asked for the specific Tunnel, Community or Gateway on which to base your view, as soon as you decide to run the view.
3. Select either **Show one record per tunnel** or **Show two records per tunnel**.
   By selecting **Show two records per tunnel** a more accurate status is displayed since the report will provide the status for the tunnels in both directions.
4. In the **Show** column, select the filter that should be associated with this view
5. In the **Filter** column edit the selected filters by clicking the corresponding Any(*) link and selecting the relevant objects.
6. Click the **Advanced** button and set a limit in the **Records limitation** window for the number of lines displayed in the report that will appear.
7. Enter a record limitation and click **OK**.
8. Click **OK**.
   A **Tunnels** view appears in the **Custom** branch of the **Tree View**.
9. Type the name of the new **Tunnel** view and press **Enter**.

### Edit a Custom Tunnel View

1. In the SmartView Monitor client, click the **Custom** branch in the **Tree View**.
2. In the **Custom** branch, select the **Tunnel** view whose settings you would like to change.
3. Select the **Query Properties** button in the view's toolbar.
4. Make the necessary changes with the options provided and click **OK**.
5. Click the **Save to Tree** button on the toolbar and enter a new name.
6. Click **Save**.
7. When you are asked to replace the specific view click **Yes** so that the new properties are saved.
   The changes are saved automatically.

**Edit a Tunnel View**

You cannot change a view in the branch **Tree View**. Therefore, when you change a view's properties you will need to save the view in the **Custom** branch of the **Tree View** in order to preserve those changes.

1. In the SmartView Monitor client, click the **Tunnels** icon in the **Tree View**.
2. Select the view whose settings you would like to change.
3. Click the **Query Properties** button in the toolbar provided.
4. Make the necessary changes in the tabs provided and click **OK**.
5. Click the **Save to Tree** button in the toolbar provided.
6. Enter a name for the new view and click **OK**.
   The changes will be preserved in a new view in the **Custom** branch of the **Tree View**.

**Delete a Custom Tunnel View**

1. In the SmartView Monitor client, click the **Custom** branch in the **Tree View**.
2. In the **Custom** branch of the **Tree View** select the **Tunnels** view you would like to delete.
3. Right click the selected view and select **Delete**.
4. Select **Yes** to delete the selected **Tunnels** view.

**Copy a Tunnel View**

1. In the SmartView Monitor client, click the **Tunnels** view (that is, **Custom** or **Predefined**) in the **Tree View**.
2. Right click the selected view and select **Copy**.
3. Right click the **Custom** branch of the **Tree View** and select **Paste**.
   A copy of the **Custom** view appears under the **Custom** branch.

**Rename a Custom Tunnel View**

1. In the SmartView Monitor client, click the **Custom** branch of the **Tree View**.
2. Right click the **Tunnels** view whose name you would like to change.
3. Select **Rename**.
4. Type the new name and press **Enter**.

**View In-Depth Information about a Specific Gateway**

1. Run the **Gateways Status** view for which you would like to view information.
2. Right-click the specific gateway in the **Results View**.
3. Right-click the specific gateway and select **Gateway Details**.
   The window that appears provides you with information about system performance, licenses, High Availability, etc., for the selected gateway.

**Create a Custom Gateways Status View**

1. In the SmartView Monitor client, select **File > New > Gateways View**.
   The **Gateway Properties > Fields** window appears.
2. Select the topics for which you would like to receive information in the **Available fields** list and move them to the **Show these fields in the grid** list.
3. Select the **Filter Gateways** tab to remove gateways from the specific **Gateways Status** view results.
4. Click **OK**.
   The results of the view appear in the SmartView Monitor console.
5. The specific **Gateways Status** view appears in the **Custom** branch of the **Tree View**. Right-click the view and type the name of the custom **Gateways Status** view.
Edit a Gateway View

The changes you make to an existing view cannot be saved. To save the changes you must perform Save To Tree and subsequently create a new view.

1. In the Custom branch of the Tree View select the Gateways Status view that you would like to change.
2. Click the View Properties button in the toolbar directly above the Results View.
3. Make the required changes by adding or removing topics from the Show these fields in the grid list.
4. Click OK.

The results of the view appear in the SmartView Monitor console.
5. To save the results of the view that has been changed, select the Save to Tree button in the toolbar directly above the Results View.
6. Enter a name for the new Gateways Status view and click Save.

The edited Gateways Status view will appear as a new view in the Custom branch of the Tree View.

Defining a Threshold

1. In the Tree View run a Gateways Status view.
2. Select the gateway for which you would like to change one or more thresholds.
3. Right-click and select Configure Thresholds.
4. You have the option of selecting one of the following:
   • Use global settings applies the global threshold settings to the selected gateway.
   • Custom enables you to select specific thresholds for the selected gateway.
   • None removes all thresholds from the selected gateway.
5. Select the Software Blade whose threshold you would like to change and make the necessary changes with the fields provided.

The Action column provides you with the following options:
   • none does not send an alert.
   • log sends a log entry to the database.
   • alert sends a pop window to your desktop.
   • mail sends a mail alert to your inbox.
   • snmptrap sends an SNMP alert.
   • useralert sends a customized alert in the manner that you configure.

Note - To configure these Action options go to SmartDashboard > Policy > Global Properties > Log and Alert > Alert Commands.

6. Click the Ok button to save your changes.

Define Global Threshold Settings

1. In the Tree View run a Gateways Status view.
2. Select the gateway for which you would like to change one or more thresholds.
3. Right-click and select Configure Thresholds.
4. Click the Edit Global Settings button.
5. Select the Software Blade whose threshold you would like to change and make the necessary changes with the fields provided.
6. Click OK to save your changes.

Delete a Custom Gateway View

1. In the Custom branch of the Tree View select the Gateways view you would like to delete.
2. Right click the selected view and select Delete.
3. Select Yes to delete the selected Custom view.
Copy a Gateway View
1. In the Tree View right-click the Gateways Status view you would like to copy.
2. Select Copy.
   The Save To Tree window appears.
3. Enter a name for the copy you are creating.
   A copy of the view appears under the Custom branch.

Rename a Custom Gateway Status View
1. In the Custom branch of the Tree View right-click the Gateways view whose name you would like to change.
2. Select Rename.
3. Type the new name and press Enter.

Export a Custom Gateway Status View
1. Right-click the Gateways view you would like to export.
2. Select Export Properties.
3. Select the directory in which you would like to save the exported view settings and click Save. A file with an svm_setting extension is created.
Chapter 5

Monitoring Traffic or System Counters

In This Chapter

Traffic or System Counters Solution 35
Traffic or System Counters Configuration 36

Traffic or System Counters Solution

SmartView Monitor provides you with the tools that enable you to be aware of traffic associated with specific network activities, servers, clients, etc., and the status of activities, hardware and software usage of different Check Point products in real-time. Among other things, this knowledge will enable you to:

- Block specific traffic when a threat is imposed
- Assume instant control of traffic flow on a gateway
- Learn about how many tunnels are currently opened or about the rate of new connections passing through the VPN gateway.

SmartView Monitor delivers a comprehensive solution for monitoring and analyzing network traffic and network usage. You can generate fully detailed or summarized graphs and charts for all connections intercepted and logged when monitoring traffic and for numerous rates and figures when counting usage throughout the network.

Traffic

Traffic Monitoring provides in-depth details on network traffic and activity. As a network administrator you can generate traffic information to:

- Analyze network traffic patterns
  Network traffic patterns help administrators determine which services demand the most network resources.
- Audit and estimate costs of network use
  Monitoring traffic can provide information on how the use of network resources is divided among corporate users and departments. Reports summarizing customer use of services, bandwidth and time can provide a basis for estimating costs per user or department.
- Identify the departments and users that generate the most traffic and the times of peak activity.
- Detect and monitor suspicious activity. Network administrators can produce graphs and charts documenting blocked traffic, alerts, rejected connections, or failed authentication attempts in order to identify possible intrusion attempts.

A Traffic view can be created to monitor the Traffic types listed in the following table.
Table 5-2 Traffic Types

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services</td>
<td>Displays the current status view about Services used through the selected gateway.</td>
</tr>
<tr>
<td>IPs/Network Objects</td>
<td>Displays the current status view about active IPs/Network Objects through the selected gateway.</td>
</tr>
<tr>
<td>Security Rules</td>
<td>Displays the current status view about the most frequently used Firewall rules. The Name column in the legend states the rule number as previously configured in SmartDashboard.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Displays the current status view about the Interfaces associated with the selected gateway.</td>
</tr>
<tr>
<td>Connections</td>
<td>Displays the current status view about current connections initiated through the selected gateway.</td>
</tr>
<tr>
<td>Tunnels</td>
<td>Displays the current status view about the Tunnels associated with the selected gateway and their usage.</td>
</tr>
<tr>
<td>Virtual Link</td>
<td>Displays the current traffic status view between two gateways (for example, Bandwidth, Bandwidth Loss and Round Trip Time).</td>
</tr>
<tr>
<td>Packet Size Distribution</td>
<td>Displays the current status view about packets according to the size of the packets.</td>
</tr>
<tr>
<td>QoS</td>
<td>Displays the current traffic level for each QoS rule.</td>
</tr>
</tbody>
</table>

Traffic Legend Output

The values that you see in the legend depend on the Traffic view you are running.

All units in the view results appear in configurable Intervals.

System Counters

Monitoring System Counters provides in-depth details about Check Point Software Blade usage and activities. As a network administrator you can generate system status information about:

- Resource usage for the variety of components associated with the gateway. For example, the average use of real physical memory, the average percent of CPU time used by user applications, free disk space, etc.

- Gateway performance statistics for a variety of firewall components. For example, the average number of concurrent CVP sessions handled by the HTTP security server, the number of concurrent IKE negotiations, the number of new sessions handled by the SMTP security server, etc.

- Detect and monitor suspicious activity. Network administrators can produce graphs and charts documenting the number of alerts, rejected connections, or failed authentication attempts in order to identify possible intrusion attempts.

Traffic or System Counters Configuration

The following pages contain a number of different sets of steps that will instruct you on how to configure Traffic or System Counters views.
To obtain an explicit understanding about the fields, text boxes, drop-down lists, etc., in each window refer to SmartView Monitor Online Help.

**Select and Run a Traffic or System Counters View**

When a Traffic or System Counters view is run the results appear in the SmartView Monitor client. A Traffic or System Counter view can be run:

- from an existing view
- by creating a new view
- by changing an existing view

To run a Traffic or System Counters view:

1. In the SmartView Monitor client, select the Traffic or System Counter branch in the Tree View and double click the Traffic or System Counter view that you would like to run.
   
   A list of available gateways appears.
2. Select the gateway for which you would like to run the selected Traffic or System Counter view.
3. Click OK.
   
   The results of the selected view appear in the SmartView Monitor client.

**Run a Specific View at Startup**

With SmartView Monitor you can select the view that will first appear when you launch SmartView Monitor.

1. Right-click the view that should be run as soon as SmartView Monitor is launched.
2. Select Run at Startup.

**Create a New Traffic or System Counters Results View**

A View is the output that is displayed when changing an existing view. The new View is not automatically saved in the Custom branch of the Tree View.

For example purposes, we will create a real-time Traffic view for Services.

1. Double-click the view you would like to change and select the gateway for which you are creating the view.
2. Select the View Properties button on the view toolbar. The Query Properties window appears.
   
   Real-Time provides information about currently monitored traffic or system counters.
   
   Select History for previously logged information.
4. Select the topic about which you would like to create a Real-Time traffic view in the drop-down list provided. For example purposes select Services.
   
   Note - The remaining tabs in the Query Properties window change according to the type of view you are creating and the selection you made in the Real-Time drop-down list.
5. Select the Target of this Custom Traffic view.
   
   The Target is the gateway for which you would like to monitor traffic.
6. Click the Monitor by Services tab.
7. Select Specific Services and the Services for which you would like to create a custom Traffic view.
8. Click the Filter tab and make the relevant selections.
9. Click the Settings tab and make the relevant selections.
10. Click OK when you are done with your selections.
11. The Select Gateway/Interface window appears.
12. Select the gateway or interface for which you would like to create/run this new view.
13. Click the Save to Tree button on the toolbar and enter a name for the new view.
14. Click OK.
The new view is saved in the **Custom** branch.

### Create a Real-Time Custom Traffic or Counter View

1. In the SmartView Monitor client, click the **Custom** branch of the **Tree View**.
   For example purposes we will create a real-time Traffic view for **Services**.
2. Right click the **Custom** branch and select **New Traffic View**.
   The **Query Properties** window appears.
3. Select **Real-Time**.
   **Real-Time** provides information about currently monitored traffic or system counters.
4. Select the topic (for example purposes **Services**) about which you would like to create a **Real-Time** traffic view in the drop-down list provided.

   **Note** - The remaining tabs in the **Query Properties** window change according to the type of view you are creating and the selection you made in the **Real-Time** drop-down list.
5. Select the **Target** of this **Custom Traffic** view.
   The **Target** is the gateway or cluster for which you would like to monitor traffic.
6. Click the **Monitor by Services** tab.
7. Select the **Services** for which you would like to create a custom traffic view.
8. Click the **Filter** tab and make the relevant selections.
9. Click the **Settings** tab and make the relevant selections.
10. Click **Save**.
    The **Select Gateway/Interface** window appears.
11. Select the gateway or interface for which you would like to create this new view.
12. Click **OK**.
13. Type the name of the new **Custom** view in the **Custom** branch and press **Enter**.

### Create a History Traffic or Counter View

1. In the SmartView Monitor client, click the **Custom** branch of the **Tree View**.
   For example purposes we will create a real-time Traffic view for **Services**.
2. Right click the **Custom** branch and select **New Traffic View**.
   The **Query Properties** window appears.
3. Select **History** in the **Type** section.
   **History** provides information about previously monitored traffic or system counters.
4. Select the **Target** of this custom **Traffic or Counter** view.
   The **Target** is the gateway for which you would like to view previously monitored traffic.
5. Click the **Traffic History** tab or the **Counter** tab, depending on the type of view you are creating.
6. In the **Time Frame** drop-down list, select the period of time for which you would like to view previously monitored traffic or system counters.
7. In the **Select history report** list, select the topic for which you are interested in viewing previously monitored information.
8. Click **Save**.
    The **Select Gateway** window appears.
9. Select the gateway for which you would like to create this new view.
10. Click **OK**.
11. Type the name of the new **Custom** view in the **Custom** branch and press **Enter**.

### Edit a System Counter or Traffic View

You cannot change a view in the **Tree View**. Therefore, when you change a view's properties you will need to save the view in the **Custom** branch of the **Tree View** in order to preserve those changes.

1. In the SmartView Monitor client, click the **Traffic or Counter** view that you would like to edit.
Monitoring Traffic or System Counters

Edit a Custom Traffic or System Counter View
1. In the SmartView Monitor client, select the Custom branch of the Tree View.
2. Click the Traffic or Counter view that you would like to edit.
   The Select Gateway/Interface window appears.
3. Select the gateway or interface for which you would like to create this new view.
4. Click OK.
5. Click the View Properties button on the view specific toolbar.
   The Query Properties window appears.
6. Make the necessary changes in the tabs provided and click Ok to preserve your changes.
   The Select Gateway/Interface window appears.
7. Select the gateway for which you would like to create this new view.
8. Click OK.
9. Enter a name for the new Custom view in the Custom branch and press Enter.
   The new view is run and the changes to the selected view are saved in the Custom branch of the Tree View.

Copy a Traffic or System Counter View
1. In the SmartView Monitor client, right-click the Traffic or System Counters view you would like to copy.
2. Select Copy.
   The Save to Tree window appears.
3. Give the view a new name and click Save.
   A copy of the view appears under the Custom branch of the Tree View.

Rename a Custom Traffic or Counter View
1. In the SmartView Monitor client, select the Custom branch of the Tree View.
2. Right-click the Traffic or System Counters view you would like to rename.
3. Select Rename.
4. Type the new name and press Enter.

Delete a Custom Traffic or Counter View
1. In the SmartView Monitor client, select the Custom branch of the Tree View.
2. Right-click the Traffic or System Counters view you would like to delete.
3. Select Delete.
4. Select Yes to delete the selected Custom view.
**Export a Custom Traffic or Counter View**

1. In the SmartView Monitor client, right-click the **Traffic or System Counters** view you would like to export.
2. Select **Export Properties**.
3. Select the directory in which you would like to save the exported view settings and click **Save**. A file with an `svm_setting` extension is created.

**Recording a Traffic or Counter View**

When recording a **Traffic** or **Counter** view you are saving a record of the **Traffic** or **Counter** view results.

1. In the SmartView Monitor client, run the **Traffic** or **System Counters** view you would like to record. Refer to Select and Run a Traffic or System Counters View (on page 37) for additional information.
2. Select the **Traffic** menu and select **Recording > Record**. A **Save As** window appears.
3. Give the record a name and save it in the relevant directory.
4. Click **Save**.
   - The word **Recording** appears underneath the **Traffic** or **Counter** toolbar. The appearance of this word signifies that the view currently running is being recorded and saved.
5. To stop recording, open the **Traffic** menu and select **Recording > Stop**. A record of the view results is saved in the directory you selected in step 3 above.

**Play the Results of a Recorded Traffic or Counter View**

1. In the SmartView Monitor client, select **Traffic > Recording > Play**. The **Select Recorded File** window appears.
2. Access the directory in which the recorded file is kept and select the relevant record.
3. Click **Open**.
   - The results of the selected recorded view begin to run and the word **Playing** appears underneath the toolbar.

<i>Note</i> - The difference between **Play** and **Fast Play** in the **Recording** menu is that **Fast Play** runs the recorded view results at a faster rate.

**Pause or Stop the Results of a Recorded View that is Playing**

- To pause the record select **Traffic > Recording > Pause**. Click **Recording > Play** to resume playing the previously recorded **Traffic** or **Counter** view results.
- To stop the record select **Traffic > Recording > Stop**.
Chapter 6

Monitoring Suspicious Activity Rules

In This Chapter

The Need for Suspicious Activity Rules 41
Suspicious Activity Rules Solution 41
Configure Suspicious Activity Rules 41

The Need for Suspicious Activity Rules

The connection of enterprise and public networks is a great information security challenge, since connections that provide access to employees and customers can also act as an open doorway for those who want to attack the network and its applications.

Modern business needs require that information be easily accessed while at the same time it remains secure and private.

The fast changing network environment demands the ability to immediately react to a security problem without having to change the entire network's Firewall rule base (for example, you want to instantly block a specific user). All inbound and outbound network activity should be inspected and identified as suspicious when necessary (for instance, when network or system activity indicates that someone is attempting to break in).

Suspicious Activity Rules Solution

Suspicious Activity Rules is a utility integrated into SmartView Monitor that is used to modify access privileges upon detection of any suspicious network activity (for example, several attempts to gain unauthorized access).

The detection of suspicious activity is based on the creation of Suspicious Activity rules. Suspicious Activity rules are Firewall rules that enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced security policy. These rules, once set (usually with an expiration date), can be applied immediately without the need to perform an INSTALL POLICY operation (see the R75.40 Security Management Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12277) for additional information).

Configure Suspicious Activity Rules

To block traffic when a threat is imposed, SmartView Monitor offers the tools needed to create and manage suspicious activity rules. These rules are based on your knowledge of the network and enable you to instantly block suspicious connections during real-time.

Create a Suspicious Activity Rule

A Suspicious Activity rule can be created from scratch or directly from or Custom view results.

Create a Suspicious Activity Rule

1. Select the Tools menu and Suspicious Activity Rules.
2. Click the Add button. The Block Suspicious Activity window is displayed.
3. Select Apply On for all gateways or for a specific gateway.
4. In the Source section select Any to define blockage of all source machines or indicate a specific IP Address or Network.
   If you would like to indicate a specific network source, define both the source machine’s IP and its Network Mask.
5. In the Destination section select Any to define the blockage of all destination machines or define a specific IP address.
   If you would like to indicate a specific network destination, define both the destination machine’s IP and its Network Mask.
6. In the Service section select Any for blocking all services or define a specific service that you wish to block.
7. In the Expiration section select a Relative time at which this rule should expire or define an Absolute Date and Time of expiration.
8. Click the Advanced button to decide how SmartView Monitor will react to behavior that applies to this rule.
   The Advanced window is displayed.
   a) Select either Drop, Reject or Notify in the Action drop-down list.
      - Notify indicates that a notification about the defined activity will be sent but the activity will not be blocked.
      - Drop indicates that packets will be dropped without sending the communicating peer a notification.
      - Reject indicates that packets will be rejected along with a notification to the communicating peer that the packet has been rejected.
   b) Select No Log, Log or Alert in the Track drop-down list.
   c) Check Close Connections to close all active connections matching this rule.
9. Click OK to return to the Block Suspicious Activity window.
10. Click Enforce to save and execute this rule.

Create a Suspicious Activity Rule Based on the Results
When running a Traffic view you can create a Suspicious Activity rule from the results that appear on the SmartView Monitor client.
You can only create a Suspicious Activity rule for Traffic views that contain information about the Source and/or Destination (for example, Top Sources, Top P2P Users, etc.).
1. In the SmartView Monitor client, click Traffic in the Tree View.
2. In the Traffic view tree, double click the view that you would like to run.
   A list of available gateways and clusters appears.
3. Select the gateway for which you would like to run the selected Traffic view.
4. Click OK.
   The results of the selected view appear in the SmartView Monitor client.
5. In the area of the screen in which the results appear, right click the Service, Network Object, Tunnel, etc., that you would like to block.
6. Select Block Source.
   The Block Suspicious Activity window is displayed containing all of the settings associated with the selected view results.
7. Modify any or none of the settings that appear.
8. Click Enforce to save and execute this rule.
Manage Suspicious Activity Rules

The Enforced Suspicious Activity Rules window provides a display of the currently enforced rules. If a rule that conflicts with another rule is added, the conflicting rule remains hidden. For example, if a rule was defined for dropping all http traffic and an additional rule is defined for rejecting http traffic, only the dropped rule, which is the dominant rule, will be displayed.

Once one or more Suspicious Activity rules are created SmartView Monitor enables you to:

- View the rules that are currently being enforced on a gateway or on all the gateways.
- Remove or add new rules.

Note - To add a new Suspicious Activity rule refer to Create a Suspicious Activity Rule (on page 41).

View a Suspicious Activity Rule

1. In SmartView Monitor, click Traffic or System Counters in the Tree View.
2. Select the Tools menu and Suspicious Activity Rules.
   The Enforced Suspicious Activity Rules window is displayed.
3. Select Apply on All to view all the Suspicious Activity rules or Show On to view rules associated with a specific gateway or cluster.

Remove a Suspicious Activity Rule

1. In the SmartView Monitor client, click Traffic or System Counters in the Tree View.
2. Select the Tools menu and Suspicious Activity Rules.
   The Enforced Suspicious Activity Rules window is displayed.
3. Select Apply on All to view all the Suspicious Activity rules or Show On to view rules associated with a specific gateway or cluster.
4. Select the rule that you would like to remove from the Enforced Suspicious Activity Rules window.
5. Click Remove.
6. Click Yes to remove the rule.
Chapter 7

Monitoring Users

In This Chapter

Users Solution 44
Users View Configuration 44

Users Solution

The User Monitor is an administrative feature allowing you to keep track of Endpoint Connect users currently logged on to the specific Security Management servers. The User Monitor provides you with a comprehensive set of filters which makes the view definition process user-friendly and highly efficient and enables you to easily navigate through the obtained results.

With information about current open sessions, overlapping sessions, route traffic, connection time, etc., the User Monitor is able to provide detailed information about remote users’ connectivity experience. This SmartView Monitor feature enables you to view real-time and historical statistics about open remote access sessions.

Users View Configuration

The following pages contain a number of different sets of steps that will instruct you on how to work with SmartView Monitor Users views.

If specific view results information is not relevant for a particular User, the column representing the information will show N/A for the User.

To obtain an explicit understanding about the fields, text boxes, drop-down lists, etc., in each window refer to SmartView Monitor Online Help.

Run a Users View

When a Users view is run, the results appear in the SmartView Monitor client:

- from an existing view
- by creating a new view
- by changing an existing view

A Users view can be created and run for:

- a specific user
- all users
- a specific gateway
- Mobile Access user

Run a User View for a Specific User

1. In SmartView Monitor, click Users in the Tree View.
2. In the Users branch, click Get User by Name.
   The User DN Filter window appears.
3. Enter the specific User DN in the area provided and click OK.
   The view results appear in the Results View.

Run a User View for all Users or Mobile Access Users
1. In SmartView Monitor, click Users in the Tree View.
2. In the Users branch, click All Users or Mobile Access Users.
   The view results appear in the Results View.

Run a User View for a Specific Gateway
1. In SmartView Monitor, click Users in the Tree View.
2. In the Users branch, click Users by Gateway.
   The Select Gateway window appears.
3. Select the gateway for which you would like to run the view and click OK.
   The view results appear in the Results View.

Refresh a Users View
Once a Users view is run the information that appears is related to the time at which the view was run. To see current information about the Users view running you must refresh the view.

To refresh the entire Users view select the specific view in the Tree View, right-click and select Run.

To refresh information about a specific gateway in the currently running Users view, right-click the specific gateway line and select Refresh.

Run a Specific View at Startup
With SmartView Monitor you can select the view that will first appear when you launch SmartView Monitor.
1. Right-click the view that should be run as soon as SmartView Monitor is launched.
2. Select Run at Startup.

Create a Custom Users View
1. In SmartView Monitor, select File > New > Users View.
   The Query Properties window appears.
2. Select Prompt on to generate a Users report about a specific User or Gateway. Do not select Prompt on if your view is not specifically about one these two.
   Prompt on signifies that you will be asked for the specific User DN or Gateway on which to base your view, as soon as you decide to run the view.
3. In the Show column, select the filter that should be associated with this view and in the Filter column edit the selected filters by clicking the corresponding Any(∗) link and selecting the relevant objects.
4. Click the Advanced button to set a limit (in the Records limitation window) to the number of lines displayed in the report that will appear.
5. Enter a record limitation and click OK.
6. Click OK.
   A Users view appears in the Custom branch of the Tree View.
7. Type a name for the new Users view and press Enter.

Edit a Custom Users View
1. In SmartView Monitor, click the Custom branch in the Tree View.
2. In the Custom branch, select the Users view whose settings you would like to change.
3. Select Query Properties from the toolbar.
4. Make the necessary changes in the tabs provided and click OK.
5. Click the **Save to Tree** button on the toolbar and click **Save**.
6. When you are asked to replace the specific view click **Yes** so that the new properties are saved.
   The changes are saved automatically.

**Edit a Users View**

You cannot change a view in the branch **Tree View**. Therefore, when you change a view's properties you will need to save the view in the **Custom** branch of the **Tree View** in order to preserve those changes.

1. In SmartView Monitor, click the **Users** branch in the **Tree View**.
2. Select the view whose settings you would like to change.
3. Click the **Query Properties** button in the toolbar provided.
4. Make the necessary changes in the tabs provided and click **OK**
5. Click the **Save to Tree** button in the toolbar provided.
6. Enter a name for the new view and click **OK**.
   The changes will be preserved in a new view in the **Custom** branch of the **Tree View**.

**Delete a Custom Users View**

1. In SmartView Monitor, click the **Custom** branch in the **Tree View**.
2. In the **Custom** branch of the **Tree View** select the **Users** view you would like to delete.
3. Right click the selected view and select **Delete**.
4. Select **Yes** to delete the selected **Users** view.

**Copy a Users View**

1. In SmartView Monitor, click the **Users** branch (that is, **Custom** or **Predefined**) in the **Tree View**.
2. Right click the selected view and select **Copy**.
3. The **Save to Tree** window appears.
4. Enter a new name for the view you are copying and click **Save**.
   A copy of the **Users** view appears under the **Custom** branch.

**Rename a Custom Users View**

1. In SmartView Monitor, click the **Custom** branch of the **Tree View**.
2. Right click the **Users** view whose name you would like to change.
3. Select **Rename**.
4. Type the new name and press **Enter**.
Chapter 8

Cooperative Enforcement

Cooperative Enforcement Solution

Cooperative Enforcement works with Check Point Endpoint Security servers. This feature utilizes the Endpoint Security server compliance capability to verify connections arriving from various hosts across the internal network.

Endpoint Security server is a centrally managed, multi-layered endpoint security solution that employs policy-based security enforcement for internal and remote PCs. Easily deployed and managed, the Endpoint Security server mitigates the risk of hackers, worms, spyware, and other security threats.

Features such as policy templates, an intuitive web-based management interface, and PC firewall and application privilege controls, enable administrators to develop, manage, and enforce Cooperative Enforcement quickly and easily.

Using Cooperative Enforcement, any host initiating a connection through a gateway is tested for compliance. This increases the integrity of the network because it prevents hosts with malicious software components from accessing the network.

This feature acts as a middle-man between hosts managed by an Endpoint Security server and the Endpoint Security server itself. It relies on the Endpoint Security server compliance feature, which defines whether a host is secure and can block connections that do not meet the defined prerequisites of software components.

The following is a typical Cooperative Enforcement workflow:

1. A host opens a connection to the network through a firewall gateway. The first packet from the client to the server is allowed. It is only on the first server's reply to the client that the Cooperative Enforcement feature begins to perform.
2. The firewall checks for host compliance in its tables and queries the Endpoint Security server, if required.
3. Upon receiving a reply, a connection from a compliant host is allowed, but if the Client is found to be non-compliant, the connection is closed unless this firewall feature is in Monitor-only mode.


Enforcement Mode

In this mode, a non-compliant host's connection is blocked by the firewall's Cooperative Enforcement feature. If it is an HTTP connection, the host will get a notification page indicating that it is not compliant. The user will be able to perform the appropriate actions in order to become compliant. For example, in order to become compliant the user may upgrade the version of the Endpoint Security client.
Monitor Only Deployment Mode

In the monitor only deployment mode, hosts can connect while the firewall gateway grants authorization status. In addition, the firewall generates logs for unauthorized hosts. The administrator can either add unauthorized hosts to the host's exception list or perform the appropriate operations to make those hosts compliant.

The logs generated for both authorized and unauthorized hosts can be viewed in SmartView Monitor.

Non-Compliant Hosts by Gateway View

The SmartView Monitor Non-Compliant Hosts by Gateway view enables you to distinguish between Host IPs that have one of the following Endpoint Security server compliances:

- **Authorized** enables access to the Internet. If a gateway has an Authorized status it will not appear in the SmartView Monitor Non-Compliant Hosts by Gateway view.
- **Unauthorized** obstructs access to the Internet.
- **No Endpoint Security client** indicates that the gateway is not associated with an Endpoint Security client.

In addition, the SmartView Monitor Non-Compliant Hosts by Gateway view provides information about Host IPs with one of the following modes:

- **Monitor Only** indicates that an Endpoint Security client will have access to the Internet whether or not it is authorized.
- **Blocked** mode obstructs access to the Internet.

The figure below illustrates Endpoint Security client access to the Internet in association with the Gateway and Endpoint Security server.

**Figure 8-8** Endpoint Security Access to the Internet

![Endpoint Security Access to the Internet Diagram]

**Configuring a Cooperative Enforcement View**

The following steps instruct you on how to run and read a Cooperative Enforcement view.

1. In the Tree View select **Cooperative Enforcement > Non-Compliant Hosts By Gateway**.
The Select Gateway window appears.

2. Select the gateway or cluster that you would like to review and select OK.
   The information appears in the Cooperative Enforcement Results view.

3. To refresh the view select the blue circular arrow on top of the Enforced On column.

The Cooperative Enforcement Results view contains the following information:

- **Enforced On** indicates the gateway associated with the information provided.
- **IP** indicates the specific gateway host.
- **Action** indicates the gateway mode (that is, Monitor Only or Blocked).
- **Reason** indicates the hosts Endpoint Security server compliance (that is, Unauthorized or No Endpoint Security client)
Run a Down Tunnel View • 30
Run a Permanent Tunnel View • 30
Run a Specific View at Startup • 28, 31, 37, 45
Run a Tunnel View • 30
Run a Tunnels on Community View • 30
Run a Tunnels on Gateway View • 31
Run a User View for a Specific Gateway • 45
Run a User View for a Specific User • 44
Run a User View for all Users or Mobile Access Users • 45
Run a Users View • 44

S
Select and Run a Gateways View • 28
Select and Run a Traffic or System Counters View • 37
SmartConsole Server • 21
SmartView Monitor Considerations • 7
SmartView Monitor Features • 6
SNMP Monitoring Thresholds • 24
Software Blade Status • 18
Start/Stop Cluster Member • 28
Suspicious Activity Rules Solution • 41
System Alert Monitoring Mechanism • 16
System Alerts • 15
System Counters • 36
System Counters View • 10
System Information • 19

T
Terminology • 7
The Need for Suspicious Activity Rules • 41
Thresholds • 23
Traffic • 35
Traffic Legend Output • 36
Traffic or System Counters Configuration • 36
Traffic or System Counters Solution • 35
Traffic View • 9
Tunnel View Configuration • 30
Tunnels Solution • 29
Tunnels View • 11
Types of Alerts • 24

U
Understanding the User Interface • 8
UserAuthority WebAccess • 21
Users Solution • 44
Users View • 12
Users View Configuration • 44

V
View a Suspicious Activity Rule • 43
View In-Depth Information about a Specific Gateway • 32
Viewing Alerts • 15
Views of a Specified Gateway • 22
Virtual Private Networks • 19