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=24848](http://supportcontent.checkpoint.com/documentation_download?ID=24848)

To learn more, visit the Check Point Support Center ([http://supportcenter.checkpoint.com](http://supportcenter.checkpoint.com)).

For more about this release, see the R77 home page ([http://supportcontent.checkpoint.com/solutions?id=sk97617](http://supportcontent.checkpoint.com/solutions?id=sk97617)).

**Revision History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>21 May 2014</td>
<td>Cover changed to be relevant for all R77 versions</td>
</tr>
<tr>
<td>20 August 2013</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

**Feedback**

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

Please help us by sending your comments ([mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on SmartView Monitor R77 Versions Administration Guide](mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on SmartView Monitor R77 Versions Administration Guide)).
Contents

Important Information ........................................................................................................ 3
Terms .................................................................................................................................... 7
Introducing SmartView Monitor ......................................................................................... 8
  SmartView Monitor Features .......................................................................................... 8
  Immediate Actions ......................................................................................................... 9
Understanding the User Interface ...................................................................................... 9
  Gateway Status View ..................................................................................................... 9
  Traffic View .................................................................................................................. 10
  System Counters View .................................................................................................. 11
  Tunnels View ................................................................................................................ 11
  Users View .................................................................................................................... 12
  Cooperative Enforcement View ..................................................................................... 12
  Setting Your Default View ............................................................................................. 13
  Refreshing Views .......................................................................................................... 13
Monitoring and Handling Alerts ......................................................................................... 14
  Alert Window ................................................................................................................ 14
  Viewing Alerts ............................................................................................................... 14
  System Alert Monitoring Mechanism ........................................................................... 15
Monitoring Suspicious Activity Rules .............................................................................. 15
  The Need for Suspicious Activity Rules .................................................................... 15
  Suspicious Activity Rules ............................................................................................ 15
  Creating a Suspicious Activity Rule ............................................................................ 15
  Creating a Suspicious Activity Rule from Results ....................................................... 16
  Managing Suspicious Activity Rules ......................................................................... 16
Configuring SmartView Monitor ....................................................................................... 17
  How SmartView Monitor Works .................................................................................. 17
  AMON ............................................................................................................................. 18
  Defining Status Fetch Frequency .................................................................................. 18
System Alerts and Thresholds ............................................................................................ 18
  Working with SNMP Monitoring Thresholds ............................................................... 19
  Types of Alerts ............................................................................................................. 20
  Configuring SNMP Monitoring .................................................................................... 20
  Configuration Procedures ............................................................................................ 21
  Monitoring SNMP Thresholds ...................................................................................... 22
  Customizing Results .................................................................................................... 23
  Editing a Custom View ................................................................................................. 23
  Custom View Example ................................................................................................. 25
  Exporting a Custom View ............................................................................................ 26
Monitoring Gateway Status ............................................................................................... 27
  Gateway Status ............................................................................................................ 27
  Displaying Gateway Data ............................................................................................. 27
  System Data .................................................................................................................. 27
  Firewall ......................................................................................................................... 28
  Virtual Private Networks ............................................................................................... 28
  QoS ................................................................................................................................. 29
  ClusterXL ....................................................................................................................... 29
  OPSEC ........................................................................................................................... 29
  Check Point Security Management .............................................................................. 29
  UserAuthority WebAccess ............................................................................................ 30
  SmartConsole Server .................................................................................................... 30
  Log Server .................................................................................................................... 30
  Correlation Unit and SmartEvent .................................................................................. 30
Anti-Virus and URL Filtering.......................................................................................... 31
Multi-Domain Security Management .......................................................................... 31
Starting and Stopping Cluster Members .................................................................... 31

Monitoring Tunnels ................................................................................................. 32
Tunnels Solution ........................................................................................................ 32
Tunnel View Updates ................................................................................................. 33
Running Tunnel Views ............................................................................................... 33
  Run a Down Tunnel View ....................................................................................... 33
  Run a Permanent Tunnel View .............................................................................. 33
  Run a Tunnels on Community View ..................................................................... 33
  Run a Tunnels on Gateway View .......................................................................... 34

Monitoring Traffic or System Counters .................................................................. 35
Traffic or System Counters Solution .......................................................................... 35
  Traffic .................................................................................................................. 35
  Traffic Legend Output ........................................................................................... 36
  System Counters .................................................................................................. 36
Select and Run a Traffic or System Counters View .................................................. 37
Recording a Traffic or Counter View ......................................................................... 37
  Play the Results of a Recorded Traffic or Counter View ..................................... 37
  Pause or Stop the Results of a Recorded View that is Playing ............................. 37

Monitoring Users ..................................................................................................... 38
Users Solution ............................................................................................................ 38
  Run a Users View .................................................................................................. 38
  Run a User View for a Specific User ..................................................................... 38
  Run a User View for all Users or Mobile Access Users ........................................ 38
  Run a User View for a Specific Gateway .............................................................. 39

Cooperative Enforcement ......................................................................................... 40
Cooperative Enforcement Solution ............................................................................. 40
  Enforcement Mode ............................................................................................... 40
  Monitor Only Deployment Mode .......................................................................... 40
  Non-Compliant Hosts by Gateway View .............................................................. 41
Running a Cooperative Enforcement View ............................................................... 41

Index ......................................................................................................................... 43
Terms

**Cluster**
Two or more Security Gateways connected to each other for High Availability and/or Load Sharing.

**Cluster Member**
A Security Gateway that is part of a cluster.

**Cooperative Enforcement**
Integration of Endpoint Security server Compliance to verify internal network connections.

**Remote Access VPN**
An encryption tunnel between a Security Gateway and remote access clients, such as Endpoint Security VPN, and communities.

**Security Cluster**
A cluster that has identical Check Point Security Gateway members for High Availability and Load Sharing.

**Security Gateway**
A computer or appliance that inspects traffic and enforces Security Policies for connected network resources.

**Security Management Server**
The application that manages, stores, and distributes the security policy to Security Gateways.

**Security Policy**
A collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources through the use of packet inspection.

**SmartConsole**
A Check Point GUI application used to manage security policies, monitor products and events, install updates, provision new computers and appliances, and manage a multi-domain environment.

**SmartDashboard**
A Check Point client used to create and manage the security policy.

**Software Blade**
A software blade is a security solution based on specific business needs, for example the need to protect against malware or viruses or prevent the loss of data. Each blade is independent, modular and centrally managed. To extend security, additional blades can be quickly added.

**System Counter**
SmartView Monitor data or report on status, activity, and resource usage of Check Point products.

**Traffic**
The flow of data between network resources.

**VPN**
Virtual Private Network. A secure, encrypted connection between networks and remote clients on a public infrastructure, to give authenticated remote users and sites secured access to an organization's network and resources.

**VPN Tunnel**
An encrypted connection between two hosts using standard protocols (such as L2TP) to encrypt traffic going in and decrypt it coming out, creating an encapsulated network through which data can be safely shared as though on a physical private line.

**Example**: A Route Based VPN tunnel works as a point-to-point connection between two peer Security Gateways in a VPN community.

**Term Type**: Industry
Chapter 1

Introducing SmartView Monitor

In This Section:

- SmartView Monitor Features ................................................................. 8
- Immediate Actions .................................................................................. 9
- Understanding the User Interface ............................................................ 9

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 Security Management Architecture, SmartView Monitor provides a single, central interface for monitoring network activity and performance of Check Point Software Blades.

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 graphical reports of monitored events can be generated to provide a comprehensive view of gateways, tunnels, remote users, network, security, and performance over time.

Examples of scenarios for which SmartView Monitor can help:

- 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.
Immediate Actions

If the status shows an issue, you can act on that network object. For example:

- **Disconnect client** - Disconnect one or more of the connected SmartConsole clients.
- **Start/Stop cluster member** - You can see all Cluster Members of a Gateway Cluster in SmartView Monitor. You can start or stop a selected Cluster Member.
- **Suspicious Action Rules** - You can block suspicious network activity while you investigate the real risk or to quickly block an obvious intruder. ("Monitoring Suspicious Activity Rules" on page 15)

Understanding the User Interface

The results you see in the SmartView Monitor SmartConsole depend on the view you select.

**Gateway Status View**

This view shows data about supported hosts.

1. **Tree** - Shows all the views.
2. **Toolbars** - Shortcuts of SmartView Monitor options.
3. **Results** - Data for all the gateways in the organization, and details for the selected gateway, linked to the view selected in the Tree. Each row in the table represents a Gateway.
4. **Gateway Details** - HTML view that behaves like a browser and allows the user to hit links associated data about the selected gateway.
5. There are tabs for every view that is currently running in SmartView Monitor. As the number of running views grows, they are added to a More tab, from which you can select a view.
Traffic View

This view shows transaction data for network sessions in a given time interval.

1. **Tree** - Shows all the views.
2. **Toolbars** - Shortcuts of SmartView Monitor options.
3. **Results** - Data for the selected view and property.
4. **Legend** - Textual report of the results.
5. **Status Bar** - (Bottom of the SmartConsole) System data for the gateway associated with the selected view.
6. There are tabs for every view that is currently running in SmartView Monitor. As the number of running views grows, they are added to a **More** tab, from which you can select a view.
**System Counters View**

This view shows reports on status, activities, and resource usage of Check Point products, in real-time or history mode.

1. **Tree** - Shows all the views.
2. **Toolbars** - Shortcuts of SmartView Monitor options.
3. **Results** - Data for the selected view and property.
4. **Legend** - Textual report of the results.
5. **Status Bar** - (Bottom of the SmartConsole) System data for the gateway associated with the selected view.
6. There are tabs for every view that is currently running in SmartView Monitor. As the number of running views grows, they are added to a **More** tab from which you can select a view.

**Tunnels View**

This view shows data on connections of site-to-site VPNs.

1. **Tree** - Shows all the views.
2. **Toolbars** - Shortcuts of SmartView Monitor options.
3. **Results** - Data for the selected view and object.
4. There are tabs for every view that is currently running in SmartView Monitor. As the number of running views grows, they are added to a **More** tab from which you can select a view.
**Users View**

This view shows data on remote access users and their connections to VPNs.

1. **Tree** - Shows all the views.
2. **Toolbars** - Shortcuts of SmartView Monitor options.
3. **Results** - Data for the selected view and object.
4. There are tabs for every view that is currently running in SmartView Monitor. As the number of running views grows, they are added to a *More* tab from which you can select a view.

**Cooperative Enforcement View**

This view shows data on internal hosts.

1. **Tree** - Shows all the views.
2. **Toolbars** - Shortcuts of SmartView Monitor options.
3. **Results** - Data for the selected view and object.
4. There are tabs for every view that is currently running in SmartView Monitor. As the number of running views grows, they are added to a *More* tab from which you can select a view.
**Setting Your Default View**

You can set which view to see when SmartView Monitor starts.
In the Tree, right-click the view and select **Run at Startup**.

**Refreshing Views**

Results are automatically refreshed every 60 seconds.
To refresh the view earlier, right-click the view name in the Tree and select **Run**.
To refresh data about an object in the currently running view, right-click the object in the results and select **Refresh**.
Chapter 2

Monitoring and Handling Alerts

In This Section:
- Alert Window ........................................... 14
- Viewing Alerts ........................................... 14
- System Alert Monitoring Mechanism .......................... 15
- Monitoring Suspicious Activity Rules .......................... 15

Alert Window

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.

Viewing Alerts

Alert commands are set in SmartDashboard > Global Properties > Log and Alert > Alerts page. The Alerts in this window apply only to Security Gateways.

To see alerts:

Click the Alerts icon in the toolbar. (Or in the main toolbar button sub-menu, select Tools > Alerts.)

The Alerts window opens. You can set alert attributes and delete displayed alerts.
System Alert Monitoring Mechanism

Check Point Security Management Server has a System Alert monitoring mechanism. It uses the System Alert thresholds you defined. If reached, it activates the defined action.

- To activate this mechanism: select Tools > Start System Alert Daemon.
- To stop the System Alert monitoring mechanism: select Tools > Stop System Alert Daemon.

Monitoring Suspicious Activity Rules

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

Suspicious Activity Monitoring (SAM) is a utility integrated in SmartView Monitor. It blocks activities that you see in the SmartView Monitor results and that appear to be suspicious. For example, you can block a user who tries several times to gain unauthorized access to a network or Internet resource.

A Security Gateway with SAM enabled has Firewall rules to block suspicious connections that are not restricted by the security policy. These rules are applied immediately (Install Policy not required).

Creating a Suspicious Activity Rule

SAM rules take some CPU resources, so set an expiration that gives you time to investigate but does not affect performance. Best practice is to keep only the SAM rules that you need. If you confirm that an activity is risky, edit the Security Policy, educate users, or otherwise handle the risk.

To block suspicious activity based on source, destination, or service:

1. Click the Suspicious Activity Rules button in the SmartView Monitor toolbar. The Enforced Suspicious Activity Rules window opens.
2. Click Add. The Block Suspicious Activity window opens.
3. In Source and in Destination, select IP or Network:
   - To block all sources or destinations that fit the other parameters, enter Any.
   - To block one suspicious source or destination, enter an IP Address and Network Mask.
4. In Service:
   - To block all connections that fit the other parameters, enter Any.
   - To block one suspicious service or protocol, click the button and select a service from the window that opens.
5. In Expiration, set your investigation time limit.
6. Click Enforce.
To create a Suspicious Activity rule based on TCP or UDP usage:
1. In the Block Suspicious Activity window > Service, click the button.
   The Select Service window opens.
2. Click Custom Service.
3. Select TCP or UDP.
4. Enter the port number.
5. Click OK.

To define SmartView Monitor actions on rule match:
1. In the Block Suspicious Activity window, click Advanced.
   The Advanced window opens.
2. In Action, select the Firewall action for SmartView Monitor to do on rule match:
   - Notify - Send a message about the activity, but do not block it.
   - Drop - Drop packets without sending a response. The connection will eventually time out.
   - Reject - Send an RST packet to the source and close the connection.
3. In Track, select No Log, Log or Alert.
4. If the action is Drop, and you want the connection to be closed immediately on rule match, select Close connections.
5. Click OK.

Creating a Suspicious Activity Rule from Results
If you are monitoring traffic, and see a suspicious result, you can create a SAM rule immediately from the results.

Note: You can only create a Suspicious Activity rule for Traffic views with data about the Source or Destination (Top Sources, Top P2P Users, and so on).
1. In SmartView Monitor open a Traffic view.
   The Select Gateway/Interface window opens.
2. Select an object and click OK.
3. In the Results, right-click the bar in the chart, or the row in the report, that represents the source, destination, service, or other traffic property that you want to block.
4. Select Block Source.
   The Block Suspicious Activity window opens.
5. Create the rule.
6. Click Enforce.

For example:
Your corporate policy does not allow peer2peer file sharing, and you see it in the Traffic > Top P2P Users results. You right-click the result bar and select Block Source. The SAM rule is set up automatically with the user IP address and the P2P_File_Sharing_Applications service. Click Enforce. For the next hour, while this traffic is dropped and logged, contact the user.

Managing Suspicious Activity Rules
The Enforced Suspicious Activity Rules window shows the currently enforced rules. If you add a rule that conflicts with another rule, the conflicting rule remains hidden. For example, if you define a rule to drop http traffic, and a rule exists to reject http traffic, only the drop rule shows.
Chapter 3

Configuring SmartView Monitor

In This Section:
- How SmartView Monitor Works ................................................................. 17
- System Alerts and Thresholds ................................................................. 18
- Working with SNMP Monitoring Thresholds ........................................... 19
- Customizing Results .................................................................................. 23

How SmartView Monitor Works

Data for the status of all gateways in the system is collected by the Security Management Server and viewed in SmartView Monitor. The data shows status for:

- Check Point Security Gateways
- OPSEC gateways
- Check Point Software Blades

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

Gateway Status is similar in operation to the SNMP daemon that also provides a mechanism to get data about gateways in the system.

SIC is initialized between Security Gateways (local and remote) and the Security Management Server. The Security Management Server then gets status data from the Software Blades with the AMON (Application Monitoring) protocol. SmartView Monitor gets the data from the Security Management Server.
**AMON**

The Security Management Server acts as an AMON client. It collects data about installed Software Blades. Each Security Gateway, or any other OPSEC gateway which runs an AMON server, acts as the AMON server itself. The gateway requests status updates from other components, such as the Firewall kernel and network servers. Requests are fetched at a defined interval.

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

The AMON protocol is SIC-based. It can collect data only after SIC is initialized.

**Defining Status Fetch Frequency**

The Security Management Server collects status data from the Security Gateways on a defined interval. The default is 60 seconds.

**To set the Status Fetching Interval:**
1. Open SmartDashboard.
2. Open Global Properties > Log and Alert > Time Settings.
3. Enter the number of seconds in Status fetching interval.

**System Alerts and Thresholds**

You can set thresholds for selected gateways. When a threshold is passed, a system alert is sent.

**To set System Alert thresholds:**
1. Open Gateways Status view.
2. Right-click a network object and select Configure Thresholds.
   The Threshold Settings window opens.
3. Set the thresholds for the selected object:
   - **Use global settings** - All objects get the same thresholds for system alerts.
   - **None** - The selected gateway object will not have thresholds for system alerts.
   - **Custom** - Change the thresholds for the selected object to be different than the global settings.

**To change Global Threshold settings:**
1. In the Threshold Settings window, click Edit Global Settings.
The Global Threshold Settings window opens.

2. Select thresholds to enable and set the operator and threshold value.
3. In Action, select:
   - **none** - No alert.
   - **log** - Sends a log entry to the database.
   - **alert** - Opens a pop-up window to your desktop.
   - **mail** - Sends a mail alert to your Inbox.
   - **snmptrap** - Sends an SNMP alert.
   - **useralert** - Runs a script. Make sure a user-defined action is available. Go to SmartDashboard > Global Properties > Log and Alert > Alert Commands.

To change custom threshold settings:
1. In the Threshold Settings window, select Custom.
   The global threshold settings show in the same window.
2. Select thresholds to enable for this gateway or cluster member, and set defining values.

**Working with SNMP Monitoring Thresholds**

You can configure a variety of different SNMP thresholds that generate SNMP traps, or alerts. You can use these 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.

**Note** - SNMP monitoring thresholds are supported from R75.20, R71.30, and higher.
In each category there 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 sent and where they are sent to.

**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:

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

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

```
%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 the 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.
Configuring SmartView Monitor

- **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:

- For a local Security 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 Security Gateway.
2. In the summary of the Security 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 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 Security 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.

### Customizing Results

You can create Custom Views, to change the fields that show in the results.

#### Editing a Custom View

The changes you make to a view are not automatically saved. To save the changes, you must **Save To Tree** and create a new view. You can use this procedure to save a predefined view as a new Custom view, if you want to a view that slightly different.

**To save a new view with changes:**
1. Right-click the results of the view and select **Properties**.
   - For some of the views, this option is **View Properties** or **Query Properties**.
2. Add or remove fields and other options for the view.
3. Click **OK**.
   - For some of the views, then select the gateway.
4. Click the **Save View to Tree** button in the Results toolbar.
5. In the window that opens, enter a name for the new view.
6. Click **Save**.
Creating a Custom Gateway Status View

1. In the **Tree**, right-click **Custom** and select **New Gateways View**.
   
   The **Gateway Properties** window opens.
2. In **Select available fields from**, select the source of the data.
3. In **Available fields**, double-click the data to add to SmartView Monitor.
4. Open the **Filter Gateways** tab to remove gateways from the results of this view.
5. Click **OK**.
6. Right-click the new **Custom** view and select **Rename**.
7. Enter a name for the view.

Creating a Custom Traffic View

1. In the **Tree**, right-click **Custom** and select **New Traffic View**.
   
   The **Query Properties** window opens.
2. Select **History** or **Real Time**.
3. If you select **Real Time**, select what you want to see:
   - Interfaces
   - Services
   - IPs / Network Objects
   - QoS Rules
   - Security Rules
   - Connections
   - Tunnels
   - Virtual Links
   - Packet Size Distribution
4. Select the **Target** gateway.
   - If you often need results for one gateway, select it in **Specific Gateway**.
   - If you have a small number of gateways, you can create a custom view for each one.
   - Otherwise, select **Prompt for Gateway before run**.
5. Open the next tabs.
   
   The tabs that show depend on the **Query Type** you selected.
   - If you select **History**, the next tab is **Traffic History**, where you select the **Time Frame** and type of report.
   - If you select **Real Time**, the next tabs let you set services or objects to monitor, gateways or specified IP addresses to monitor, update interval, result type, and chart settings.
6. Click **Save**.
7. Right-click the new **Custom** view and select **Rename**.
8. Enter a name for the view.

Creating a Custom Counters View

1. In the **Tree**, right-click **Custom** and select **New Counters View**.
   
   The **Query Properties** window opens.
2. Select **History** or **Real Time**.
3. Select the **Target** gateway.
   - If you often need results for one gateway, select it in **Specific Gateway**.
   - If you have a small number of gateways, you can create a custom view for each one.
   - Otherwise, select **Prompt for Gateway before run**.
4. Open the **Counters** tab.
5. Select a category and then the counters to add.
   
   You can add counters from different categories to one view.
6. If the Query Type is **History**, select the **Time Frame** and click **Save**.
7. If the Query Type is **Real Time**, open the **Settings** tab and set the update interval and chart type.
8. Click **Save**.
9. Right-click the new **Custom** view and select **Rename**.
10. Enter a name for the view.

### Creating 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**.

### 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**.

### Custom View Example

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.
3. Select **Real-Time**.
   **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.

   The Select Gateway/Interface window appears.

11. Select the gateway or interface for which you would like to create/run this new view.

12. Click the Save to Tree button on the toolbar and enter a name for the new view.

13. Click OK.

   The new view is saved in the Custom branch.

Exporting a Custom View

You can back up a custom view before you install an upgrade. You can share a custom view with other SmartView Monitor GUI clients and other users.

To export a custom view:

1. Right-click the view and select Export Properties.

2. In the window that opens, enter a pathname for the export file.

3. Click Save.

   A file with an svm_setting extension is created.
Chapter 4

Monitoring Gateway Status

In This Section:
- Gateway Status ............................................................... 27
- Displaying Gateway Data .................................................. 27
- Starting and Stopping Cluster Members .............................. 31

Gateway Status

Status updates show for Security Gateways and Software Blades. The Overall status of a gateway is the most serious status of its Software Blades. For example, if all the Software Blades statuses are OK except for the SmariReporter blade, which has a Problem status, then the Overall status will be Problem.

<table>
<thead>
<tr>
<th>Status Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ OK</td>
<td>The gateway and all its Software Blades are working properly.</td>
</tr>
<tr>
<td>✧ Attention</td>
<td>At least one Software Blade has a minor issue, but the gateway works.</td>
</tr>
<tr>
<td>◯ Problem</td>
<td>At least one Software Blade reported a malfunction, or an enabled Software Blade is not installed.</td>
</tr>
<tr>
<td>☢ Waiting</td>
<td>SmartView Monitor is waiting for the Security Management Server to send data from Security Gateways.</td>
</tr>
<tr>
<td>✗ Disconnected</td>
<td>Cannot reach the Security Gateway.</td>
</tr>
<tr>
<td>✠ Untrusted</td>
<td>Cannot make Secure Internal Communication between the Security Management Server and the gateway.</td>
</tr>
</tbody>
</table>

Displaying Gateway Data

Gateway Status data shows for each Check Point or OPSEC gateway.

To see data about a gateway, click the gateway in the Gateway Results view. Details about the gateway show in the Gateway Details pane.

System Data

- 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 that 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 that 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 the gateway 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 working mode as a cluster member, active or not, and its place in the priority sequence. Working modes are: ClusterXL, Load Sharing, and Sync only. Running modes: active, standby, ready and down.

- **Interfaces** - Interfaces recognized by the gateway. The interface data includes the IP Address and status of the specified interface: if the connection passing through the interface is verified, trusted or shared.

- **Problem Notes** - 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
• 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 connection 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).

**Starting and Stopping Cluster Members**

To stop and start one member of a cluster from SmartView Monitor:

1. Open a Gateway Status view.
2. Right-click the cluster member and select Cluster Member > Start Member or Stop Member.
Chapter 5

Monitoring Tunnels

In This Section:

- Tunnels Solution .......................................................... 32
- Tunnel View Updates .................................................. 33
- Running Tunnel Views .................................................. 33

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 organization's 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.

This table shows the possible Tunnel states and their significance to a Permanent or Regular Tunnel.

<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>
</tbody>
</table>
Tunnel View Updates

If a Tunnel is deleted from SmartDashboard, the **Tunnel Results View** shows the deleted Tunnel for an hour after it was deleted.

If a community is edited, the **Results View** shows removed tunnels for one hour after they were removed from the community.

Running Tunnel Views

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 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.
Chapter 6

Monitoring Traffic or System Counters

In This Section:
- Traffic or System Counters Solution ................................................................. 35
- Select and Run a Traffic or System Counters View ......................................... 37
- Recording a Traffic or Counter View ................................................................. 37

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>
<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.
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.

Recording a Traffic or Counter View

You can save a record of the Traffic or System Counter view results.

1. Run the Traffic or System Counters view.
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

After you record a view, you can play it back. You can choose Play or Fast Play, to see results change faster.

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.

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 7

Monitoring Users

In This Section:

Users Solution ........................................................................................................................................... 38
Run a Users View ...................................................................................................................................... 38

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 that makes the view definition process user-friendly and highly efficient and lets you to easily navigate through the obtained results.

With data on current open sessions, overlapping sessions, route traffic, connection time, and more, the User Monitor gives detailed information about remote users' connectivity experience. This SmartView Monitor feature lets you view real-time statistics about open remote access sessions.

If specific data are not relevant for a given User, the column shows N/A for the User.

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.
Chapter 8

Cooperative Enforcement

In This Section:
Cooperative Enforcement Solution .......................................................... 40
Running a Cooperative Enforcement View ............................................. 41

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.

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 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.

---

**Running 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)
System Counter  •  7
System Counters  •  36
System Counters View  •  11
System Data  •  27

T
The Need for Suspicious Activity Rules  •  15
Traffic  •  7,  35
Traffic Legend Output  •  36
Traffic or System Counters Solution  •  35
Traffic View  •  10
Tunnel View Updates  •  33
Tunnels Solution  •  32
Tunnels View  •  11
Types of Alerts  •  20

U
Understanding the User Interface  •  9
UserAuthority WebAccess  •  30
Users Solution  •  38
Users View  •  12

V
Viewing Alerts  •  14
Virtual Private Networks  •  28
VPN  •  7
VPN Tunnel  •  7

W
Working with SNMP Monitoring Thresholds  •  19