IMPORTANT
Check Point recommends that customers stay up-to-date with the latest service packs and versions of security products, as they contain security enhancements and protection against new and changing attacks.

For additional technical information about Check Point products, consult Check Point's SecureKnowledge at:

http://support.checkpoint.com/kb/

See the latest version of this document in the User Center at:

http://www.checkpoint.com/support/technical/documents/docs_r55.html

Part No.: 700728
January 2004
# Table Of Contents

## Chapter 1  SmartView Monitor Overview
- SmartView Monitor Technologies  7
  - Overview  7
- SmartView Monitor Features  8
- Installing Check Point SmartView Monitor  9

## Chapter 2  SmartView Monitor Sessions
- Starting SmartView Monitor Sessions  11
  - Certificate Management, Compression Optimization and Advanced Options  13
- Defining a SmartView Monitor Session  14
- Recording Monitoring Sessions  15
  - To record a monitoring session  15
  - To stop recording a monitoring session or a playing a previously recorded session  15
  - To play a previously recorded session  15
  - To fast play a previously recorded session  15
  - To pause playing  16
- Viewing Monitored Information  16
  - Legend  16
  - Scaling  17
- Viewing Previous Data  17
  - Enabling Graph Values Display  17
- Interrupting the Monitoring Session Process  17
- Change Data Display for Monitoring Sessions  18
  - Changing the display using other SmartConsole options  20

## Chapter 3  Monitoring — Check Point System Counters
- Overview  21
- Monitoring Check Point System Counters  22
  - Session Properties Window — Counters Tab  23
- Displaying Check Point System Counters Data  23
  - Example — Check Point System Counters  24

## Chapter 4  Monitoring — Real-Time Traffic
- Overview  25
- Monitoring Services  26
  - Session Properties Window — Monitor by Services Tab  27
- Monitoring Network Objects  28
  - Session Properties Window — Monitor by Network Objects Tab  29
- Example — Services and Network Objects  30
  - Generating a Real-Time Session  30
In This Chapter

SmartView Monitor Technologies  page 7
Installing Check Point SmartView Monitor  page 9

SmartView Monitor Technologies

Overview

Check Point SmartView Monitor is an easy-to-use monitoring tool that allows you to inspect network traffic and connectivity. In addition, it provides real-time information about the performance and security state of both FireWall-1 and VPN-1 operations. As an administrator you have to ensure high network availability, efficient bandwidth usage and data integrity. If your network experiences problems such as sluggishness, loss of data or security related problems, you need to be able to immediately identify changes in the network traffic flow patterns or security activities. You need to find out the cause of these problems, when and why they occur, and fix them. An enterprise implementing its data network on the Internet must monitor connectivity to ensure high network availability and efficient bandwidth usage. Check Point SmartView Monitor User Guide provides network administrators with the tools they need to monitor traffic and identify bottlenecks as they occur.

Many Internet Service Providers (ISPs) contractually commit to a Service Level Agreement (SLA) under which they undertake to provide a guaranteed level of service, usually defined in terms of network delay, CIR (Committed Information Rate), percentage of dropped packets etc.
SmartView Monitor provides network administrators with the following tools.

1) Analysis capabilities
   • Diagnose network, security and performance problems.
   • Inspect various Check Point products such as FireWall-1, VPN-1, FloodGate-1.
   • Target specific network activities for monitoring.
   • Get information about services that are being used, servers and clients that are being accessed and by whom.
   • Inspect bandwidth and get hardware indicators such as CPU usage, used memory, etc.

2) Management and control capabilities
   • Assume instant control of traffic flow on a Gateway.
   • Block a specific traffic when a threat is imposed.
   • Track Service Level between two Gateways, and receive alarms when the Service Level agreement (SLA) is violated.
   • Recall past activities, create reports and record monitored activities.

SmartView Monitor Features

Check Point System Counters
Check Point System Counters collect information about the status, activities, hardware and software usage of different Check Point products in real-time mode. You can use System Counters to plot graphs and to view reports of current or archived data collected by Counter Logs. For example, if you want to focus on VPN tracking, you can use System Counters to ascertain how many tunnels are currently open.

Traffic Flow Through a Single / All Interfaces of a Gateway
Traffic flow can be monitored per service or network object. In addition, SmartView Monitor enables monitoring based on a variety of parameters, for example the QoS Policy rules installed on an interface, or the top Security Rules set for an interface, or the SL (Service Level) of an end-to-end link, between two Check Point VPN-1 Pro or FloodGate-1 Modules. In addition, the degree of compliance to a Service Level Agreement (SLA) can be monitored on the Virtual Link, and alerts can be generated in the event that there are SLA violations. For information on how to use traffic monitoring, see Chapter 4, “Monitoring — Real-Time Traffic.”
Virtual Link Monitoring
Monitor traffic between two Check Point VPN-1 Pro modules or two FloodGate-1 Modules for real time analysis of bandwidth and latency. Virtual Link Monitoring can track compliance with a Service Level Agreement (SLA). SmartView Monitor has to be installed on the module in order to enable traffic monitoring and in order to support the process by which reports are generated. It is not required for running Counters. For more information, see “Report Mode” on page 65.

Blocking Suspicious Connections
Suspicious Activity rules are security rules, which once set can be applied immediately without the need to perform the "Install Policy" action. These rules enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced Security Policy.

Installing Check Point SmartView Monitor
To install a Check Point SmartView Monitor Module from the Check Point installation CD (see Check Point Getting Started Guide), select SmartView Monitor in the Server/Gateway Components window (FIGURE 1-1).

FIGURE 1-1 SmartView Monitor selected in the Server/Gateway Components window
To install a SmartView Monitor SmartConsole, select **SmartConsole Clients** in the **Server/Gateay Components** window. Then select **SmartView Monitor** in the **Check Point SmartConsole** window (FIGURE 1-2).

**FIGURE 1-2 Check Point SmartConsole Clients Installation**
SmartView Monitor Sessions

In This Chapter

Starting SmartView Monitor Sessions .......................... page 11
Defining a SmartView Monitor Session ......................... page 11
Recording Monitoring Sessions ............................... page 16
Viewing Monitored Information ............................... page 16
Interrupting the Monitoring Session Process ................. page 17
Change Data Display for Monitoring Sessions ............... page 18

Starting SmartView Monitor Sessions

To start SmartView Monitor, do one of the following:

- Double-click the SmartView Monitor icon.
- Choose SmartView Monitor from the Window menu in the SmartDashboard window.

The SmartView Monitor Login window (FIGURE 2-1) is displayed.
You can log in using either your:

- **User name and password:**
  1. Select **User Name**.
  2. Enter your user name and password.
  3. Click **OK**.

- **Certificate:**
  1. Select **Certificate**.
  2. Enter the name of your PKCS#12 certificate file.
     You can browse for the file using by clicking [ ].
  3. Enter the password you used to create the certificate.
  4. Click **OK**.

Enter the name of the machine on which the SmartCenter Server is running. You can enter one of the following:

- A resolvable machine name.
- A dotted IP address.

To work in local mode, check **Demo Mode**.

If you do not wish to modify a policy, check **Read Only** before clicking on **OK**.

**Note** - If you are not defined as a user, and therefore do not possess a user name, see “To Add an Administrator” on page 49, for information how to define users on the SmartCenter Server.
Certificate Management, Compression Optimization and Advanced Options

In the SmartView Monitor Login window (FIGURE 2-1), click More Options >> to display the Certificate Management, Connection Optimizations and Advanced options (FIGURE 2-2).

FIGURE 2-2 SmartView Monitor login window — More Options

To change the certificate password, click Change Password.

To compress the connection to the SmartCenter Server, check Use compressed connection.

Enter the text describing why the administrator wants to make a change in the security policy in Session ID (optional). The text appears as a log entry in the SmartView Tracker in the Session ID column (in Audit mode only). If the Session ID column does not appear in the SmartView Tracker, use the Query Properties pane to display it. For more information on the SmartView Tracker, see the chapter called SmartView Tracker in the Check Point SmartCenter Guide.

To hide the Certificate Management, Connection Optimizations and Advanced options, click Less Options <<.
Defining a SmartView Monitor Session

The Session Pane provides an easy-to-use interface for performing the following actions:

- Configuring new monitoring sessions.
- Running pre-defined (already-configured) sessions.
- Managing sessions, for instance renaming, deleting or modifying sessions. You can also copy and paste Custom or Predefined sessions into the custom sessions tree.

The properties of a monitoring session are defined in the **Session Properties** window. While monitoring, you can open the **Session Properties** window for a new monitoring session by choosing **New** from the **File** menu.

New or modified sessions are marked by an asterisk (*). This mark remains till the configuration is saved. If you exit SmartView Monitor without saving your new configuration, you will be prompted to save it. To save your new configuration, select the session name from a displayed list of sessions.

In addition to modifying a configuration through the Session pane, you can modify a specific session by right click on the session view. You can also configure custom sessions.

**Predefined Sessions**
These are already-configured sessions that enable you to monitor different aspects of network activities. This is done by the following easy two steps:

1. Double click on the Predefined Sessions. A list of modules and their interfaces is displayed.
2. Select the module or interface you wish to monitor. The View window displays the session parameters. No further configuration is required.

This feature also provides an efficient and quicker way for configuring new sessions. This is achieved by modifying a predefined session and copy the modified session's settings into a new created custom session.

The followings are some of the different predefined sessions variables for monitoring a selected module or interface:

- Top Destinations - the top active destination servers.
- Top Matched Security rules - the most used Security Rules.
- Top Services - the top active services.
- Top Sources - the top active clients.
- VPN-1 performance - various indicators of VPN activities.
Run a Sessions

To run either a custom or predefined session double click the session.

Recording Monitoring Sessions

It is possible to make instantaneous live recording sessions.

To record a monitoring session

1) Click in the toolbar, or select Record from the Recording menu. The Save As window appears.

2) Specify the name and location of the recording session. The default file name for the recording session consists of the monitoring session configuration name (see “Defining a SmartView Monitor Session” on page 14), the current date and the current time. The default location is the MonitorData directory which is found under the directory in which the Check Point SmartConsole Clients are located.

3) Click Save to begin recording. The word Recording appears in the top-right corner of the window.

To stop recording a monitoring session or a playing a previously recorded session

Click in the toolbar, or select Stop from the Recording menu.

To play a previously recorded session

1) Click in the toolbar, or select Play from the Recording menu. The Select Recorded window appears.

2) Select the desired file and click Open. The word Playing appears in the top-right corner of the window.

To fast play a previously recorded session

1) Click in the toolbar, or select Fast Play from the Recording menu. The Select Recorded window appears.

2) Select the desired file and click Open. The word Fast Playing appears in the top-right corner of the window.
To pause playing

1) Click in the toolbar, or select Pause from the Recording menu. The word Pausing appears in the top-right corner of the window.

2) To resume playing, click in the toolbar, or select Play from the Recording menu.

Viewing Monitored Information

The Pane in which the monitored information is displayed, consists of either a line graph or a bar chart, depending on whether or was selected respectively. Each monitor has a significant title which explains what is being monitored. Below this heading, in Real-time mode there is a clock which displays the current time, during which the information is being monitored.

Legend

Below the monitor is a new enhanced Legends view. This view consists of a table. This table classifies all significant information appearing in the monitor according to:

- **Color** — the color which represents the object in the monitor
- **Counter Name** — the name of the object being monitored
- **Current** — the current number of the option being passed
- **Average** — the average number of the option usually generated
- **Maximum** — the maximum number of the option that has been generated thus far
- **Minimum** — the minimum number of the option that has been generated thus far
- **Y-Scale, Units** — length, units of Y-Scale

When tracking Services and Network Objects:

- If you select to monitor specific Services or Network Objects, the Aggregate Data, that is the total amount of Services and Network Objects traffic in the system will be displayed.
- If you select to monitor top Services or Network Objects you can capture the current objects displayed in the monitor, by clicking the Lock icon. This icon ensures that the currently displayed top objects will continue to be monitored, and the monitor will not be constantly updating with new objects as they are being updated.
Scaling

Use the scaling option to provide an enhanced view of the monitored information. The current scaling range appears on the vertical axis of the display graph itself, or in the Scaling toolbar.

You can enter new upper and lower limits in the Scaling toolbar text boxes. To optimize scaling, click in the Scaling toolbar.

If you wish to return to the default scaling setting, open the Settings tab of the Session Properties window and reselect Set to automatic scaling.

Viewing Previous Data

If you have chosen to view a line chart, you can use the horizontal scroll bar to view previous monitoring data.

When you move the scrollbar to the left, the chart will return to the time period defined by the scrollbar position. The data in the chart will be static, but monitoring will continue.

To return to the current time, move the scrollbar back to the right.

Enabling Graph Values Display

When graph values are enabled, you can click on a line or bar in the display graph and see the exact value of the corresponding monitoring data.

To select a bar or line graph, select Chart Type from the View menu.

Interrupting the Monitoring Session Process

Monitoring can be interrupted and resumed at any time by selecting Freeze View from the View menu, or by clicking in the SmartView Monitor toolbar.

After an interruption, monitoring will resume at current values. Changes that occurred during the interruption will not be displayed.

In line graphs, the interrupted time range will be indicated by a dotted black line and the word Interrupt (FIGURE 2-3).
Change Data Display for Monitoring Sessions

You can change the way traffic statistics are displayed at any time during a monitoring session by choosing **Properties** from the **Session** menu, or by clicking  in the SmartView Monitor toolbar. In the **Settings** tab of the **Session Properties** window you can modify the display settings.

![Monitoring Interruption](image-url)
**Change the Display — Settings Tab**

**FIGURE 2-4** Session Properties window — Settings tab

<table>
<thead>
<tr>
<th>Session Properties - Traffic - Top Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Rate</td>
</tr>
<tr>
<td>Update interval: X seconds</td>
</tr>
<tr>
<td>Chart Type</td>
</tr>
<tr>
<td>Line</td>
</tr>
<tr>
<td>Bar</td>
</tr>
<tr>
<td>Measurement</td>
</tr>
<tr>
<td>Data Transfer Rate: X Bytes per record</td>
</tr>
<tr>
<td>Packets per Second</td>
</tr>
<tr>
<td>Connections: Average Concurrent Connections</td>
</tr>
<tr>
<td>Line Utilization (%)</td>
</tr>
<tr>
<td>Percent</td>
</tr>
<tr>
<td>Milliseconds</td>
</tr>
<tr>
<td>Scaling</td>
</tr>
<tr>
<td>Set to automatic scaling</td>
</tr>
<tr>
<td>Set scaling from 0 to 1000 bytes per record</td>
</tr>
</tbody>
</table>

**Chart Type** — Select **Line** or **Bar**.

**Measurement** — Select one of the following measurement options:

- **Data Transfer Rate** — If you choose to monitor data transfer rate, select a unit of measurement from the **Units** drop down menu.
- **Packets per second**
- **Line Utilization (%)**
- **Percent**
- **Milliseconds**

**Scaling** — Select one of the following:

- **Set to automatic scaling** — depends on units of measurement.
Change Data Display for Monitoring Sessions

- **Set scaling from... to...** — Specify the upper and lower limits of the scaling range in the appropriate text boxes. Measurement units depend on the option selected in the Measurement field.

  **Note** - You can change setup parameters during a session by choosing Properties from the Sessions menu.

**Monitor Rate** — Specify the rate at which the display will be updated.

**Update interval...seconds** — Click the appropriate arrow to increase or decrease the number of seconds between updates.

**Changing the display using other SmartConsole options**

The following menu items and toolbar buttons also allow you to change the graph display:

**TABLE 2-1 Toolbar Buttons and Menu Options**

<table>
<thead>
<tr>
<th>Toolbar Button</th>
<th>Menu Option</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>View &gt; Chart Type &gt; Line Graph</td>
</tr>
<tr>
<td></td>
<td>View &gt; Chart Type &gt; Bar Graph</td>
</tr>
<tr>
<td></td>
<td>Action &gt; Suspend QoS Policy</td>
</tr>
<tr>
<td></td>
<td>View &gt; Optimize Scaling</td>
</tr>
<tr>
<td></td>
<td>Play &gt; Pause</td>
</tr>
</tbody>
</table>
In This Chapter

Overview ........................................ page 21
Monitoring Check Point System Counters .......... page 22
Displaying Check Point System Counters Data ......... page 23

Overview

Check Point SmartView Monitor allows you to monitor Check Point System Counters. Check Point System Counters are collectors of information about the status, activities, hardware and software usage of different Check Point products in real-time. You can use System Counters to design graphs and to view reports of current or archived data collected by Counter Logs. For instance, for VPN, you can ascertain how many tunnels are currently open.
To set up SmartView Monitor for monitoring a Check Point System Counter:

1. Select **Real Time** in the **Mode** drop-down menu of the **Session Type & Target** tab of the **Session Properties** window.

2. Select **Check Point System Counters**.

3. Select a module under **Select monitored Module/Interface**. Only one module can be monitored at any given time.

4. In the **Counters** tab select the Counters to display.
   
   For information about the fields in the **Counters** tab, see “Session Properties Window — Counters Tab” on page 23.

5. In the **Settings** tab, specify the display parameters for the session.
   
   For information about the fields in the **Settings** tab, see “Change the Display — Settings Tab” on page 19.

When the Counters parameters have been set up, you can begin the monitoring display (see “Displaying Check Point System Counters Data” on page 23).
Session Properties Window — Counters Tab

**FIGURE 3-2** Session Properties window — Counters tab

**Counters Category** — select a category:

The **Available Counters** box lists currently defined counters.

To add an object, select it in the **Available** box and click on **Add**.

To remove an object, select it in the **Selected Counters** box, and click on **Remove**.

**Detailed description** — view a detailed description about the selected category.

**Displaying Check Point System Counters Data**

After you define monitoring parameters in the tabs of the **Session Properties** window, click **OK** to view monitoring data.
Example — Check Point System Counters

Generating a Real Time Session

It is the start of the working day, the whole of the Marketing and Sales department of company **ABCD** are attending a conference away from the office and they need to connect remotely using SecuRemote/SecureClient. Much to their dismay they are unable to connect to the network and to start working. Kate is told to generate a Report immediately in order to see what is holding the system back.

Kate decides to make report for several Check Point System Counters that have been in use on the **Remote_Gateway** module over the past hour. In SmartConsole:

- She opens a new session, by selecting Session > New
- In the Session Type & Target tab, she chooses the Real-Time Mode and she makes sure that Check Point System Counter is selected.
- In the Counters tab, she chooses the following Counters Categories:
  - VPN Tunnels — IKE Failures Rate, IKE Successes Rate, IKE Concurrent, Active Tunnels.
  - OS CPU — Cpu Usage %.
  - OS MEMORY — Total Physical Memory.
- She clicks on OK, and the monitor is displayed. In the graph, Kate right-clicks on the Y-axis and selects Modify Y Xcale. She adjusts the value of the Y scale so that the selected field is emphasized and Kate can examine it more clearly.
- Conclusions: the SmartView Monitor indicates that there are more failures than successes, therefore, the system administrator understands that the company **ABCD** cannot accommodate all the employees attempting to log on at once. Once the system administrator has used SmartView Monitor in order to discover the problem, she can now concentrate on finding a solution!
Overview

SmartView Monitor allows you to monitor the traffic that flows through a single interface. You can choose to monitor:

- The traffic that flows through a single interface of by service.
  - For information see “Monitoring Services” on page 26.
- The traffic that flows through a single interface by network object.
  - For information see “Monitoring Network Objects” on page 28.
- By QoS Rules, based on the QoS Policy installed on a Check Point FloodGate-1 Module.
  - For information on Monitoring by QoS Rules, see “Monitoring by QoS Policy Rules” on page 32.
- By top Security Rules.
  - For information on Monitoring by top Security Rules, see “Monitoring by Top Security Rules” on page 37.
To set up SmartView Monitor for monitoring an interface:

1. Select **Real Time** Mode in the **Session Type & Target** tab of the **Session Properties** window.

2. Select **Services** in the **Traffic by** section in the **Session Type & Target** tab of the **Session Properties** window.

3. Select an interface under **Select Monitored Module/Interface**. Only one interface can be monitored at any given time.

4. In the **Monitor by Services** tab, select the services to display.
   
   For information about the fields in the **Monitor by Services** tab, see “Session Properties Window — Monitor by Services Tab” on page 27.

5. In the **View Settings** tab specify the display parameters for the session.
   
   For information about the fields in the **View Settings** tab, see “Change the Display — Settings Tab” on page 19.
When the interface monitoring parameters have been set up, you can begin the monitoring display (see “Monitoring Services” on page 26).

**Session Properties Window — Monitor by Services Tab**

![Session Properties Window — Monitor by Services Tab](image.png)

**Services** — select one of the following:
- **Top Services** — display the top services in use.
- **Specific Services** — select specific services to be displayed:
  - The Available box lists currently defined services.
  - To add an object, select it in the Available box and click on Add.
  - To remove an object, select it in the Selected box, and click on Remove.

**Data Direction** — Choose the direction of monitored traffic. Select one of the following:
- **Eitherbound** — traffic passing through the specified interface in either direction.
- **Outbound** — traffic exiting the gateway through the specified interface.
- **Inbound** — traffic entering the gateway through the specified interface.
Monitoring Network Objects

FIGURE 4-3 Session Properties window — Session Type & Target tab [Network Objects (IPs)]

To set up SmartView Monitor for monitoring an interface:

1. Select **Real Time** Mode in the **Session Type & Target** tab of the **Session Properties** window.

2. Select **Network Objects (IP)** in **Traffic by** under the **Monitor** section in the **Session Type & Target** tab of the **Session Properties** window.

3. Select an interface under **Select Monitored Module/Interface**. Only one interface can be monitored at any given time.

4. In the **Monitor by Network Objects** tab, select the network objects to display.
   
   For information about the fields in the **Monitor by Network Objects** tab, see “Session Properties Window — Monitor by Network Objects Tab” on page 29.

5. In the **Settings** tab, specify the display parameters for the session.
   
   For information about the fields in the **Settings** tab, see “Change the Display — Settings Tab” on page 19.
When the interface monitoring parameters have been set up, you can begin the monitoring display (see “Monitoring Network Objects” on page 28).

**Session Properties Window — Monitor by Network Objects Tab**

![Session Properties window — Monitor by Network Objects tab](image)

**Network Objects** — select one of the following.

**Top Network Objects** — display the top network objects in use.

**Specific Network Objects** — select specific network objects to be displayed.

The **Available** box lists currently defined network objects.

To add an object, select it in the **Available** box and click on **Add**.

To remove an object, select it in the **Selected** box, and click on **Remove**.

**Data Direction** — Choose the direction of monitored traffic. Select one of the following:

- **Eitherbound** — traffic passing through the specified interface in either direction.
- **Outbound** — traffic exiting the gateway through the specified interface.
- **Inbound** — traffic entering the gateway through the specified interface.
Data Origin — check one of the following:
- **Source** — Display connections if the source is any of the selected network objects.
- **Destination** — Display connections if the destination is any of the selected network objects.
- **Source or Destination** — Display connections if the source or destination is one of the selected network objects.

If you check both **Source** and **Destination**, connections will be displayed if either their source or destination is any of the selected network objects.

Example — Services and Network Objects

**Generating a Real-Time Session**

The Help Desk in a company called **ABCD** gets many complaints that Internet access is slow and sluggish. A junior administrator called Kate is told to determine what is slowing down the system. She opens a SmartView Monitor, so that she can create a traffic report for the **Company_Gateway** interface.

- In SmartView Monitor she opens a new session, by selecting **Session > New**.
- In the **Session Type & Target** tab, she chooses the **Real-Time** Session Mode and she makes sure that **Traffic by > Services** is selected. She chooses to monitor the **Company_Gateway** module monitored.
- In the **Monitor by Services** tab, she chooses to select KaZaA and H323 from the **Specific Services** listbox, since she knows that these are services that often impede the smooth running of the system. She decides to monitor this traffic in both direction, therefore she selects **eitherbound**.
- In the **Settings** tab, she set the **Chart Type** as **Line** in order that she can see the interaction of the two Services. She selects the **Measurement** as the **Data transfer Rate** in **BPs**, and she click on **OK**.
- When the monitor is displayed, Kate sees that in real-time the rate of KaZaA and H323 traffic is heightened.
- Whenever specific services or network objects are displayed, the Legend displays the Aggregate system information as well, this is the total amount of Network Objects and Services traffic in the system at the present time. Since Kate has no current use for this Aggregate information, she selects it in the Legend and deletes it.

Kate decides to check the most prominent users.
- She right clicks on H323 and selects **Top Sources**.
Kate examines the list of ten top H323 service users and may decide to record the behavior of the aggressive users so that she can show it to her Manager at the first opportunity.

**Generating a Report**

For the purpose of comparison, Kate wants to make sure that the level of H323 and KaZaA that have been identified in the *Check Point SmartView Monitor User Guide* are indeed higher than usual, so she decides to make a traffic report for the same services from the previous week. She opens the SmartView Monitor, so that she can create a traffic reports for the *Company Gateway* interface.

Kate decides that she want to make a traffic report on the Services that have been in use over the past hour on the *Company Gateway* module, so in her SmartConsole she proceeds as follows:

- She opens a new session, by selecting **Session > New**.
- In the **Session Type & Target** tab, she chooses the **History Report** Mode and she makes sure that **Traffic** is selected. She choose the module for which she wishes to examine the traffic (*Company Gateway*).
- In the **Traffic History** tab, she chooses to create a Report from the **Time Frame** of the **Last week**. In the **Select Throughput Report** listbox she selects the **Top Services** report. She clicks on **OK**, and the report is displayed.
- From the monitor, Kate sees that the top Services in use are HTTP, KaZaA and H323. She notices that the average number of HTTP and H323 from the previous week are not as high as the levels being generated in real-time. She considers this fact for a moment, and then moves on.

Kate continues by making a similar traffic report for the Network Objects that have been in use on the *Company Gateway* module over the last week. So she opens a second SmartConsole and she proceeds as follows:

- She opens a new session, by selecting **Session > New**
- In the **Session Type & Target** tab, she chooses the **History Report** Mode and she makes sure that **Traffic** is selected. She makes sure that she selects the same module that she selected for the Services Report (*Company Gateway*).
- In the **Traffic History** tab, she chooses to create a Report from the **Time Frame** from the **Last Hour**. In the **Select Throughput Report** listbox she selects the **top network objects** report. She clicks on **OK**, and the report is displayed.
- The Legend of the monitor displays the top Network Objects in use. Kate optimizes the monitor view, by selecting **Monitor > Optimize Scaling**. When Kate selects a Network Object in the Legend, the Network Object is marked in the monitor.
Conclusion: Kate sees that in the monitor there are no specifically aggressive users in the previous week’s monitor.

**Conclusion**

Once her manager is in her office, Kate shows the saved file recorded from real-time as well as the report generated in Report mode and the Real-time charts that she created. Kate and her manager conclude that they need to contact the aggressive users and reduce the heightened Services count.

- Kate’s manager calls Joe_user_ABCD. Joe_user_ABCD admits to downloading multiple MP3s, thereby causing over-use of KaZaA.
- Kate’s manager also calls the CEO’s secretary, to discover that the CEO is in a video conference, thus explaining the increased H323 services.

**Monitoring by QoS Policy Rules**

**FIGURE 4-5 Session Properties — selecting to monitor traffic by QoS Rules**

To set up SmartView Monitor for monitoring an interface by QoS Policy rules:

1. Select **Real Time** Mode in the **Session Type & Target** tab of the **Session Properties** window.
2. Select **Monitor by QoS Policy Rules** in the **Session Type & Target** tab of the **Session Properties** window.

3. Select an interface under **Select Monitored Module/Interface**. Only one interface can be monitored at any given time.

4. In the **Monitor by QoS Rules** tab, select the rules by which you wish to monitor. For information about the fields in the **Monitor by QoS Rules** tab, see “Session Properties Window — Monitor by QoS Rules Tab” on page 33.

5. In the **View Settings** tab, specify the display parameters for the session. For information about the fields in the **View Settings** tab, see “Change the Display — Settings Tab” on page 19.

When the monitoring parameters have been set up, you can begin the monitoring display. See “Monitoring by QoS Policy Rules” on page 32.

**Session Properties Window — Monitor by QoS Rules Tab**

**FIGURE 4-6** Session Properties window — Monitor by QoS Rules tab

**Data Direction** — Choose the direction of monitored traffic. Select one of the following:
Monitoring by QoS Policy Rules

- **Inbound** — traffic entering the gateway through the specified interface.
- **Outbound** — traffic exiting the gateway through the specified interface.
- **Eitherbound** — traffic passing through the specified interface in either direction.

**Installed QoS Policy** — Choose the rules you wish to monitor.

Click **Refresh Rules** to display all the rules in the installed rule base.

All the rules will be selected by default. If there are rules that you do not wish to monitor, deselect them. You may also click:
- **Select All** — to reselect all the rules.
- **Clear All** — to deselect all the rules.
- **Select Main Rules** — to select only the rules at the first level of the QoS Policy, without subrules.

**Example — QoS Rules**

Kate decides to check the status of traffic distribution by QoS rules using the SmartView Monitor in order to validate the effectiveness of the QoS policy. Therefore:

1. She opens a new session, by selecting **Session > New**
2. In the **Session Type & Target** tab, she chooses the **Real-Time** Session Mode and she makes sure that **Traffic > Top QoS Rules** is selected. She choose the same module monitored as in the previous reports.
3. In the **Monitor by Top QoS Rules** tab, she clicks **Refresh Rules** to ensure that the QoS rules displayed in the **Installed QoS policy** listbox are up-to-date. She selects the QoS rules that she would like to monitor.
4 In the **Settings** tab she selects **Packets per second** and she clicks on **OK**.
Suspending QoS Policy

If there is a FloodGate-1 QoS Policy installed on the monitored interface, you can choose to suspend it and view unrestricted traffic at any time during a monitoring session.

To suspend QoS Policy, select **Suspend QoS Policy** from the **Monitor** menu.
Monitoring by Top Security Rules

To set up SmartView Monitor for monitoring by Top Security rules:

1. Select **Real Time** Mode in the *Session Type & Target* tab of the *Session Properties* window.

2. Select **Monitor by Top Security Rules** in the *Session Type & Target* tab of the *Session Properties* window.

3. Choose an interface under **Select Monitored Module/Interface**. Only one interface can be monitored at any given time.

4. In the **Monitor by Top FW Rules** tab, select the rules by which you wish to monitor. For information about the fields in the **Monitor by Top FW Rules** tab, see “Session Properties Window — Monitor by Top Security Rules Tab” on page 38.

5. In the **View Settings** tab, specify the display parameters for the session.

For information about the fields in the **View Settings** tab, see “Change the Display — Settings Tab” on page 19.
After you have set up the monitoring parameters, click **OK** and the monitoring display opens.

**Session Properties Window — Monitor by Top Security Rules Tab**

![Session Properties window — Monitor by Top FW Rules tab](image)

**Data Direction** — Choose the direction of monitored traffic.

Select one of the following:
- **Eitherbound** — traffic passing through the specified interface in either direction
- **Outbound** — traffic exiting the gateway through the specified interface
- **Inbound** — traffic entering the gateway through the specified interface

**Example — Top Security Rules**

**Generating a Report**

Kate decides to make traffic report for the top Security rules that have been in use on the **London_Gateway** module over the past hour. In SmartConsole:
- She opens a new session, by selecting **Session > New**
In the **Session Type & Target** tab, she chooses the **History Report** Mode and she makes sure that **Traffic** is selected. She makes sure that she selects the same module that she selected for the Services Report.

In the **Traffic History** tab, she chooses to create a Report with a **Time Frame** of the **Last Hour**. In the Report listbox she selects the **Top Security Rules** report. She clicks **OK**, and the report is displayed.

**FIGURE 4-11** Top Security Rules

Kate discovers that she can stand on the bars in the monitor and a tooltip is displayed. This tooltip displays information about the selected top security rule.

**Conclusions** —

Kate discovers that the FireWall-1 rule that is in most frequent use is **rule 17**. She goes to the SmartDashboard to see what this rule is about:

**TABLE 4-1** The drop rule on the Rule Base

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Drop</td>
</tr>
</tbody>
</table>
Kate discovers that the FireWall-1 rule that is in the next most frequent use is rule 39. She goes to the SmartDashboard to see what this rule is about:

**TABLE 4-2 The drop rule on the Rule Base**

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>39</td>
<td>Any</td>
<td>Server1</td>
<td>http</td>
<td>Accept</td>
</tr>
</tbody>
</table>

### Generating a Real Time Monitor

In her SmartConsole, Kate has discovered that rule 17 is the most prolific rule. Kate decides to check if this is still the case in real-time. Therefore:

- She opens a new session, by selecting **Session > New**
- In the **Session Type & Target** tab, she chooses the **Real-Time Session Mode** and she makes sure that **Traffic > Top Security Rules** is selected. She choose the same module monitored in the previous reports.
- In the **Monitor by Top FW Rules** tab, she chooses to monitor the **Top Security Rules**. She decides to monitor this traffic in both direction, therefore she selects **eitherbound**.
- In the **Settings** tab, she set the **Chart Type** as **Bar** so that she will be able to see an effect distinctly if it occurs. She selects the **Measurement** to be **Line Utilization**.

Kate clicks **OK**, and the SmartView Monitor displays the top six rules. The monitor is dynamic and every few seconds the rules change, but Kate is able to see that Rule 17 does indeed recur on several occasions.

When Kate sees that Rule 17 recurs, she decides to investigate further. She selects **View > Freeze View**. The **Top Security Rules** monitoring ceases to run. Kate changes the **Chart Type** from **Bar** to **Line**, since in **Line** charts, when the monitoring is interrupted, the chart is marked by a broken line at the place where the monitor was interrupted.

### Conclusions:

Rule 17 stipulates that all connections should be dropped. In a typical system the drop rule is the last rule in the Rule Base and is generally added in to ensure that all connections that cannot be matched against the Rule Base are immediately dropped. In this scenario, where there are many connections being dropped. When Kate sees the prolific appearance of the drop rule, she feels that there may be some suspicious activities going on. Since this suspicious activity may indicate some sort of security hazard, she decides to further her investigations in order to ensure that there is not some form of attack being performed.
Kate sees that Rule 39 is a very influential rule. She decides to move it to the beginning of the Rule Base in the SmartDashboard in order to improve the performance and effectiveness of the policy.

Filtering Traffic
Filtering enables you to target specific network activities for monitoring. It provides you narrow view angle of the specific components you have selected. You can focus on a specific user's activities or target the source and destination of a particular service.

How to Configure Filtering
You can configure filtering in one of the following ways:
- through the Session View window.
- through the Session Properties window.

When monitoring services and your goal is to focus on the HTTP service and to find out which IP machine is the heaviest HTTP service consumer.

Filtering from the Session View window
Right click on the http bar/line and select Top Sources on http. The View window displays the top ten IP machines that generate the heaviest http traffic (that passes through the monitored module). The session properties change according to the new settings.

Filtering from the Session Properties window
1. In the Traffic by section select the Network Objects (IP's).
2. In the Monitor by Network Object section select Top Network Objects.
3. In the Data Direction section select the appropriate choice.
4. In the Data Origin section select Source.
5. In the Filter tab, enable filtering by selecting the traffic types to be monitored. Click Monitor Traffic that Matches the Below, then check Services.
6. Select http from the Available Services list and click Add. The http appears on the Match window.
7. Click OK.

Other options include:
- Monitor all traffic: this option disables filtering, resulting in monitoring all types of traffic that passes through the selected module/interface.
• The **Not** check box in the **Match** section enables you to filter out traffic types you do not wish to include in the monitoring process. Hence, all categories except those that are specified in the **Not** section will be included in the monitoring scheme.

• The **Custom IP** or **Custom Service** button (depending on the highlighted traffic filter type) enables you to include a specific user machine or a service that is not provided by the SmartCenter database.

When using **Filtering**, only traffic that matches at least one of the categories you have selected is displayed. For example, you configure the **Filter** to monitor **Top IP** and match **HTTP** and **Telnet** services. The view will display the following top IP machines that use either HTTP or Telnet. In addition, you can add another server machine by following these steps:

• In the **Monitor traffic that matches the below**, check the **Destination-Network Objects** box.

• Select the appropriate machine to be the destination (i.e. **London_Server**).

The **View** window displays a bar representing the following result: **Top** heaviest traffic consumer machines of **either** HTTP or Telnet traffic that is sent to the **London_Server**.
Blocking Real-Time Traffic

In This Chapter

Suspicious Activity Rules .......................... page 43
Managing Suspicious Activity Rules ............. page 45

Blocking Traffic

Blocking can be enabled through suspicious activity rules, which allow the system administrator to instantly block suspicious connections.

Suspicious Activity Rules

Suspicious Activity rules are security 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, can be applied immediately without the need to perform an Install Policy action.

There are two ways to block suspicious activity: using the Action menu or by right clicking in the Session View.

Using the Action menu

1. Select Action > Block Suspicious Activity. The Block Suspicious Activity window is displayed.

2. Select Apply On for either all VPN-1 & FireWall-1 modules or for a specific module.
In the **Source** section select *Any* to define blockage of all source machines or indicate a specific IP address/ network. If you would like to indicate a specific network source, define both the source machine’s IP and its netmask.

In the **Destination** section select *Any* to define 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 netmask. In the Service section either select *Any* for blocking all services or define the specific service you wish to block.

In the **Expiration** section either select time of expiration or check the box for defining an *Absolute Date and Time*.

Click the **Advanced** button to:

- Select either *Drop*, *Reject* or *Notify* in the **Action** drop-down list.
  - **Notify** – a notification about the defined activity will be sent but the activity will not be blocked.
  - **Drop** – will drop the packets without sending the communicating peer a notification.
  - **Reject** – will reject the packets while informing the communicating peer it had rejected it.

- Select *No Log*, *Log* or *Alarm* in the **Track** drop-down list.

- Check **Close Connections** in order to close all active connections that match the defined rule.

**By Right Clicking in the Session View**

The **Session View** allows you a quick way to block traffic by right clicking on its bar/line. This action opens up the **Block Suspicious Activity** window. This window will already have the appropriate settings of the particular session’s parameters you wish to block (either Service or IP parameters).

For example, assume you are viewing a session by **Top Services** on a specific client machine defined as a source and you wish to block KaZaA service simply right click on the KaZaA’s bar or line. The **Block Suspicious Activity** window is displayed. This window will already have the following settings:

- KaZaA service defined as the **Blocked** service.
- The client machine **IP** is defined as the source IP Address.
- **Any** in the destination field.

You can modify all the parameters in this session including the default **Expiration Date** and **Time**.
Managing Suspicious Activity Rules

Suspicious Activity rules are security rules, which, once they are set they can be applied immediately without the need to perform "Install Policy". These rules enable the system administrator to instantly block suspicious connections that are not restricted by the currently enforced Security Policy.

In the Enforced Suspicious Activity Rules window you can:
- View the rules that are currently being enforced on a module.
- Remove or add new rules.

There are two View types:
- Rules that are being enforced on the specific module.
- Rules that are being enforced on all of the modules.

To view these rules perform the following steps:
- From the main menu select Action
- Select Suspicious Activity Rules.

Note: Since the Suspicious Activity Rules View window provides a display of the currently enforced rules, if the system administrator adds a rule that is shadowed by another rule, the shadowed 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 drop rule, which is the dominant rule, will be displayed.
Virtual Link Monitoring (VLM)

In This Chapter

Overview page 47
Creating a Virtual Link page 48
Monitoring a Virtual Link page 52
Displaying Virtual Link Monitoring Data page 55
Virtual Link Monitoring Example page 57
Displaying Monitoring Data page 62

Overview

Virtual Link Monitoring allows you to monitor traffic between two Check Point VPN-1 Pro or FloodGate-1 Modules and to track compliance with a Service Level Agreement (SLA).

A Virtual Link is a path between two Check Point VPN-1 Pro or FloodGate-1 Modules (gateways), defined in SmartDashboard. You can monitor the following data on a Virtual Link:

- Committed Information Rate (CIR), or bandwidth
- Throughput loss, or bandwidth loss
- Round trip time

Monitoring a Virtual Link using SmartView Monitor requires the following:

- A Virtual Link between two gateways must first be created in the VPN-1 Pro SmartDashboard.
Creating a Virtual Link

To track compliance with SLA parameters, SLA parameters and Log and Alert parameters must also be defined in the SmartDashboard.

For information on creating a Virtual Link and defining SLA parameters and Log and Alert parameters, see “Creating a Virtual Link” on page 48.

- Once a Virtual Link has been created and its properties have been defined, you can use SmartView Monitor to monitor traffic between the two gateways that define the link.

For information on monitoring a Virtual Link, see “Monitoring a Virtual Link” on page 52.

For information on using SmartView Monitor to monitor other types of traffic, see Chapter 4, “Monitoring — Real-Time Traffic.

Creating a Virtual Link

To create a Virtual Link and define SLA parameters and Log and Alert parameters, proceed as follows:

1. In the SmartDashboard choose SmartView Monitor > Virtual Links from the Manage menu.

   The Virtual Links window is displayed (FIGURE 6-1).

   ![Virtual Links window](image)

   FIGURE 6-1 Virtual Links window

2. Click New and choose Virtual Link.

   The Virtual Link Properties window will be displayed.

3. In the General tab of Virtual Link Properties window (FIGURE 6-2 on page 50):
   - Specify the Name and Color of the Virtual Link. You may also include a Comment.
• Choose the **Virtual Link End Points**, the two gateways that define the Virtual Link.

• Check **Activate Virtual Link** to enable the Virtual Link.

For detailed information about the fields in the **General** tab, see “Virtual Link Properties Window — General Tab” on page 50.

4 In the **SLA Parameters** tab of the **Virtual Link Properties** window, define the following SLA parameters:

• **Thresholds** — limits on Committed Information Rate, bandwidth loss and/or round trip time. You may choose to be informed when these limits are violated.

**Note** • At least one SLA threshold must be defined for every Virtual Link.

• **SLA Statistics** — specify whether or not Virtual Link information will be logged in the Check Point SmartView Tracker.

For detailed information about the fields in the **SLA Parameters** tab, see “Virtual Link Properties Window — SLA Parameters Tab” on page 51.

5 Click **OK**.

The Virtual Link and its SLA Parameters have been defined.

6 Display the **Global Properties** window by choosing **Global Properties** from the **Policy** menu, or by clicking ![icon](image) in the SmartDashboard Toolbar.

7 Specify Log and Alert parameters in the **Log and Alert** page of the **Global Properties** window.

For information about the **Log and Alert** page, see “Global Properties Window — Log and Alert Page” on page 52.

8 Click **OK**.

**Editing or Deleting a Virtual Link**

After a Virtual Link has been created, you can edit its properties or delete it. Enter the **Virtual Links** window and select the link from the list of Virtual Links.

To delete the selected Virtual Link, click **Remove**.

To edit the selected Virtual Link, click **Edit** and redefine the desired parameters in the **General** and **SLA Parameters** tabs. You may go directly to these tabs by double-clicking the name of the Virtual Link in the SmartDashboard Objects Tree.
Creating a Virtual Link

When you close the SmartDashboard, you will be asked if you wish to save the changes you made.

**Virtual Link Properties Window — General Tab**

**FIGURE 6-2 Virtual Link Properties**

![Virtual Link Properties Window](image)

**Name** — the name of the Virtual Link

**Comment** — descriptive text

**Color** — the color of the Virtual Link's icon

**Virtual Link End Points** — Choose the two gateways that define the Virtual Link from the appropriate drop down menus:

- **End Point A** — This gateway must be internal, meaning that it is managed by the SmartCenter Server that the SmartDashboard is working with.

- **End Point B** — Gateway B can be internal or external.

Each of the gateways must have VPN-1Pro and SmartView Monitor installed. Before defining a gateway as an end point, display the **General** page of the **Workstation Properties** window for the gateway in the SmartDashboard. Verify that **VPN-1 & FireWall-1** is checked under **Check Point products installed**.
For example:

**FIGURE 6-3 E2ECP rule**

<table>
<thead>
<tr>
<th>NO</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>SERVICE</th>
<th>ACTION</th>
<th>TRACK</th>
<th>INSTALL ON</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Local_Gateway</td>
<td>Remote_Gateway</td>
<td>E2ECP</td>
<td>accept</td>
<td>Log</td>
<td>Install On</td>
</tr>
</tbody>
</table>

**Activate Virtual Link** — Specify whether or not the Virtual Link will be enabled.

If this option is not selected, you will not be able to monitor the Virtual Link using SmartView Monitor. The link will not appear in the *Monitored Virtual Link* list in the *Session Type* tab of the *Session Properties* window.

**Virtual Link Properties Window — SLA Parameters Tab**

**Thresholds** — Define the parameters for each gateway in the direction you wish to monitor.

For each of the traffic directions, you can:

- Check **Alert when Committed Information Rate is lower than...** and specify a rate in the corresponding text box. The **SLA Violation** action will be initiated when the CIR drops below the specified rate.

  For example, if your SLA guarantees a CIR of 10,000 Bps, you may wish to be alerted any time CIR drops below 10,000 Bps.

- Check **Alert when bandwidth loss exceeds...** and specify a percentage in the corresponding text box. The **SLA Violation** action will be initiated when bandwidth loss exceeds the specified percentage.

  For example, if your SLA states that bandwidth loss will not exceed 22 percent, you can choose to be informed when this occurs.

If you check and define both a CIR limit and a bandwidth loss percentage, the CIR violation alert will be based on the remaining percentage of the bandwidth.

For example, if you define a CIR limit of 10,000 Bps and a bandwidth loss limit of 5%, the CIR alert will be triggered when the CIR drops below 95% of 10,000 Bps (9,500 Bps).
For round trip traffic, you can check **Alert when round trip time exceeds...** and specify a time limit in the corresponding text box. The **SLA Violation** action will be initiated when round trip time exceeds the specified limit.

You can also check **Alert when disconnected** to ensure that you are informed if the connection between the two end points of the Virtual Link is disconnected.

**Note** - “Alert...” in this tab refers to the **SLA Violation** track option specified under **Track Options** in the **Log and Alert** page of the **Global Properties** window (see “Global Properties Window — Log and Alert Page” on page 52).

**Log SLA values** — Specify whether or not Virtual Link information will be logged in the Check Point SmartView Tracker.

The frequency with which statistics will be logged is specified by **Virtual Link statistics logging interval** in the **Log and Alert** page of the **Global Properties** window (see “Global Properties Window — Log and Alert Page” on page 52).

For information regarding the SmartView Tracker, see the **Check Point SmartCenter Guide**.

**Note** - An alert will be sent when thresholds return to an acceptable range.

---

**Global Properties Window — Log and Alert Page**

The **Log and Alert** page allows you to define system-wide logging and alerting parameters. The following fields define SLA-related parameters:

**SLA violation** (under **Track Options**) — Choose the action to be taken if one of the thresholds defined in the **SLA Parameters** tab of the **Virtual Links** window (FIGURE 6-2 on page 50) is violated.

**Virtual Link statistics logging interval** (under **Time Settings**) — Set the frequency with which SLA statistics will be logged.

This parameter is relevant only for Virtual Links with **Log SLA Statistics** checked in the **SLA Parameters** tab of the **Virtual Link Properties** window.

**Monitoring a Virtual Link**

To monitor a Virtual Link, proceed as follows:

1. Select **Real Time** Mode in the **Session Type** tab of the **Session Properties** window.
2 Select **Virtual Link** under **Monitor** in the **Session Type** tab of the **Session Properties** window (FIGURE 6-4). Select a Virtual Link under **Monitored Virtual Link**.

Only one Virtual Link can be monitored at any given time.

**FIGURE 6-4** Session Properties window — Session Type tab (Virtual Link)

3 In the **Virtual Link Monitoring** tab, specify the data to display.

For information about the fields in the **Virtual Link Monitoring** tab, see “Session Properties Window — Virtual Link Monitoring Tab” on page 54.

4 In the **Settings** tab, specify the display parameters for the session.

For information on the **Settings** tab in Virtual Link Monitoring, see “Change the Display — Settings Tab” on page 19.
Session Properties Window — Virtual Link Monitoring Tab

FIGURE 6-5 Session Properties window — Virtual Link Monitoring tab

Displayed Data — Choose the type and direction of data to display.

Select one of the following:

- **Bandwidth** — the effective bandwidth.
- **Bandwidth Loss** — the difference between the transmission rate and the receiving rate.

If you choose **Bandwidth** or **Bandwidth Loss**, use the arrow button to select the direction that you wish to monitor. Clicking an arrow button will toggle the monitoring direction between the following options:

- Monitor in both directions.
- Monitor from Gateway A to Gateway B.
- Monitor from Gateway B to Gateway A.

- **Round Trip Time** — the time required to make the round trip between the gateways.

Data Type — Select one of the following:
• **Application Data** — the data as the application sees it, uncompressed and unencrypted.

For example, if you were interested in the amount of data sent out in its original form you would choose to monitor using **Application Data**.

• **Wire Data** — the data on the wire, after compression or encryption.

To see how much data was actually transferred in its compressed or encrypted form, in order to compare with SLA guarantees for example, you would choose **Wire Data**.

**Settings Tab — Virtual Link Monitoring**

The **Chart Type** and **Scaling** fields of the **Settings** tab are identical when monitoring a Virtual Link and monitoring an interface.

For more information on these fields, see “Change the Display — Settings Tab” on page 19.

When you monitor a Virtual Link, the **Measurement** options depend on the data you have chosen to display, as follows:

• **Bandwidth** — You can choose **Data Transfer Rate** or **Packets per Second**.

  If you choose **Data Transfer Rate**, specify the units in the corresponding drop down menu.

• **Bandwidth Loss** — **Percent** is the only measurement option.

• **Round Trip Time** — **Milliseconds** is the only measurement option.

**Displaying Virtual Link Monitoring Data**

After you define monitoring parameters in the tabs of the **Session Properties** window, save the Session definitions or click **OK** to view monitoring data without saving.

**Virtual Link Monitoring Display**

SmartView Monitor displays traffic data for the selected Virtual Link. **FIGURE 6-6** on page 56 shows the percentage of bandwidth loss between Local Gateway and Remote Gateway, in both directions.

With the exception of displaying traffic statistics within a Virtual Link, rather than for a single interface, the **Virtual Link Monitoring** display is identical to the **Interface Monitoring** display.
Displaying Virtual Link Monitoring Data

**FIGURE 6-6** SmartView Monitor — Virtual Link Monitoring

If you have chosen to monitor *Bandwidth Loss* within a Virtual Link in the **Virtual Link Monitoring** tab, you may also choose to display SLA data. This will show the upper limit for bandwidth loss, as defined in the **SLA Parameters** tab of the **Virtual Link Properties** window in the SmartDashboard.

For example, FIGURE 6-6 shows traffic data for the Virtual Link between Local Gateway and Remote Gateway. **Show SLA Data** is checked, at 25 percent bandwidth loss for traffic from Local Gateway to Remote Gateway, and 10 percent for traffic in the opposite direction. The line graph shows that the 10 percent limit has been exceeded, initiating the **SLA Violation** action defined in the **Log and Alert** page of the **Global Properties** window (see “Global Properties Window — Log and Alert Page” on page 52).

SLA data will be shown by default when the display window opens. To remove this data from the graph, uncheck **Show SLA Data** in the **Monitor** menu.
SmartView Tracker

If **Log SLA Statistics** is checked in the **SLA Parameters** tab of the **Virtual Link Properties** window, Virtual Link data will be shown in the SmartView Tracker regardless of whether or not the Virtual Link is being monitored (see FIGURE 6-7).

The data in the SmartView Tracker will include high, low, and average watermarks for bandwidth loss and CIR, in both directions, as well as round trip time.

**FIGURE 6-7 Virtual Link Statistics in the SmartView Tracker**

In addition, if the SLA violation action defined in the **Log and Alert** page of the **Global Properties** window is **Log**, then SLA violations will also be shown in the SmartView Tracker. For general information about the SmartView Tracker, see the *Check Point SmartCenter Guide*.

Virtual Link Monitoring Example

The following section presents an example of how to set up and monitor a Virtual Link.

Consider a Virtual Link between **Local Gateway** and **FireWall ExtraNet**, for which you wish to:

- Monitor bandwidth loss in the direction from **Local Gateway** to **FireWall ExtraNet**.
- Be informed when bandwidth loss exceeds 25 percent.
- Log SLA statistics.
- Display monitoring and SLA data in a line graph.

Begin by defining the Virtual Link and its SLA and log parameters in the SmartDashboard:

1. Choose **Virtual Links** from the **Manage** menu. You can also click ![Virtual Links button](image) in the SmartDashboard Toolbar.
Virtual Link Monitoring Example

The **Virtual Links** window is displayed (FIGURE 6-1 on page 48)

2. Click **New** and choose **Virtual Link**.

3. In the **General** tab of **Virtual Link Properties** window (FIGURE 6-8 on page 58):
   - Define a name, description, and color for the Virtual Link.
   - Define the Virtual Link End Points, such that **Local Gateway** is **Gateway A**, and **FireWall ExtraNet** is **Gateway B**.
   - Check **Activate Virtual Link**.

**FIGURE 6-8 Virtual Link Properties window — General tab (example)**

4. In the **SLA Parameters** tab of **Virtual Link Properties** window (FIGURE 6-9 on page 59):
   - For the direction **Local Gateway** to **FireWall ExtraNet**, check **Inform when bandwidth loss exceeds** and define a 25 percent bandwidth loss limit.
   - Check **Log SLA statistics**.
5 Click **OK**.

The Virtual Link and its SLA Parameters have been defined.

6 Open the **Global Properties** window by choosing **Global Properties** from the **Policy** menu, or by clicking ![Global Properties](image) in the SmartDashboard Toolbar.

7 In the **Log and Alert** page of the **Global Properties** window:
   - Select **Log** from the **SLA Violation** drop-down menu.
   - Leave **Virtual Link statistics logging interval** at its default value of 60 seconds.

8 Click **OK**.

The Log parameters for the Virtual Link have been defined.

Now, the Virtual Link may be monitored using the SmartView Monitor:

1 Choose **New** from the **File** menu.

   The **Session Type** window is displayed.

2 In the **Session Type** tab (FIGURE 6-10):
   - Select **Monitor a Virtual Link**.
   - Select **Local ExtraNet** under **Monitored Virtual Link**.
3 In the **Virtual Link Monitoring** tab (FIGURE 6-11 on page 61):
   • Select **Bandwidth Loss**.
   • Set the monitoring direction to **Local ExtraNet** by clicking on the arrow button.
In the **Settings** tab:

- Select **Line** under **Chart Type**.
- Select **Set Default Scaling**.

Measurement will automatically be set to **Percent** when **Bandwidth Loss** is selected.

5. Click **OK**.
   You will be asked if you wish to save the configuration.

6. Click **Yes**.

7. In the **Save As** window, enter a name for the configuration.

8. Click **OK**.

Percent bandwidth loss from Local Gateway to FireWall ExtraNet is displayed (FIGURE 6-12 on page 62).

To view the bandwidth loss SLA parameter on the graph, choose **Show SLA Data** from
the **Monitor** menu.
Displaying Monitoring Data

To change monitoring or display parameters, you may open the Session Properties window at any time during the monitoring session.

For more information on how to set up and monitor a configuration, see “Creating a Virtual Link” on page 48, and “Monitoring a Virtual Link” on page 52.

Displaying Monitoring Data

After you define monitoring parameters in the tabs of the Session Properties window, save the session definitions or click OK to view monitoring data without saving.
Virtual Link Monitoring

FIGURE 6-13 Virtual Link Monitoring

FIGURE 6-13 shows how SmartView Monitor can be used to monitor a Virtual Link. The graph displays bandwidth loss within the Virtual Link between Local Gateway and Remote Gateway, in both directions. Also present on the graph are SLA parameters that specify bandwidth loss upper limits at 25% for traffic from Local Gateway to Remote Gateway and 10% for traffic in the opposite direction.

The graph shows us that the percentage of bandwidth loss in traffic going from Local Gateway to Remote Gateway often exceeds the SLA guarantee of no more than 10% bandwidth loss.
Report Mode

Overview

SmartView Monitor allows you to make reports of monitored events. These reports allow you to specify and recall any past traffic and to create a monitored report retrospectively. You can get reports for the last hour, the previous day, the last month and even a report from when the system was installed. The events that can be monitored include any of the following:

- Check Point System Counters.
- Traffic reports show the distribution of outbound traffic per specified module by one of the following factors: Services, Network Objects or IP Addresses, FireWall-1 rules and FloodGate-1 rules, and time period of report (Last Week reports).

Configuration

SmartView Monitor reports are configured in the following manner:

In the SmartDashboard:

1. In the Check Point Gateway window, select SmartView Monitor in the Check Point Products listbox. The SmartView Monitor branch is added to the object tree.
2. Select the SmartView Monitor branch in the Object's tree and configure the settings for SmartView Monitor reports displayed in the SmartView Monitor page.
When you choose to create reports for a specified module, you should be aware that the reports creation process may affect the performance of the module. Therefore, you can choose to enable or disable the reports creation in the **SmartView Monitor** page of the object’s window:

- **Checkpoint System Counters** — check this field in order to enable the creation of System Counters reports.
- **Traffic Connections** — check this field in order to enable the creation of reports regarding number of traffic connections established.
- **Traffic Throughput** — check this field in order to enable the creation of reports regarding the volume/duration of connected traffic.

In the SmartView Monitor:

4 In the **Session > Properties > Sessions Type & Target** tab, select **Real-Time** as the **Monitor Mode**, select whether you would like to monitor by **Check Point Session Counters** or by **Traffic**. Configure the following pages, depending on what you have chosen to monitor, and click **OK** to display the report monitor.

---

**Report Mode — Check Point System Counters**

**FIGURE 7-1 Session Properties window — Session Type tab (Check Point System Counters)**
To set up Report monitoring:

1. Select **Real-Time** in the **Session Type & Target Type** tab of the **Session Properties** window.

2. Select **Check Point System Counters** in the **Monitor Type** tab of the **Session Properties** window.

3. Select a module under **Monitored Module**. Only one interface can be monitored at any given time.

4. Configure the **Counters** tab.

   For information about the fields in the **Counters** tab, see “Session Properties Window — Counters Tab” on page 67.

When the Check Point System parameters have been set up, you can begin the monitoring display, (see “Displaying Reports — Traffic” on page 69).

### Session Properties Window — Counters Tab

**FIGURE 7-2** Session Properties window — Report, Counters tab

**Time Frame** — specify the time frame from which the report is to be created.
Counters Category — select categories to be monitored. Click on Add to send them to the Selected Counters listbox, or click on Delete to delete them from the Selected Counters listbox.

Read indepth information about a selected counter category in the Detailed description listbox.

Displaying Reports — Check Point System Counters

After you define monitoring parameters in the tabs of the Session Properties window, save the session definitions or click OK to view monitoring data without saving.

See “Example — Check Point System Counters” on page 24.

Report Mode — Traffic

FIGURE 7-3 Session Properties window — Session Type tab (interfaces)

To set up SmartView Monitor for monitoring an interface:

1. Select History Report in the Monitor Type tab of the Session Properties window.
2. Select Traffic from the Session Properties window.
3 Select an interface under Select Monitored Module/Interface.
Only one interface can be monitored at any given time.

4 Configure the Traffic History tab, see “Session Properties Window — Traffic History Tab” on page 69.

When the interface monitoring parameters have been set up, you can begin the monitoring display.

**Session Properties Window — Traffic History Tab**

**FIGURE 7-4** Session Properties window — Traffic History tab

- **Module** — displays the module that you selected.
- **Time Frame** — specify the time frame from which the report is to be created.
- **Select a report** — select the report that is relevant to the traffic that you would like to monitor.

**Displaying Reports — Traffic**

After you define monitoring parameters in the tabs of the Session Properties window, save the session definitions or click OK to view monitoring data without saving.

See “Monitoring by Top Security Rules” on page 37.
Report Mode — Traffic
CHAPTER 8

Graphical User Interface

Check Point SmartView Options
SmartView Monitor Toolbars
SmartView Monitor Status Bar

Check Point SmartView Options

File Options

TABLE 8-1 File Options

<table>
<thead>
<tr>
<th>Options</th>
<th>Toolbar Button</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Window</td>
<td></td>
<td>Define the configuration of a new monitoring session.</td>
<td>“Defining a SmartView Monitor Session” on page 14.</td>
</tr>
<tr>
<td>Export View</td>
<td>none</td>
<td>Export to file.</td>
<td></td>
</tr>
<tr>
<td>Exit</td>
<td>none</td>
<td>Close the SmartView Monitor.</td>
<td></td>
</tr>
</tbody>
</table>
### Action Options

<table>
<thead>
<tr>
<th>Options</th>
<th>Toolbar Button</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Suspicious Activity</td>
<td>![Image]</td>
<td>Block suspicious activity.</td>
<td>“Suspicious Activity Rules” on page 43.</td>
</tr>
</tbody>
</table>

### Session Options

<table>
<thead>
<tr>
<th>Options</th>
<th>Toolbar Button</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>![Image]</td>
<td>Start a new monitoring session.</td>
<td>“Starting SmartView Monitor Sessions” on page 11.</td>
</tr>
<tr>
<td>Run</td>
<td>none</td>
<td>Run a monitoring session for a selected Module.</td>
<td>“Defining a SmartView Monitor Session” on page 14.</td>
</tr>
<tr>
<td>Rename</td>
<td>none</td>
<td>Rename a monitoring session.</td>
<td></td>
</tr>
<tr>
<td>Copy</td>
<td>none</td>
<td>Copy a monitoring session’s configuration.</td>
<td></td>
</tr>
<tr>
<td>Paste</td>
<td>none</td>
<td>Paste a monitoring session’s configuration.</td>
<td></td>
</tr>
<tr>
<td>Undo Changes</td>
<td>none</td>
<td>Undo changes to a monitoring session’s configuration.</td>
<td></td>
</tr>
<tr>
<td>Delete</td>
<td>none</td>
<td>Delete a monitoring session.</td>
<td></td>
</tr>
</tbody>
</table>
### TABLE 8-3 Session Options

<table>
<thead>
<tr>
<th>Options</th>
<th>Toolbar Button</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save All</td>
<td>none</td>
<td>Save all the configurations of the current monitoring session.</td>
<td>“Monitoring Services” on page 26.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“Monitoring Network Objects” on page 28.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“Filtering Traffic” on page 41.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>“Monitoring Check Point System Counters” on page 22.</td>
</tr>
<tr>
<td>Save</td>
<td>![Image]</td>
<td>Save the current configuration of the current monitoring session.</td>
<td></td>
</tr>
<tr>
<td>Properties</td>
<td>![Image]</td>
<td>Change a session’s configuration.</td>
<td></td>
</tr>
</tbody>
</table>
# Recording Options

**TABLE 8-4 Recording Options**

<table>
<thead>
<tr>
<th>Options</th>
<th>Toolbar Button</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record</td>
<td><img src="image" alt="Record Icon" /></td>
<td>Record a monitoring session</td>
<td>“Recording Monitoring Sessions” on page 15.</td>
</tr>
<tr>
<td>Stop</td>
<td><img src="image" alt="Stop Icon" /></td>
<td>Stop recording a monitoring session or playing a recorded session.</td>
<td>“To stop recording a monitoring session or a playing a previously recorded session” on page 15.</td>
</tr>
<tr>
<td>Play</td>
<td><img src="image" alt="Play Icon" /></td>
<td>Play a previously recorded session</td>
<td>“To play a previously recorded session” on page 15.</td>
</tr>
<tr>
<td>Fast Play</td>
<td><img src="image" alt="Fast Play Icon" /></td>
<td>Fast play a previously recorded session.</td>
<td>“To fast play a previously recorded session” on page 15.</td>
</tr>
<tr>
<td>Pause</td>
<td><img src="image" alt="Pause Icon" /></td>
<td>Pause playing a previously recorded session.</td>
<td>“To pause playing” on page 16.</td>
</tr>
</tbody>
</table>

# View Options

**TABLE 8-5 View Options**

<table>
<thead>
<tr>
<th>Options</th>
<th>Toolbar Button</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optimize Scaling</td>
<td><img src="image" alt="Optimize Icon" /></td>
<td>Optimize the scaling range in the display.</td>
<td>“Scaling” on page 17. “Changing the display using other SmartConsole options” on page 20</td>
</tr>
<tr>
<td>Freeze View</td>
<td><img src="image" alt="Freeze Icon" /></td>
<td>Freeze a monitoring session.</td>
<td>“Viewing Monitored Information” on page 16.</td>
</tr>
<tr>
<td>Chart Type</td>
<td><img src="image" alt="Chart Icon" /></td>
<td>Select chart display: Line - <img src="image" alt="Line Icon" /> Bar - <img src="image" alt="Bar Icon" /></td>
<td>“Enabling Graph Values Display” on page 17.</td>
</tr>
</tbody>
</table>
### Table 8-5: View Options

<table>
<thead>
<tr>
<th>Options</th>
<th>Toolbar Button</th>
<th>Description</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bar Properties</td>
<td>none</td>
<td>Select Bar Chart properties.</td>
<td></td>
</tr>
<tr>
<td>Line Properties</td>
<td>none</td>
<td>Select Line Chart properties.</td>
<td></td>
</tr>
<tr>
<td>Toolbar</td>
<td>none</td>
<td>Toggle the display of the toolbars.</td>
<td></td>
</tr>
<tr>
<td>Status Bar</td>
<td>none</td>
<td>Toggle the display of the status bar.</td>
<td></td>
</tr>
<tr>
<td>Show SLA Data</td>
<td>none</td>
<td>Toggle the display of SLA data.</td>
<td></td>
</tr>
<tr>
<td>Show Tree</td>
<td></td>
<td>Toggle the display of the object tree</td>
<td></td>
</tr>
</tbody>
</table>

### Table 8-6: Window Options

<table>
<thead>
<tr>
<th>Options Entry</th>
<th>Toolbar Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartDashboard</td>
<td>none</td>
<td>Open the SmartDashboard.</td>
</tr>
<tr>
<td>SmartView Status</td>
<td>none</td>
<td>Open the SmartView Status.</td>
</tr>
<tr>
<td>SmartView Tracker</td>
<td>none</td>
<td>Open the SmartView Tracker.</td>
</tr>
<tr>
<td>SmartView Reporter</td>
<td>none</td>
<td>Open SmartView Reporter.</td>
</tr>
<tr>
<td>SecureClient Packaging Tool</td>
<td>none</td>
<td>Open SecureClient Packaging Tool.</td>
</tr>
<tr>
<td>User Monitor</td>
<td>none</td>
<td>Open the User Monitor.</td>
</tr>
<tr>
<td>SmartLSM</td>
<td>none</td>
<td>Open SmartLSM.</td>
</tr>
<tr>
<td>SmartUpdate</td>
<td>none</td>
<td>Open SmartUpdate.</td>
</tr>
</tbody>
</table>
## Help Options

**TABLE 8-7 Help Options**

<table>
<thead>
<tr>
<th>Options Entry</th>
<th>Toolbar Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help Topics</td>
<td>none</td>
<td>Display Help.</td>
</tr>
<tr>
<td>About Check Point SmartView Monitor</td>
<td>none</td>
<td>Display the <em>About Check Point SmartView Monitor</em> window.</td>
</tr>
</tbody>
</table>
SmartView Monitor Toolbars

The toolbar buttons are shortcuts for the following Options commands:

**Standard Toolbar**

**TABLE 8-8** Standard toolbar

<table>
<thead>
<tr>
<th>Toolbar Button</th>
<th>Options Command</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Session &gt; Properties" /></td>
<td>Session &gt; Properties</td>
<td>Open the Session Properties window.</td>
</tr>
<tr>
<td><img src="image" alt="File &gt; Save" /></td>
<td>File &gt; Save</td>
<td>Save the current configuration of the current monitoring session.</td>
</tr>
<tr>
<td><img src="image" alt="View &gt; Chart Type &gt; Line Graph" /></td>
<td>View &gt; Chart Type &gt; Line Graph</td>
<td>Display online data as a line graph.</td>
</tr>
<tr>
<td><img src="image" alt="View &gt; Chart Type &gt; Bar Graph" /></td>
<td>View &gt; Chart Type &gt; Bar Graph</td>
<td>Display online data as a vertical bar graph.</td>
</tr>
<tr>
<td><img src="image" alt="Action &gt; Suspend QoS Policy" /></td>
<td>Action &gt; Suspend QoS Policy</td>
<td>Toggle the suspension of the QoS Policy.</td>
</tr>
<tr>
<td><img src="image" alt="View &gt; Interrupt Monitoring" /></td>
<td>View &gt; Interrupt Monitoring</td>
<td>Resume or interrupt SmartView Monitor.</td>
</tr>
<tr>
<td><img src="image" alt="none" /></td>
<td>none</td>
<td>Enter upper and lower scaling range limits.</td>
</tr>
<tr>
<td><img src="image" alt="Monitor &gt; Optimize Scaling" /></td>
<td>Monitor &gt; Optimize Scaling</td>
<td>Optimize the scaling range in the display.</td>
</tr>
<tr>
<td><img src="image" alt="Help &gt; Help Topics" /></td>
<td>Help &gt; Help Topics</td>
<td>Click this button. The mouse pointer changes to an arrow and question mark. Then click a field or a toolbar button. The Help topic is displayed for the item you clicked.</td>
</tr>
<tr>
<td><img src="image" alt="Recording &gt; Record" /></td>
<td>Recording &gt; Record</td>
<td>Record a monitoring session.</td>
</tr>
</tbody>
</table>
The SmartView Monitor status bar, displayed at the bottom of the SmartView Monitor window, shows information on the state of SmartView Monitor, as well as explanations of Options items and toolbar buttons.

<table>
<thead>
<tr>
<th>Toolbar Button</th>
<th>Options Command</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Recording &gt; Stop" /></td>
<td>Recording &gt; Stop</td>
<td>Stop recording a monitoring session or playing a recorded session.</td>
</tr>
<tr>
<td><img src="image" alt="Recording &gt; Play" /></td>
<td>Recording &gt; Play</td>
<td>Play a previously recorded session.</td>
</tr>
<tr>
<td><img src="image" alt="Recording &gt; Fast Play" /></td>
<td>Recording &gt; Fast Play</td>
<td>Fast play a previously recorded session.</td>
</tr>
<tr>
<td><img src="image" alt="Recording &gt; Pause" /></td>
<td>Recording &gt; Pause</td>
<td>Pause playing a previously recorded session.</td>
</tr>
</tbody>
</table>
SmartView Monitor
Command Line Interface

The following command line commands relate to SmartView Monitor and are documented in the Command Line Interface (CLI) Guide.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTM</td>
<td>This command and all its derivatives are used to execute SmartView Monitor operations.</td>
</tr>
<tr>
<td>rtm debug</td>
<td>This command sends debug printouts to the $FWDIR/log/rtmd.elg file.</td>
</tr>
<tr>
<td>rtm drv</td>
<td>This command starts, stops or checks the status of the SmartView Monitor kernel driver.</td>
</tr>
<tr>
<td>rtm monitor - Interface Monitoring</td>
<td>This command starts the monitoring process and specifies parameters for monitoring an interface.</td>
</tr>
<tr>
<td>rtm monitor - Virtual Link Monitoring</td>
<td>This command starts the monitoring process and specifies parameters for monitoring a Virtual Link.</td>
</tr>
<tr>
<td>rtm rtmd</td>
<td>This command starts the SmartView Monitor daemon manually. This also occurs manually when rtmstart is run.</td>
</tr>
<tr>
<td>rtm stat</td>
<td>This command displays the general SmartView Monitor status. In addition, it displays the status of the daemon, driver, opened views and active virtual links.</td>
</tr>
</tbody>
</table>
### SmartView Monitor Command Line Interface

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rtm ver</td>
<td>This command displays the SmartView Monitor version.</td>
</tr>
<tr>
<td>rtmstart</td>
<td>This command loads the SmartView Monitor kernel module and starts the SmartView Monitor daemon.</td>
</tr>
<tr>
<td>rtmstop</td>
<td>This command kills the SmartView Monitor daemon and unloads the SmartView Monitor kernel module.</td>
</tr>
</tbody>
</table>
Index

A
Aggregate Data 16
Alert when disconnected 52
application data 55

B
bandwidth
monitoring for Virtual Links 47
selecting direction 54
bandwidth loss
defining limit 51
monitoring for Virtual Links 47
selecting direction 54
showing SLA data 56
bar graph
selection 19

C
capture screen
Lock 16
chart type
selection 19
CIR 7
defining limit 51
Committed Information Rate
see CIR 7

data
application 55
changing display 18
direction 27, 29
displayed 23, 29, 54
in Log Manager 57
showing SLA data 56
type 54

E
E2ECP
rule example 51
service 51
example
Counters 24

F
Fast playing
a previously recorded session 15

G
graph
enabling values 17
graph values
enabling 17

I
interface
Interface Monitoring tab 27, 28, 67
Module Selection tab 26, 28, 60, 68
Monitoring Type tab 22
Internet Service Providers
see ISPs 7

L
Legend 16
Aggregate 30
Change Y scale 24
line graph
selection 19
Lock 16
log
Global Properties - Log and Alert page 52
Log Manager 57
logging interval 52
SLA statistics 52

M
measurement
for Virtual Links 55
selection 19
menu options
using to change display 20
Menus
File 71
Help 76
Monitor 72
Window 75
Modify Y Scale 24
Monitored Information
viewing 16
Monitoring Session
interrupt 17

N
Network Objects
add 23, 27, 29
destination 30
remove 23, 27, 29
source 30

O
Optimize Scaling 31

P
pause playing
a monitoring session 16
playing
a previously recorded session 15

Q
QoS Policy
installed policy 34, 38
suspending 36
QoS Rules
Monitor by QoS Rules tab 33
monitoring by 25
selecting main 34

R
recording
a monitoring session 15
reports
Check Point System
Counters 65
configure in
SmartDashboard 65
monitored events 65
traffic report 68
traffic reports 65
round trip time
defining limit 52
monitoring for Virtual Links 47

S
Scaling
setting default 17
scaling
setting default 19
setting range 20
toolbar 17
scroll bar 17
Service Level Agreement
see SLA 7
Services
add 23, 27, 29
remove 23, 27, 29
Session
interrupt 17
session configuration
defining 14
Session Properties 14
Interface Monitoring tab 27,
28, 67
Monitor by QoS Rules tab 33,
38
saving definitions 23, 62, 68, 69
settings
tab 19
View Settings tab 26, 28
Virtual Link Monitoring tab 54
SLA
defining violation action 52
definition of 7
logging statistics 52
monitoring compliance 47
showing SLA data 56
thresholds 51
SmartDashboard
Global Properties - Log and
Alert page 49, 52
SmartView Monitor page 65
tracking SLA parameters 48
Virtual Links window 48
SmartView
Legend 16
Report Mode 65
SmartView Monitor
Check Point System
Counters 22
configuration session 14
Login window 11
measurement options 19
Scaling 17, 19
starting 11
SmartView Tracker 57
source
network object as 30
status bar 78
stop recording or playing
a monitoring session 15
suspend QoS Policy 36

T
Toolbar
Scaling 17
Standard 77
using to change display 20
Traffic Monitoring
by network object 25
by QoS Rules 25, 32
by service 25
data direction 27, 29
display 62
Interface Monitoring tab 27, 28
through a single interface 25

V
View Settings 22
View Settings tab 22
Virtual Link
activating 51
creating 48
defining SLA parameters 49
display data 54
editing 49
endpoint gateway
requirements 50
endpoints 50
log and alert parameters 49
monitoring 52
monitoring display 55
monitoring tab 54
naming 50
statistics logging interval 52
Virtual Link Monitoring
E2ECP Rule 51
example 57
measurement options 19, 55
monitoring example 63
monitoring options 47
requirements 48
scaling 19
selecting monitored link  53
View Settings  55

window
Session Properties
Interface Monitoring
tab 23
windows
Counters 23
Global Properties
Log and Alert page 49, 52
Session Properties 14
Interface Monitoring
tab 27, 28, 67
Module Selection tab 22, 26, 28, 60, 61, 66, 68
Monitor by Network
Objects 29
Monitor by QoS Rules
tab 33, 38
Monitor by Services 27
View Settings tab 22, 26, 28
Virtual Link Monitoring
tab 54
SmartView Monitor
Login 11
page 65
Traffic History 69
Virtual Link Properties
General tab 48, 50
SLA Parameters tab 49, 51
Virtual Links window 48
wire data 55