CHAPTER 39

Viewing Router Information

The Cisco Router and Security Device Manager (Cisco SDM) Monitor mode lets you view a current snapshot of information about your router, the router interfaces, the firewall, and any active VPN connections. You can also view any messages in the router event log.

Note The Monitor window is not dynamically updated with the latest information. To view any information that has changed since you brought up this window, you must click **Update**.

Monitor mode works by examining the router log and by viewing the results of Cisco IOS **show** commands. For Monitor mode functions that are based on log entries, such as firewall statistics, logging must be enabled. Logging is enabled by default by Cisco SDM, but you can change that setting using the **Additional Tasks > Router Properties > Logging** window. In addition, individual rules may need configuration so that they generate log events. For more information, see the help topic How Do I View Activity on My Firewall?

If you want to:	Do this:
View information about router interfaces.	From the toolbar, click **Monitor**, and then in the left frame, click **Interface Status**. From the Select Interface field select the interface for which you want to view information, then in the Available Items group, select the information you want to view. Then click **Show Details**.
View graphs of CPU or memory usage.	From the toolbar, click **Monitor**. The Overview page includes graphs of CPU usage and memory usage.
View information about the firewall.	From the toolbar, click **Monitor**, and then in the left frame, click **Firewall Status**.
View information about VPN Connections	From the toolbar, click **Monitor**, and then in the left frame, click **VPN Status**. Then select the tab for IPSec Tunnels, DMVPN Tunnels, Easy VPN Servers, or IKE SAs.
View messages in the router event log.	From the toolbar, click **Monitor**, and then in the left frame, click **Logging**.

Overview

The Monitor mode Overview screen displays an overview of your router activity and statistics, and serves as a summary of the information contained on the other Monitor mode screens. It contains the information described in this help topic.

Note If you do not see feature information described in this help topic on the Overview screen, the Cisco IOS image does not support the feature. For example, if the router is running a Cisco IOS image that does not support security features, the Firewall Status, and VPN status sections do not appear on the screen.

Launch Wireless Application Button

If the router has radio interfaces, you can click this button to monitor and configure radio interfaces. The Monitor Overview window provides interface status information for these interfaces, but radio interfaces are not listed in the Monitor Interface Status window.

This button does not appear if the router does not have radio interfaces.

Update Button

Retrieves current information from the router, updating statistics displayed by this screen.

Resource Status

Shows basic information about your router hardware and contains the following fields:

CPU Usage

Shows the percentage of CPU usage.

Memory Usage

Shows the percent of RAM usage.

Flash Usage

Shows the available flash over the amount of flash installed on the router.

Interface Status

Shows basic information about the interfaces installed on the router and their status.

Note Only interface types supported by Cisco SDM are included in these statistics. Unsupported interfaces will not be counted.

Total Interface(s) Up

The total number of enabled (up) interfaces on the router.

Total Interface(s) Down

The total number of disabled (down) interfaces on the router.

Interface

The interface name.

IP

The IP address of the interface.

Status

The status of the interface, either Up, or Down.

Bandwidth Usage

The percent of interface bandwidth being used.

Description

Available description for the interface. Cisco SDM may add descriptions such as $FW_OUTSIDE$ or ETH_LAN.

Firewall Status Group

Shows basic information about the router resources and contains the following fields:

Number of Attempts Denied

Shows the number of log messages generated by connection attempts (by protocols such as Telnet, HTTP, ping, and others) rejected by the firewall. Note that in order for a log entry to be generated by a rejected connection attempt, the access rule that rejected the connection attempt must be configured to create log entries.

Firewall Log

If enabled, shows the number of firewall log entries.

QoS

The number of interfaces with an associated QoS policy.

VPN Status Group

Shows basic information about the router resources and contains the following fields:

Number of Open IKE SAs

Shows the number of IKE Security Associations (SAs) connections currently configured and running.

Number of Open IPSec Tunnels

Shows the number of IPSec Virtual Private Network (VPN) connections currently configured and running.

No. of DMVPN Clients

If the router is configured as a DMVPN hub, the number of DMVPN clients.

No. of Active VPN Clients

If the router is configured as an EasyVPN Server, this field shows the number of Easy VPN Remote clients.

NAC Status Group

Shows a basic snapshot of Network Admission Control (NAC) status on the router.

No. of NAC enabled interfaces field

The number of router interfaces on which NAC is enabled.

No. of validated hosts field

The number of hosts with posture agents that have been validated by the admissions control process.

Log Group

Shows basic information about the router resources and contains the following fields:

Total Log Entries

The total number of entries currently stored in the router log.

High Severity

The number of log entries stored that have a severity level of 2 or lower. These messages require immediate attention. Note that this list will be empty if you have no high severity messages.

Warning

The number of log entries stored that have a severity level of 3 or 4. These messages may indicate a problem with your network, but they do not likely require immediate attention.

Informational

The number of log entries stored that have a severity level of 6 or higher. These information messages signal normal network events.

Interface Status

The Interface Status screen displays the current status of the various interfaces on the router, and the numbers of packets, bytes, or data errors that have travelled through the selected interface. Statistics shown on this screen are cumulative since the last time the router was rebooted, the counters were reset, or the selected interface reset.

Monitor Interface and Stop Monitoring Button

Click this button to start or stop monitoring the selected interface. The button label changes based on whether Cisco SDM is monitoring the interface or not.

Test Connection Button

Click to test the selected connection. A dialog appears that enables you to specify a remote host to ping through this connection. The dialog then reports on the success or failure of the test. If the test fails, information about why the test may have failed is given, along with the steps you need to take to correct the problem.

Interface List

Select the interface for which you want to display statistics from this list. The list contains the name, IP address and subnet mask, the slot and port it is located in, and any Cisco SDM or user description entered.

Select Chart Types to Monitor Group

These check boxes are the data items for which Cisco SDM can show statistics on the selected interface. These data items are as follows:

- Packet Input—The number of packets received on the interface.
- Packet Output—The number of packets sent by the interface.
- Bandwidth Usage—The percent of bandwidth used by the interface, shown as a percentage value. Here is how bandwidth percentage is computed:

  Bandwidth percentage=(Kbps/bw) * 100,

  where

  bits per second= ((change in input+change in output) * 8) / poll interval

  Kbps= bits per second/1024

  bw=bandwidth capacity of the interface

  Because the differences in bytes input and bytes output can only be computed after the second view interval, the bandwidth percentage graph shows the correct bandwidth usage starting with the second view interval. See the View Interval section of this topic for polling intervals and view intervals.
- Bytes Input—The number of bytes received on the interface.
- Bytes Output—The number of bytes sent by the interface.
- Errors Input—The number of errors occurring while receiving data on the interface.
- Errors Output—The number of errors occurring while sending data from the interface.
- Packets flow—The number of packets in the flow for the chosen interface. This data item appears only if configured under **Configure > Interfaces and Connections > Edit > Application Service** for the chosen interface.

- Bytes flow—The number of bytes in the flow for the chosen interface. This data item appears only if configured under **Configure > Interfaces and Connections > Edit > Application Service** for the chosen interface.
- Total flow—The total number flows, from sources and destinations, for the chosen interface. This data item appears only if configured under **Configure > Interfaces and Connections > Edit > Application Service** for the chosen interface.

Note If the router Cisco IOS image does not support Netflow, the flow counters will not be available.

To view statistics for any of these items:

Step 1 Select the item(s) you want to view by checking the associated check box(es).

Step 2 Click **Monitor Interface** to see statistics for all selected data items.

Interface Status Area

View Interval

This pull-down field selects both the amount of data shown for each item and the frequency with which the data is updated. It has the following options

Note The polling frequencies listed are approximations and may differ slightly from the listed times.

- Real-time data every 10 sec. This option will continue polling the router for a maximum of two hours, resulting in approximately 120 data points.
- 10 minutes of data polled every 10 sec.
- 60 minutes of data, polled every 1 minute.
- 12 hours of data, polled every 10 minutes.

Note The last three options will retrieve a maximum of 60 data points. After 60 data points have been retrieved, Cisco SDM will continue to poll data, replacing the oldest data points with the newest ones.

Show Table/Hide Table

Click this button to show or hide the performance charts.

Reset button

Click this button to reset the interface statistic counts to zero.

Chart Area

This area shows the charts and simple numerical values for the data specified.

Note The last three options will retrieve a maximum of 30 data points. After 30 data points have been retrieved, Cisco SDM will continue to poll data, replacing the oldest data points with the newest ones.

Firewall Status

This window displays the following statistics about the firewall configured on the router:

- Number of Interfaces Configured for Inspection—The number of interfaces on the router that are configured to have traffic inspected by a firewall.
- Number of TCP Packets Count—The total number of TCP packets transmitted through the interfaces configured for inspection.
- Number of UDP Packets Count—The total number of UDP packets transmitted through the interfaces configured for inspection.
- Total number of active connections—The count of current sessions.

The Firewall Status window also displays active firewall sessions in a table with the following columns:

- Source IP Address—The IP address of the packet's origin host.

- Destination IP Address—The IP address of the packet's destination host.
- Protocol—The network protocol being examined.
- Match Count—The number of packets matching the firewall conditions.

Update button

Click this button to refresh the firewall sessions in the table and display the most current data from the router.

Zone-Based Policy Firewall Status

If the router runs a Cisco IOS image that supports the Zone-Based Policy Firewall feature, you can display the status of the firewall activity for each zone pair configured on the router.

Firewall Policy List Area

The firewall policy list area displays the policy name, source zone, and destination zone for each zone pair. The following table contains sample data for two zone pairs.

Zone Pair Name	Policy Name	Source Zone	Destination Zone
wan-dmz-in	pmap-wan	zone-wan	zone-dmz
wan-dmz-out	pmap-dmz	zone-dmz	zone-wan

In this sample table there is a zone pair configured for traffic inbound to the DMZ, and traffic outbound from the DMZ.

Choose the zone pair that you want to display firewall statistics for.

View Interval

Choose one of the following options to specify how data should be collected:

- Real-time data every 10 sec—Data is reported every 10 seconds. Each tick mark on the horizontal axis of the Dropped Packets and Allowed Packets graph represents 10 seconds.

- 60 minutes of data polled every 1 minute—Data is reported every 1 minute. Each tick mark on the horizontal axis of the Dropped Packets and Allowed Packets graph represents 1 minute.
- 12 hours of data polled every 12 minutes—Data is reported every 12 minutes. Each tick mark on the horizontal axis of the Dropped Packets and Allowed Packets graph represents 12 minutes.

Monitor Policy

Click **Monitor Policy** to collect firewall data for the selected policy.

Stop Monitoring

Click **Stop Monitoring** to stop collecting firewall data .

Statistics Area

This area displays the firewall statistics for the selected zone pair. Control the display in this area by clicking on nodes in the tree on the left hand side. The following sections describe what you see when you click on each of the nodes.

Active Sessions

Clicking **Active Sessions** displays the traffic type, source IP address, and destination IP address for traffic that is inspected in the chosen zone pair.

Dropped Packets

For the chosen zone pair, clicking **Dropped Packets** displays a graph showing the cumulative number of dropped packets against the time interval chosen in the View Interval list. Data is collected on the traffic configured to be dropped and logged in the Layer 4 policy map.

Allowed Packets

For the chosen zone pair, clicking **Allowed Packets** displays a graph showing the cumulative number of allowed packets against the time interval chosen in the View Interval list. Data is collected on the traffic configured with the pass action in the Layer 4 policy map.

VPN Status

This window displays a tree of VPN connections that are possible on the router. You can choose one of the following VPN categories from the VPN connections tree:

- IPSec Tunnels
- DMVPN Tunnels
- Easy VPN Server
- IKE SAs
- SSL VPN Components

To view statistics on an active VPN category, choose it from the VPN connections tree.

IPSec Tunnels

This group displays statistics about each IPSec VPN that is configured on the router. Each row in the table represents one IPSec VPN. The columns in the table and the information they display are as follows:

- Interface column

  The WAN interface on the router on which the IPSec tunnel is active.

- Local IP column

  The IP address of the local IPSec interface.

- Remote IP column

  The IP address of the remote IPSec interface.

- Peer column

  The IP address of the remote peer.

- Tunnel Status

  The current status of the IPSec tunnel. Possible values are:

  - Up—The tunnel is active
  - Down—The tunnel is inactive due to an error or hardware failure.

- Encapsulation Packets column

  The number of packets encapsulated over the IPSec VPN connection.
- Decapsulation Packets column

  The number of packets decapsulated over the IPSec VPN connection.
- Send Error Packets column

  The number of errors that have occurred while sending packets.
- Receive Error Packets column

  The number of errors that have occurred while receiving packets.
- Encrypted Packets column

  The number of packets encrypted over the connection.
- Decrypted Packets column

  The number of packets decrypted over the connection.

Monitor Tunnel Button

Click to monitor the IPSec tunnel chosen in the IPSec Tunnel table. See Monitoring an IPSec Tunnel.

Test Tunnel.. Button

Click to test a selected VPN tunnel.The results of the test will be shown in another window.

Update button

Click this button to refresh the IPSec Tunnel table and display the most current data from the router.

Monitoring an IPSec Tunnel

To monitor an IPSec tunnel, follow these steps:

Step 1 Choose the tunnel you want to monitor in the IPSec Tunnel table.

Step 2 Choose the types of information you want to monitor by checking the checkboxes under **Select Item to Monitor**.

Step 3 Choose the time interval for the real-time graphs using the **View Interval** drop-down list.

DMVPN Tunnels

This group displays the following statistics about Dynamic Multi-point VPN (DMVPN) tunnels. Each row reflects one VPN tunnel.

- Remote Subnet column

  The network address of the subnet to which the tunnel connects.

- Remote Tunnel IP column

  The IP address of the remote tunnel. This is the private IP address given the tunnel by the remote device.

- IP Public Interface of Remote Router column

  IP address of the public (outside) interface of the remote router.

- Status column

  The status of the DMVPN tunnel.

- Expiration column

  The time and date when the tunnel registration expires and the DMVPN tunnel will be shut down.

Monitor Tunnel Button

Click to monitor the DMVPN tunnel chosen in the DMVPN Tunnel table. See Monitoring a DMVPN Tunnel.

Update button

Click this button to refresh the DMVPN Tunnel table and display the most current data from the router.

Reset Button

Click to reset statistics counters for the tunnel list. Number of packets encapsulated and decapsulated, number of sent and received errors, and number of packets encrypted and decrypted are set to zero.

Monitoring a DMVPN Tunnel

To monitor a DMVPN tunnel, follow these steps:

Step 1 Choose the tunnel you want to monitor in the DMVPN Tunnel table.

Step 2 Choose the types of information you want to monitor by checking the checkboxes under **Select Item to Monitor**.

Step 3 Choose the time interval for the real-time graphs using the **View Interval** drop-down list.

Easy VPN Server

This group displays the following information about each Easy VPN Server group:

- Total number of server clients (in upper right corner)
- Group Name
- Number of client connections

Group Details Button

Clicking **Group Details** shows the following information about the selected group.

- Group Name
- Key
- Pool Name
- DNS Servers
- WINS Servers

- Domain Name
- ACL
- Backup Servers
- Firewall-R-U-There
- Include local LAN
- Group lock
- Save password
- Maximum connections allowed for this group
- Maximum logins per user

Client Connections in this Group

This area shows the following information about the selected group.

- Public IP address
- Assigned IP address
- Encrypted Packets
- Decrypted Packets
- Dropped Outbound Packets
- Dropped Inbound Packets
- Status

Update button

Click this button to display the most current data from the router.

Disconnect button

- Choose a row in the table and click Disconnect to drop the connection with the client.

IKE SAs

This group displays the following statistics about each active IKE security association configured on the router:

- Source IP column

  The IP address of the peer originating the IKE SA.

- Destination IP column

  The IP address of the remote IKE peer.

- State column

  Describes the current state of IKE negotiations. The following states are possible:

  - MM_NO_STATE—The Internet Security Association and Key Management Protocol (ISAKMP) SA has been created but nothing else has happened yet.
  - MM_SA_SETUP—The peers have agreed on parameters for the ISAKMP SA.
  - MM_KEY_EXCH—The peers have exchanged Diffie-Hellman public keys and have generated a shared secret. The ISAKMP SA remains unauthenticated.
  - MM_KEY_AUTH—The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE and a Quick mode exchange begins.
  - AG_NO_STATE—The ISAKMP SA has been created but nothing else has happened yet.
  - AG_INIT_EXCH—The peers have done the first exchange in Aggressive mode but the SA is not authenticated.
  - AG_AUTH—The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE and a Quick mode exchange begins.
  - QM_IDLE—The ISAKMP SA is idle. It remains authenticated with its peer and may be used for subsequent Quick mode exchanges.

- Update button—Click this button to refresh the IKE SA table and display the most current data from the router.

- Clear button—Select a row in the table and click Clear to clear the IKE SA connection.

SSL VPN Components

Clicking the VPN Status button in the monitoring window causes the router to begin monitoring SSL VPN activity. This window displays the data gathered for all SSL VPN contexts configured on the router.

By default, this data is refreshed every 10 seconds. If 10 seconds is too short an interval for you to view data before the next refresh, you can select an auto-refresh interval of **Real-time data every minute**.

Choose a context in the SSL VPN tree to view data for that context and data for the users who are configured for the context.

System Resources

The percentage of CPU and memory resources that SSL VPN traffic is using across all contexts is shown in this area.

Number of Connected Users

This graph shows the number of active users over time. The peak number of active users since monitoring began is displayed at the top of the graph area. The time that monitoring began is shown in the lower left-hand corner of the graph, and the current time is shown centered under the graph.

Tabbed Area

This area of the window displays gathered statistics in a series of tabs for easier viewing.

Click any of the links below for a description of the data the tab displays.

User Sessions

URL Mangling

Port Forwarding

CIFS

Full Tunnel

Note If a feature such as port forwarding or full tunnel has not been configured on the router, no data will be shown in the tab for that feature.

Some statistics are collected anew each time the router refreshes monitoring data. Other statistics, such as peak number of active users statistics, are collected at refresh time, but compared against the same data collected when monitoring began. Monitoring of all VPN activity, including SSL VPN, begins when you click the **VPN Status** button.

SSL VPN Context

This window shows the same types of information as the SSL VPN Components window but only shows the data gathered for the chosen context. For a description of the information displayed, click SSL VPN Components.

User Sessions

This tab displays the following information about SSL VPN user sessions.

- Active user sessions—The number of SSL VPN user sessions, of all traffic types, active since monitoring data was refreshed.
- Peak user sessions—The highest number of active SSL VPN user sessions since monitoring began.
- Active user TCP connections—The number of TCP-based SSL VPN user sessions active since monitoring data was refreshed.
- Session alloc failures—The number of session allocation failures that have occurred since monitoring began.
- VPN Session timeout—The number of VPN session timeouts that have occurred since monitoring began.
- User cleared VPN Sessions—The number of VPN sessions that have been cleared by users since monitoring began.
- AAA pending requests—The number of AAA requests that have been pending since monitoring data was refreshed.
- Peak time— The longest user session recorded since monitoring began.

- Terminated user sessions—The number of users sessions that have terminated since monitoring began.
- Authentication failures—The number of sessions that have failed to be authenticated since monitoring began.
- VPN Idle timeout—The number of VPN idle timeouts that have occurred since monitoring began.
- Exceeded context user limit—The number of times, since monitoring began, that a user has attempted to initiate a session when the context session limit had already been reached.
- Exceeded total user limit—The number of times, since monitoring began, that a user has attempted to initiate a session when the total session limit had already been reached.

URL Mangling

This tab displays data about URL mangling activities. For more information, refer to the command reference available at the following link:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

Port Forwarding

This tab displays data gathered about port forwarding activities. For more information, refer to the command reference at the following link:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

CIFS

This tab displays data gathered about CIFS requests, responses, and connections. For more information refer to the command reference available at the following link:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_command_reference_chapter09186a0080419245.html#wp1226849

Full Tunnel

This tab displays information about full tunnel connections between SSL VPN clients and servers on the corporate intranet.

- Active tunnel connections—The number of active full tunnel connections since data was last refreshed. Data can be refreshed every 10 seconds, or every minute.
- Active connections peak time—The full tunnel connection of the longest duration since monitoring began.
- Peak active tunnel connections—The highest number of active full tunnel connections since monitoring began.
- Tunnel connection attempts failed—The number of full tunnel connection attempts that have failed since monitoring began.
- Tunnel connection attempts succeeded— The number of full tunnel connections successfully established since monitoring began.

Server:

- IP packets sent to server—The number of IP packets from full-tunnel clients that the router forwarded to servers on the corporate intranet.
- IP traffic sent to server in bytes—The amount of IP traffic, in bytes, forwarded from full-tunnel clients to servers on the corporate intranet.
- IP packets received from server—The number of IP packets that the router has received from servers with full-tunnel connections to clients.
- IP traffic received from server in bytes—The amount of IP traffic, in bytes, received from servers on the corporate intranet with full-tunnel connections to clients.

User List

This window displays user information for the context chosen in the SSL VPN Components tree. Because there can be multiple group polices configured for the context, each using their own URL list and server lists, this screen provides valuable information about how individual users are using their SSL VPN connections.

You can control individual use of the SSL VPN in this window by choosing a user and clicking the **Disconnect** button.

User List Area

This area lists all active users in all groups configured for this context. This area displays the following information:

- User Login Name—The username that is authenticated with the AAA server.
- Client IP address—The user's assigned SSL VPN IP address for this session. This IP address is drawn from the address pool configured for this context.
- Context—The SSL VPN context under which the group policy for this user has been configured.
- No. of connections—The number of active connections for the user. For example, the user might have a connection to a mail server, and might also be browsing files on another server in the network.
- Created—The time at which the session was created.
- Last used—The time at which the user last sent traffic over any active connection.
- Cisco Secure Desktop—True or False. Indicates whether Cisco Secure Desktop has been downloaded to the user's PC.
- Group name—The name of the group policy under which the user is configured. The group policy specifies the URL list, the services available to the users, the WINS servers available to resolve server names, and the servers that the users can see when browsing files on the corporate intranet.
- URL list name—The name of the URL list that appears on the user's portal page. The URL list is configured for the group to which the user belongs. See Group Policy: Clientless Tab for more information.
- Idle timeout—The number of seconds that a session can remain idle before the router terminates it. This value is configured for the group to which the user belongs. See Group Policy: General Tab for more information.
- Session timeout—The maximum number of seconds that a session can remain active before being terminated. This value is configured for the group to which the user belongs. See Group Policy: General Tab for more information.
- Port forwarding list name—This value is configured for the group to which the user belongs. See Group Policy: Thin Client Tab for more information.
- WINS Name Service list name—This value is configured for the group to which the user belongs. See Group Policy: Clientless Tab for more information.

Traffic Status

This window displays a tree of traffic types that can be monitored on an interface. Before any traffic type can be monitored, it must be enabled on at least one interface.

You can choose one of the following traffic types from the Traffic Status tree:

- Netflow Top Talkers
- QoS
- Application/Protocol Traffic

  This type uses Network-based application recognition (NBAR) to monitor traffic.

Netflow Top Talkers

If Netflow statistics have been enabled for at least one interface in **Configure > Interfaces and Connections > Edit Interface/Connection**, you can view Netflow statistics. Choose **Top N Traffic Flows > Top Protocols** or **Top N Traffic Flows > Top Talkers** (high-traffic sources) from the Traffic Status tree.

Note If the router Cisco IOS image does not support Netflow, the Netflow choices will not be available in the Traffic Status tree.

Top Protocols

This window displays a table with the following columns:

- Protocol—Protocol being examined.
- Total Flows—Total number of flows associated with that protocol.
- Flows/Sec—Active flows per second for the protocol.
- Packets/Flow—Packets transmitted per flow.
- Bytes/Packet—Bytes per transmitted packet.
- Packets/Sec—Packets transmitted per second.

Update Button

Updates the window with current information about the flows.

Top Talkers

This window displays a table with the following columns:

- **Source IP Address**—Source IP address of the top talker.

  Select a source IP address to see more information in **Flow status for the source address**.
- **Packets**—Total number of packets received from the source IP address.
- **Bytes**—Total number of bytes received from the source IP address.
- **Flows**—Number of flows associated with the source IP address.

Note If Netflow top talkers is not enabled in **Configure > Additional Tasks > Router Properties > NetFlow**, then statistics for the top ten talkers are displayed.

Flow status for the source address

This table displays the following information about the flow associated with the selected source IP address:

- **Destination IP Address**—Target IP address of the top talker.
- **Protocols**—Protocols used in the packets exchanged with the destination IP address.
- **Number of Packets**—Number of packets exchanged with the destination IP address.

Update Button

Updates the window with current information about the flows.

QoS

The QoS Status window allows you to monitor the performance of the traffic on QoS configured interfaces (see Associating a QoS Policy With an Interface). This window also allows you to monitor bandwidth utilization and bytes-sent for interfaces with no QoS configuration. Monitoring inbound traffic on QoS interfaces shows the statistics only at a protocol level. Protocol-level statistics for non-QoS interfaces are collected for traffic in both directions.

This window allows you to monitor the following statistics:

- Bandwidth utilization for Cisco SDM defined traffic types
  - Bandwidth utilization per class under each traffic type
  - Bandwidth utilization for protocols under each class

  Bandwidth utilization is shown in Kbps.
- Total incoming and outgoing bytes for each traffic type
  - Incoming and outgoing bytes for each class defined under the traffic type
  - Incoming and outgoing bytes for each protocol for each class

  If the value is more than 1,000,000, then the graph may show the bytes as a multiple of 10^6. If the value is more than 1,000,000,000, then the graph may show the bytes as a multiple of 10^9.
- Packets dropped statistics for each traffic type

Interface—IP/Mask—Slot/Port—Description

This area lists the interfaces with associated QoS policies, their IP addresses and subnet masks, slot/port information if applicable, and available descriptions.

Select the interface that you want to monitor from this list.

View Interval

Select the interval at which statistics should be gathered:

- Now—Statistics are gathered when you click **Start Monitoring**.
- Every 1 minute—Statistics are gathered when you click **Start Monitoring**, and refreshed at 1-minute intervals.

- Every 5 minutes—Statistics are gathered when you click **Start Monitoring**, and refreshed at 5-minute intervals.
- Every 1 hour—Statistics are gathered when you click **Start Monitoring**, and refreshed at 1-hour intervals.

Start Monitoring

Click to start monitoring QoS statistics.

Select QoS Parameters for Monitoring

Select the traffic direction and type of statistics you want to monitor.

Direction

Click either **Input** or **Output**.

Statistics

Select one of the following

- Bandwidth
- Bytes
- Packets dropped

All Traffic—Real-Time—Business-Critical—Trivial

Cisco SDM displays statistics for all traffic classes in bar chart form, based on the type of statistic you selected. Cisco SDM displays a message instead of a bar chart if there are not adequate statistics for a particular traffic type.

Associating a QoS Policy With an Interface

Step 1 Go to **Interfaces and Connections > Edit Interface/Connection**.

Step 2 From the Interface List, choose the interface to which you want to associate a QoS policy.

Step 3 Click the **Edit** button.

Step 4 Click the **Application Service** tab.

Step 5 Choose a QoS policy from the **Inbound** drop-down list to associate with inbound traffic on the interface.

Step 6 Choose a QoS policy from the **Outbound** drop-down list to associate with outbound traffic on the interface.

Application/Protocol Traffic

This window allows you to monitor application and protocol traffic using Network-based application recognition (NBAR), a protocol and application discovery feature. NBAR is used to classify packets for more efficient handling of network traffic through a specific interface.

Note If the router Cisco IOS image does not support NBAR, this status window will not be available.

Enable NBAR

To display the status of NBAR for a specific interface, NBAR must first be enabled on that interface. To enable NBAR, follow these steps:

Step 1 Go to **Interfaces and Connections > Edit Interface/Connection**.

Step 2 Choose the interface for which you want to enable NBAR from the Interface List.

Step 3 Click the **Edit** button.

Step 4 Click the **Application Service** tab.

Step 5 Check the **NBAR** checkbox.

NBAR Status

The NBAR status table displays the following statistics for the interface you choose from the **Select an Interface** drop-down list:

- Input Packet Count—The number of packets of the protocol shown incoming to the chosen interface.
- Output Packet Count—The number of packets of the protocol shown outgoing from the chosen interface.
- Bit rate (bps)—The speed, in bits per second, of traffic passing through the interface.

NAC Status

If NAC is configured on the router, Cisco SDM can display snapshot information about the NAC sessions on the router, the interfaces on which NAC is configured, and NAC statistics for the selected interface.

The top row in the window displays the number of active NAC sessions, the number of NAC sessions being initialized, and a button that allows you to clear all active and initializing NAC sessions

The window lists the router interfaces with associated NAC policies.

```
FastEthernet0/0    10.10.15.1/255.255.255.0   0
```

Clicking on an interface entry displays the information returned by posture agents installed on the hosts in the subnet for that interface. An example of the interface information follows:

```
10.10.10.5     Remote EAP Policy      Infected       12
```

10.10.10.1 is the host's IP address. Remote EAP Policy is the type of authentication policy that is in force. The host's current posture is Infected, and it has been 12 minutes since the host completed the admissions control process.

Note This area of the window contains no data if no posture information is returned by the hosts on the selected subnet.

The authentication types are:

- **Local Exception Policy**—An exception policy that is configured on the router is used to validate the host.
- **Remote EAP Policy**—The host returns a posture, and an exception policy assigned by an ACS server is used.

- **Remote Generic Access Policy**—The host does not have a posture agent installed, and the ACS server assigns an agentless host policy.

The posture agents on the hosts may return the following posture tokens:

- **Healthy**—The host is free of known viruses, and has the latest virus definition files.
- **Checkup**—The posture agent is determining if the latest virus definition files have been installed.
- **Quarantine**—The host does not have the latest virus definition files installed. The user is redirected to the specified remediation site that contains instructions for downloading the latest virus definition files.
- **Infected**—The host is infected with a known virus. The user is redirected to a remediation site to obtain virus definition file updates.
- **Unknown**—The host's posture is unknown.

Logging

Cisco SDM offers the following logs:

- Syslog—The router log.
- Firewall Log— If a firewall has been configured on the router, this log records entries generated by that firewall.
- Application Security Log—If an application firewall has been configured on the router, this log records entries generated by that firewall.
- SDEE Message Log—If SDEE has been configured on the router, this log records SDEE messages.

To open a log, click the tab with the log's name.

Syslog

The router contains a log of events categorized by severity level, like a UNIX syslog service.

Note It is the router log that is displayed, even if log messages are being forwarded to a syslog server.

Logging Buffer

Shows whether or not the logging buffer and syslog logging are enabled. The text "Enabled" is displayed when both are enabled. The logging buffer reserves a specified amount of memory to retain log messages. The setting in this field is not preserved if your router is rebooted. The default settings for these fields are for the logging buffer to be enabled with 4096 bytes of memory.

Logging Hosts

Shows the IP address of any syslog hosts where log messages are being forwarded. This field is read-only. To configure the IP addresses of syslog hosts, use the **Additional Tasks > Router Properties > Logging** window.

Logging Level (Buffer)

Shows the logging level configured for the buffer on the router.

Number of Messages in Log

Shows the total number of messages stored in the router log.

Select a Logging Level to View

From this field, select the severity level of the messages that you want to view in the log. Changing the setting in this field causes the list of log messages to be refreshed.

Log

Displays all messages with the severity level specified in the Select a Logging Level to View field. Log events contains the following information:

- Severity Column

Shows the severity of the logging event. Severity is shown as a number from 1 through 7, with lower numbers indicating more severe events. The descriptions of each of the severity levels are as follows:

- 0 - emergencies

  System unusable
- 1- alerts

  Immediate action needed
- 2 - critical

  Critical conditions
- 3 - errors

  Error conditions
- 4 - warnings

  Warning conditions
- 5 - notifications

  Normal but significant condition
- 6 - informational

  Informational messages only
- 7 - debugging

  Debugging messages

- Time Column

  Shows the time that the log event occurred.
- Description Column

  Shows a description of the log event.

Update Button

Updates the window with current information about log details and the most current log entries.

Clear Log Button

Erases all messages from the log buffer on the router.

Search Button

Opens a search window. In the search window, enter text in the Search field and click the **Find** button to display all entries containing the search text. Searches are *not* case sensitive.

Firewall Log

The log entries shown in the top part of this window are determined by log messages generated by the firewall. In order for the firewall to generate log entries, you must configure individual access rules to generate log messages when they are invoked. For instructions on configuring access rules to cause log messages, see the help topic How Do I View Activity on My Firewall?

In order for firewall log entries to be collected, you must configure logging for the router. Go to **Additional Tasks > Router Properties > Logging**. Click **Edit**, and configure logging. To obtain firewall logging messages, you must configure a logging level of debugging (7).

Firewall Log

The firewall log is displaed if the router is configured to maintain a log of connection attempts denied by the firewall.

Number of Attempts Denied by Firewall

Shows the number of connection attempts rejected by the firewall.

Attempts Denied by Firewall Table

Shows a list of connection attempts denied by the firewall. This table includes the following columns:

- Time column

  Shows the time that each denied connection attempt occurred.

- Description column

  Contains the following information about the denied attempt: log name, access rule name or number, service, source address, destination address, and number of packets. An example follows:

```
%SEC-6-IPACCESSLOGDP: list 100 denied icmp 171.71.225.148->10.77.158.140 (0/0), 3 packets
```

Update Button

Polls the router and updates the information shown on the screen with current information.

Search Button

Opens a search window. Choose a search type from the **Search** menu and enter the appropriate text in the Search field, then click the **Find** button to display matching log entries.

The search types are:

- Source IP Address—The IP address of the origin of the attack.

  A partial IP address can be entered.

- Destination IP Address—The IP address of the target of the attack.

  A partial IP address can be entered.

- Protocol—The network protocol used in the attack.
- Text—Any text found in the log entry.

Searches are *not* case sensitive.

View Top Attacks

From the View drop-down menu, choose one of the following ways to display information on top attacks:

- Top Attack Ports—Top attacks by target port.
- Top Attackers—by attacker IP address.

The top-attacks table below the View drop-down menu displays the top attack entries. If you choose Top Attack Ports from the View drop-down menu, the top-attacks table displays entries with the following columns:

- Port Number—The target port.
- Number of attacks—The number of attacks against the target port.
- Number of packets denied—The number of packets denied access to the target port.

- View Details—A link that opens a window containing the full log of attacks against the chosen port.

If you choose Top Attackers from the View drop-down menu, the top-attacks table displays entries with the following columns:

- Attacker's IP Address—The IP address from which the attacks are coming.
- Number of attacks—The number of attacks that have come from the IP address.
- Number of packets denied—The number of packets that have come from the IP address and were denied access.
- View Details—A link that opens a window containing the full log of the attacks from the chosen IP address.

Monitoring Firewall with a "Non-Administrator View" User Account

Firewall monitoring requires that Logging to Buffer be enabled on the router. If Logging to Buffer is not enabled, log in to Cisco SDM using an Administrator view account or a non-view based user account with privilege level 15 and configure logging.

To configure logging in Cisco SDM, go to **Additional Tasks > Router Properties > Logging**.

Application Security Log

If logging has been enabled, and you have specified that alarms be generated when the router encounters traffic from applications or protocols that you have specified, those alarms are collected in a log that can be viewed from this window.

In order for Application Security log entries to be collected, you must configure logging for the router. Go to **Additional Tasks > Router Properties > Logging**. Click **Edit**, and configure logging. To obtain firewall logging messages, you must configure a logging level of **informational (6)**, or higher. If you have already configured logging for **debugging(7)**, the log will contain application security log messages.

The following is example log text:

```
*Sep  8 12:23:49.914: %FW-6-DROP_PKT: Dropping im-yahoo pkt
128.107.252.142:1481 => 216.155.193.139:5050
```

```
*Sep  8 12:24:22.762: %FW-6-DROP_PKT: Dropping im-aol pkt
128.107.252.142:1505 => 205.188.153.121:5190
*Sep  8 12:26:02.090: %FW-6-DROP_PKT: Dropping im-msn pkt
128.107.252.142:1541 => 65.54.239.80:1863
*Sep  8 11:42:10.959: %APPFW-4-HTTP_PORT_MISUSE_IM: Sig:10006 HTTP
Instant Messenger detected - Reset - Yahoo Messenger from
10.10.10.2:1334 to 216.155.194.191:80
*Sep  8 12:27:54.610: %APPFW-4-HTTP_STRICT_PROTOCOL: Sig:15 HTTP
protocol violation detected - Reset -  HTTP Protocol not detected from
10.10.10.3:1583 to 66.218.75.184:80
*Sep  8 12:26:14.866: %FW-6-SESS_AUDIT_TRAIL_START: Start im-yahoo
session: initiator (10.10.10.3:1548) -- responder (66.163.172.82:5050)
*Sep  8 12:26:15.370: %FW-6-SESS_AUDIT_TRAIL: Stop im-yahoo session:
initiator (10.10.10.3:1548) sent 0 bytes -- responder
(66.163.172.82:5050) sent 0 bytes
*Sep  8 12:24:44.490: %FW-6-SESS_AUDIT_TRAIL: Stop im-msn session:
initiator (10.10.10.3:1299) sent 1543 bytes -- responder
(207.46.2.74:1863) sent 2577 bytes
*Sep  8  11:42:01.323: %APPFW-6-IM_MSN_SESSION: im-msn un-recognized
service session initiator 14.1.0.1:2000 sends 1364 bytes to responder
207.46.108.19:1863
*Sep  8  11:42:01.323: %APPFW-6-IM_AOL_SESSION: im-aol text-chat
service session initiator 14.1.0.1:2009 sends 100 bytes to responder
216.155.193.184:5050
```

Update Button

Updates the screen with current information about log details and the most current log entries.

Search Button

Opens a search window. In the search window, enter text in the Search field and click the **Find** button to display all entries containing the search text. Searches are *not* case sensitive.

SDEE Message Log

This window lists the SDEE messages received by the router. SDEE messages are generated when there are changes to IPS configuration.

SDEE Messages

Choose the SDEE message type to display:

- All— SDEE error, status, and alert messages are shown.
- Error—Only SDEE error messages are shown.
- Status—Only SDEE status messages are shown.
- Alerts—Only SDEE alert messages are shown.

Update Button

Click to check for new SDEE messages.

Search Button

Opens a search window. Choose a search type from the **Search** menu and enter the appropriate text in the Search field, then click the **Find** button to display matching log entries.

The search types are:

- Source IP Address
- Destination IP Address
- Text

Searches are *not* case sensitive.

Time

The time the message was received.

Type

Types are Error, Status, and Alerts. Click SDEE Message Text to see possible SDEE messages.

Description

Available description.

IPS Status

This window appears if the router is using a Cisco IOS image that supports IPS version 4.x or earlier. This window displays a table of IPS signature statistics, grouped by signature type. The following statistics are shown:

- **Signature ID**—Numerical signature identifier.
- **Description**—Description of the signature.
- **Risk Rating**—A a value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network.
- **Action**—The action that is to be taken when a packet matches a signature.
- **Source IP Address**—The IP address of the packet's origin host.
- **Destination IP Address**—The IP address of the packet's destination host.
- **Hits**—Number of matching packets.
- **Drop Counts**—Number of matching packets dropped.

To sort the signatures, click the column head with the name of signature statistic you want to sort by.

Note If you sort the signatures, the signatures may no longer be grouped by type. To restore the grouping of signatures by type, click the **Update** button.

Total Active Signatures

Displays the total number of signatures available that are active on your router.

Total Inactive Signatures

Displays the total number of signatures available that are inactive on your router.

Update Button

Click to check for and include the latest signature statistics.

Clear Button

Click to set set all signature statistic counters to 0.

SDEE Log

Click to view SDEE messages. You can also view these messages by clicking **Monitor > Logging > SDEE Message Log**.

IPS Signature Statistics

This window is displayed if the router is using an IOS IPS 5.x configuration. Statistics are displayed for each enabled signature in the IOS IPS configuration. The top of the window displays signature totals to provide a snapshot of the signature configuration. The following totals are provided:

- Total Signatures
- Total Enabled Signatures
- Total Retired Signatures
- Total Compiled Signatures

Update and Clear Buttons

Click **Update** to check for and include the latest signature statistics. Click **Clear** to set set all signature statistic counters to 0.

SDEE Log

Click to view SDEE messages. You can also view these messages by clicking **Monitor > Logging > SDEE Message Log**.

Signature List Area

The Signature ID, Description, number of hits, and drop count is shown for all signatures. If packet arrives that matches a signature, the source and destination IP addresses are listed as well.

IPS Alert Statistics

The IPS Alert Statistics window displays alert statistics in a color-coded format for easy recognition. The top part of the screen displays a legend that explains the use of colors in the display.

Color	Explanation
RED	The event that generated the alert has a high Risk Rating (RR) in the range of 70 to 100.
MAGENTA	The event that generated the alert has a medium Risk Rating (RR) in the range of 40 to 69.
BLUE	The event that generated the alert has a low Risk Rating (RR) in the range of 0 to 39.

By clicking on a column heading, you sort the display based on the values of that parameter. For example, by clicking on the **Signature ID** heading, you sort the display in ascending or descending numerical order of signature IDs. Each column is described in the following list:

- **Signature ID**—Numerical signature identifier.
- **Description**—Description of the signature.
- Risk Rating—A value between 0 and 100 that represents a numerical quantification of the risk associated with a particular event on the network.
- Event Action—The action that IOS IPS is to take when an event matching the signature occurs.
- Source IP Address—The IP address from which the packet originated.
- Destination IP Address—The IP address to which the packet was addressed. If the packet is malicious, the Destination IP address can be considered the target.
- Hits—Number of matching packets.
- Drop Count—The number of matching packets dropped.
- Engine—The signature engine associated with the signature.

802.1x Authentication Status

802.1x Authentication on Interfaces Area

Interface

802.1x Authentication

Reauthentication

802.1x Clients Area

Client MAC Address

Authentication Status

Interface