CHAPTER 60

Using External Monitoring, Troubleshooting, and Diagnostic Tools

High network availability is a requirement for large enterprises and service providers. Network managers face various challenges to providing high availability, including unscheduled down time, lack of expertise, insufficient tools, complex technologies, business consolidation, and competing markets. Network monitoring, problem diagnosis and troubleshooting are essential to meeting and overcoming these challenges.

Monitoring involves the study of network activity and device status to identify anomalous events and behaviors. Quickly diagnosing and correcting network and system faults such as outages and degradations increase service availability, and thus tools to isolate, analyze and correct problems are essential.

The main Security Manager tool for monitoring device events is Event Viewer (select **Tools > Event Viewer**). In addition to Event Viewer, the following topics describe additional monitoring, troubleshooting and diagnostic tools that are available with Security Manager:

Analyzing an ASA or PIX Configuration Using Packet Tracer

Packet tracer is a policy debugging tool for ASA and PIX security appliances running version 7.2.1+ that are not operating in transparent mode. It inspects the active policies currently running on the appliance. Without having to generate real traffic, you can analyze how traffic between two addresses traverses the security appliance, whether it is dropped or allowed. If the result is unexpected, you can determine where the issue exists and update the corresponding policy in Security Manager to resolve it.

Packet tracer presents a step-by-step analysis of how a simulated packet is processed by the security appliance's active configuration. It traces the packet's flow through the active firewall modules, such as route lookup, access lists, NAT translations, and VPN. The set of active modules changes based on the type of packet configured and the active configuration. For example, if no VPN policies are configured, the VPN module is not evaluated.

You can inspect the simulated packet's traversal rather than having to generate network traffic, enable syslog messages, and manually review resulting syslog messages. Packet tracer details the actions enforced by the active configuration on the packet. If a configuration command causes the packet to be dropped, the reason is provided, such as "Drop-reason: (telnet-not-permitted) Telnet not permitted on least secure interface."

You can trace the life span of a simulated packet through the security appliance to see whether the packet is behaving as expected. Packet tracer uses include the following:

- Debug all packet drops in a production network.
- Verify the configuration is working as intended.
- Show all rules applicable to a packet including the CLI that defines the rule.
- Show a time line of packet changes in a data path.
- Trace packets in the data path.
- If the packet is blocked or permitted by some explicit access rule, you can use a short-cut to go to the policy so that you can edit the rule.

Tips:

- Packet Tracer is also available in the ASDM application and the ASA command line, and the Security Manager version is equivalent to the ASDM version. For an example of using Packet Tracer from ASDM and the CLI to analyze a configuration, see PIX/ASA 7.2(1) and later: Intra-Interface Communications.
- Before you can use packet tracer on a device, you must submit your policy changes at least once after adding the device to the inventory.
- Packet tracer analyzes only the active configuration running on a device. Therefore, you cannot use packet tracer to test proposed configurations before they are deployed and running on the device. Do not use packet tracer on a device with pending configuration changes—deploy the changes first and then use packet tracer to ensure the packet tracer results are valid.

To use Packet Tracer:

Step 1 (Device view) Right click on the ASA or PIX 7.2.1+ device and select **Packet Tracer** on the shortcut menu to open the Packet Tracer window.

Step 2 Select the interface you want to test from the **Interfaces** list. The list contains all interfaces defined on the device.

Step 3 Model the packet that you want to trace by configuring the following fields:

- **Packet Type**—Select whether you are tracing a TCP, UDP, ICMP, or IP packet.
- **Source, Destination IP Address**—Enter the host IP addresses for both ends of the communication (from source to destination).
- **Source, Destination Port (TCP and UDP only)**—Enter, or select, the port numbers that represent the traffic type. The selection list uses names that equate to the standard port numbers for the named application. For example, selecting **http** and entering **80** is the same.
- **Type, Code, ID (ICMP only)**—When modeling an ICMP packet, you must enter values in all of these fields:
  - **Type**—Select the ICMP packet type or enter the equivalent number. The list includes all main ICMP types. For a complete list of types and related codes, see RFC 1700 at http://www.ietf.org/rfc/rfc1700.txt and search for "ICMP Type Numbers."

  - **Code**—Enter **0** unless you are modeling a packet type that has non-zero codes. These are destination unreachable (type 3, codes 0-12), redirect (type 5, codes 0-3), time exceeded (type 11, codes 0-1), and parameter problem (type 12, codes 0-2). See RFC 1700 for code explanations, and note that additional codes might have been introduced in other RFCs.
  - **ID**—You must enter a value for ID even though the field is used for a limited number of message types only. The ID is used for ICMP types that include request and reply versions, such as echo and echo request, to help match replies to requests. The value should be between 1-255.
- **Protocol (IP only)**—Enter the number that identifies the next level protocol. For a complete list of protocol codes, see RFC 1700 at http://www.ietf.org/rfc/rfc1700.txt and search for the "Protocol Numbers" heading. As of the writing of this topic, numbers 1-54 and 61-100 represent values assigned to actual protocols from the accepted range of 0-255.

Step 4 If you want to see the progress of the trace while it is happening, select **Show animation**. Otherwise, the window is not updated with the results until the trace is completed.

Step 5 Click **Start** to trace the packet.

The policies are examined, and the bottom of the window shows the results in two forms: graphical and detailed information. The graphical view summarizes the phases evaluated in the packet's path. Checkmarks indicate the packet passed the phase, a red X indicates the packet was dropped at that point.

The detailed information organizes the results in folders that correspond to the phases, with an Action column that indicates the results of the phase (checkmark for passed, red X for dropped). To open a folder, click its heading. Detailed information can include the specific configuration commands evaluated and the data derived from **show** commands. The final folder, named Result, summaries the results of the trace.

Tips:

- If the packet is allowed or denied by an explicit access rule, then you can jump to that rule. Select the Access-List folder to open it, then click the **Show access rule** link at the top of the section. You are taken to the Access Rule policy with the rule highlighted; you can edit the rule as desired. If a packet is dropped due to an implicit drop rule, the Show access rule link is not available because the rule does not exist in the policy table.
- If the device is shut down or not reachable due to a network failure during the analysis, an error message stating "Device Connectivity is Failed" appears.
- If you start a new trace, the information shown is cleared automatically. However, you can clear it yourself by clicking **Clear**.

Starting Device Managers

You can start a device manager to view a device's configuration and status from within Security Manager. You can start device managers for ASA, PIX, FWSM, IPS, and IOS devices. Each device manager includes several monitoring and diagnostic features that provide information regarding the services running on the device and a snapshot of the overall health of the system. You can use these device managers to view the existing device configuration and to monitor current status, but you cannot use it to apply configuration changes to the device.

Note You cannot launch device managers for IPS virtual sensors.

To start a device manager, select the device in Device view, right-click and select **Device Manager**. You can also start the device manager by selecting **Tools > Device Manager**.

When you start a device manager from Security Manager, the device manager executable is downloaded to your client system; the device manager does not need to be installed on the network device. The first time you start a device manager, it takes time to download the software to your workstation (you are shown a progress bar). (If you run into problems, review the tips in Troubleshooting Device Managers, page 60-5.)

Security Manager selects the most appropriate device manager version based on the operating system running on the network device. Subsequent communications with the selected device are completely transparent. By starting a device manager from Security Manager, you eliminate the need to open an HTTPS connection between your client system and the device you want to monitor.

Tip When you start a device manager session, Security Manager opens a version of the manager that is appropriate for the operating system software version running on the device. However, Security Manager might not open the most recently-available version of the device manager if new device manager versions have been released after the release of the Security Manager version you are using. When you start the device manager, check its version (for example, select **Help > About** in the device manager window); if there is a more recent device manager available with features that you require, you must install and use that device manager outside of Security Manager to use those new features.

Keep in mind that if you use an external device manager running on the device to modify device configurations directly, these changes are considered out-of-band by Security Manager, and might be subsequently overwritten when you next deploy configurations from Security Manager. For more information about out-of-band changes, and what you can do to identify and recreate them, see the following topics:

- Understanding How Out-of-Band Changes are Handled, page 8-12
- Detecting and Analyzing Out of Band Changes, page 8-43

Security Manager starts only one instance of a device manager per device, and closes the device manager when you exit Security Manager, or the idle-session timeout period is exceeded. You can have more than one device manager window open at one time (connected to different devices).

The following table outlines the device managers you can launch from Security Manager.

Table 60-1 Device Managers Available in Security Manager

Device Manager	Description
IDM	The IPS Device Manager (IDM) lets you monitor IPS sensors and modules that are part of the Security Manager inventory. See the IDM documentation for more information about using this device manager.
PDM	The PIX Device Manager (PDM) lets you monitor PIX 6.x devices and early FWSMs, specifically FWSM releases 1.1, 2.2 and 2.3 in single- or multiple-context modes. See the PDM documentation for more information about using this device manager.

Table 60-1 Device Managers Available in Security Manager (Continued)

Device Manager	Description
ASDM	The Adaptive Security Device Manager (ASDM) lets you monitor ASA, PIX 7.x+, and FWSM 3.x+ devices. See the ASDM documentation for more information about using this device manager.
SDM	The Security Device Manager (SDM) lets you monitor Cisco IOS-based resources. SDM requires no previous experience with Cisco devices or the Cisco command-line interface (CLI). Cisco SDM supports a wide range of Cisco IOS software releases. See the SDM documentation for more information about using this device manager.

The following topics explain more about troubleshooting and using device managers:

Troubleshooting Device Managers

If you can successfully deploy configurations to a device, Security Manager should be able to open a device manager session with the device (as described in Starting Device Managers, page 60-3). However, if you have problems making a connection or using one that is open, consider the following troubleshooting tips, which are divided into basic tips and tips for using multiple device managers.

Basic Device Manager Troubleshooting Tips

- Generally, the credentials configured for the device in the Security Manager inventory are used to start the device manager. However, some versions of SDM require that you enter a user name and password when the device manager is started. If you get an error that says device credentials are missing, or they are not valid, update the Device Properties Credentials page with a username and password that can log into the device. In Device view, right-click the device and select **Device Properties**. For more information, see Viewing or Changing Device Properties, page 3-34 and Device Credentials Page, page 3-38.
- All users associated with any of the CiscoWorks Common Services roles have permission to start device managers from Security Manager, with the exception of the Help Desk role or any of the predefined Cisco Secure ACS roles. Ensure you have appropriate permissions.
- SSL/HTTPS must be enabled on the target device to provide secure communications between Security Manager and the device. An error message is displayed if SSL is not enabled on the device. See Understanding Device Communication Requirements, page 2-1 for more information.
- You might need to modify Cisco Security Agent, or other anti-virus and network firewall software, on the Security Manager system and your workstation to allow the device manager service (**xdm-launcher.exe**) to be started.

- Ensure that Security Manager is correctly configured for contacting and communicating with the target device. Specifically verify device properties such as identity, operating system and credentials. Select the desired device, right-click and choose **Device Properties**. Verify the settings on the General and Credentials pages. You can test whether Security Manager can connect to the device by selecting the Credentials tab and clicking **Test Connectivity** (see Testing Device Connectivity, page 9-1).
- Device managers can be started for FWSMs and ASAs running in transparent mode (Layer 2 firewall) or routed mode (Layer 3 firewall), and supporting a single security context or multiple security contexts. For FWSM and ASA devices running multiple security contexts, you must define a unique management IP address for each security context.
- If you get a message saying that the platform is not supported for device manager launch, but you believe the platform should be supported based on information in this guide, consider the relative newness of the operating system version running on the device and the age of the Security Manager software version you are using. If you are using very recent operating systems, but a relatively downlevel version of Security Manager, you might need to upgrade Security Manager (or apply a service pack), contact Cisco Technical Support, or simply install the latest device manager on the network device and use it outside of Security Manager. Before using a device manager outside of Security Manager, review the information on out-of-band changes in Starting Device Managers, page 60-3.

Multiple Device Manager Sessions Troubleshooting Tips

- Starting multiple device managers might affect the performance of both the Security Manager server and your client. On the client, memory requirements and performance impact are proportional to the number of device managers launched. On the server, a large number of requests to start device managers or retrieve current information from the device can have an adverse impact on performance.
- The maximum number of persistent HTTPS connections that can be established with any one device from all clients depends on the device type and model. An error message is displayed if you attempt to exceed this limit.

  For example, a single PIX 6.x allows multiple clients to each have one browser session open, supporting up to 16 concurrent PDM sessions. An FWSM (1.1, 2.2, or 2.3) allows up to 32 PDM sessions for the entire module, with a maximum of five concurrent HTTPS connections per context.

  Refer to the appropriate device documentation for information about specific limits.

Access Rule Look-up from Device Managers

A set of access rules is associated with each device interface. These rules are presented in the form of an ordered list or table. This list is often referred to as an access-control list (ACL), with each rule in the list known as an access-control entry (ACE). When deciding whether to forward or drop a packet, the device tests the packet against each access rule in the order listed. When a rule is matched, the device performs the specified action, either permitting the packet into the device for further processing, or denying entry. If the packet does not match any rule, the packet is denied.

Activity on your firewall or router can be monitored through syslog messages. If logging is enabled on the device, whenever an access rule that is configured to generate syslog messages is matched—for example, a connection was attempted from a denied IP address—a log entry is generated.

Note For the device to generate log entries, logging must be enabled on the device (on the Logging Setup Page for ASA/PIX devices and the Logging policies for IOS devices, described in Logging on Cisco IOS Routers, page 55-1), and the individual access rules must be configured to generate log messages when they are matched (in the Advanced and Edit Options Dialog Boxes, page 14-13).

You can monitor syslog messages in device managers launched from Security Manager, and for certain device managers, you can look up the access rule in Security Manager that generated a particular message from the monitoring window. The access rule that triggered the syslog entry is highlighted in Security Manager on a first-match basis, even if there are multiple matches.

This access rule look-up is available through SDM for all managed routers running IOS, and through ASDM for managed PIX and ASA version 8.0(3) devices, and FWSM version 3.1 and 3.2 blades.

The following topics describe how to look up access rules in Security Manager from a device manager:

- Navigating to an Access Rule from ASDM, page 60-7
- Navigating to an Access Rule from SDM, page 60-8

Navigating to an Access Rule from ASDM

In an ASDM device manager launched from Security Manager, you can monitor system log messages in the Real-time Log Viewer window and the Log Buffer window. You can select a syslog message displayed in either window and navigate to the access-control rule in Security Manager that triggered the message, where you can update the rule as necessary.

The Real-time Log Viewer is a separate window that lets you view syslog messages as they are logged. The separate Log Buffer window lets you view messages present in the syslog buffer.

You can look up access rules associated with the following syslog message IDs:

- 106023 – Generated when an IP packet is denied by the access rule. This message appears even when logging is not enabled for the rule.
- 106100 – If logging is enabled for a matched access rule (in the Advanced and Edit Options Dialog Boxes, page 14-13), this message provides information about the traffic flow, depending on the parameters set. This message provides more information than message 106023, which logs only denied packets.

This procedure describes how to look up an access rule in Security Manager from ASDM's Real-time Log Viewer or Log Buffer windows.

Related Topics

- Access Rule Look-up from Device Managers, page 60-6
- Navigating to an Access Rule from SDM, page 60-8

Step 1 Select a PIX, ASA, or FWSM in the Security Manager device inventory.

Step 2 Choose **Device Manager** from the Tools menu to launch ASDM. For more information about starting device managers, see Starting Device Managers, page 60-3.

Step 3 In the ASDM window, click the **Monitoring** button to display the Monitoring panel; click **Logging** in the left pane to access the log-viewing options.

Step 4 Select either **Real-time Log Viewer** or **Log Buffer**.

Step 5 Click the **View** button to open the selected log-viewing window.

Note The View button is not displayed if logging is not enabled on the device.

Each syslog message listed in the window includes the following information: message ID number, date and time the message was generated, the logging level, and the network or host addresses from which the packet was sent and received.

Step 6 To view the access rule that triggered a specific syslog message, select the message and click the **Show Rule** button in the ASDM toolbar (or right-click the message and choose **Go to Rule in CSM** from the pop-up menu).

The Security Manager client window is activated and the Access Rules page appears with the rule highlighted in the rules table. If the syslog entry was triggered by an access rule not referenced in the current Security Manager activity, an error message appears.

Navigating to an Access Rule from SDM

In an SDM device manager launched from Security Manager, you can view a log of events categorized by security level under the Syslog tab of the Logging window. You can select a syslog message and navigate to the access-control rule in Security Manager that triggered the message, where you can update the rule as necessary.

The Monitor > Logging option in SDM offers four log tabs; Syslog is the only one of these offering the Security Manager access-rule look-up option. The router contains a log of events categorized by severity level. The Syslog tab displays the router log, even if log messages are being forwarded to a syslog server.

On Cisco IOS devices, syslog messages are generated for access rules configured with the **log** or **log-input** keywords. The **log** keyword produces a message when a packet matches the rule. The **log-input** keyword produces a message that includes ingress interface and source MAC address, in addition to the packet's source and destination IP addresses and ports. When identical packets are matched, the message is updated at five-minute intervals with the number of packets permitted or denied in the previous five minutes.

This procedure describes how to look up an access rule in Security Manager from the Syslog tab of SDM's Logging panel.

Related Topics

- Access Rule Look-up from Device Managers, page 60-6
- Navigating to an Access Rule from ASDM, page 60-7

Step 1 Select an IOS router in the Security Manager device inventory.

Step 2 Choose **Device Manager** from the Tools menu to launch SDM. For more information about starting device managers, see Starting Device Managers, page 60-3.

Step 3 In the SDM window, click the **Monitoring** button to display the Monitoring panel; click **Logging** in the left pane to access the log-viewing options.

The Logging pane appears with Syslog tab displayed.

Step 4 To view the access rule that triggered a specific syslog message, select the message and click the **Go to Rule in CSM** button above the table of log messages.

The Security Manager client window is activated and the Access Rules page appears with the rule highlighted in the rules table. If the syslog entry was triggered by an access rule not referenced in the current Security Manager activity, an error message appears.

Viewing Inventory Status

You can view a summary of device properties for all devices that you are authorized to view. The summary includes device contact information and all device configurations, indicating which settings are local and which are using a shared policy, and indicating any policy object overrides in effect.

If you are using Performance Monitor to monitor your devices, status information from Performance Monitor can be included in the inventory summary if Security Manager is configured to provide it. You can also view the status of configuration deployment to the device. For information on how to configure the inventory status to show this information, see Configuring Status Providers, page 60-9.

The report is in table format, allowing you to organize information by filtering, sorting, reordering and removing columns. You can also export the table contents to a comma-separated values (CSV) file on the Security Manager server.

Step 1 In Device view, select **Tools > Inventory Status** to open the Inventory Status Window, page 60-11.

Step 2 Select the device whose detailed status you want to view in the upper table. The detailed information is shown in the tabs in the lower pane. The information is organized into folders; click the +/- icons to open and close folders, or double-click the folder name. The following tabs are available:

- Inventory—Lists summary information about the selected device's device properties, deployment methods, device group membership, and the parent device for modules.
- Policy—Lists the current status of the policies that can be configured for the selected device, whether the policy is unassigned (not defined), a local policy, or a shared policy.
- Policy Object Overrides—Lists policy objects that have overrides defined for the selected device.
- Status—Lists status providers with any status messages for the selected device, organized by event type. You can see status from Security Manager deployment jobs or from Performance Monitor.

  An **event** is a notification that a managed device or component has experienced an abnormal condition. Multiple events can occur simultaneously on a single monitored device or service module. However, you can configure thresholds in Performance Monitor, and only events exceeding specified thresholds are displayed.

  Security Manager displays only the most-recent event of each type. To view historical status information, use the Deployment Manager or Performance Monitor, as appropriate. If you have problems with Performance Monitor status, see Troubleshooting Performance Monitor Status Collection, page 60-10.

Step 3 Click **Close** to close the Inventory Status window.

Configuring Status Providers

Users can view configuration summary and status information about the devices they can configure by selecting **Tools > Inventory Status** (see Viewing Inventory Status, page 60-9).

The information that is available on the Status tab depends on the type of status providers you configure. By default, Security Manager provides status on deployment jobs that affect a device.

You can also provide status that is obtained from Cisco Performance Monitor if your system is configured appropriately. (Performance Monitor is part of the Cisco Security Management Suite.) As a registered status provider, Performance Monitor collects the status of events, such as VPN tunnel up/down status, device reachability, and CPU usage threshold for the devices that it monitors, and reports the status to Security Manager.

To enable Security Manager to collect status information from your Performance Monitor servers, you must register them with Security Manager. You can add up to five servers. This procedure explains how to register a Performance Monitor server as a status provider.

Step 1 Choose **Tools > Security Manager Administration** and select **Status** from the table of contents to open the Status Page, page 11-35.

Step 2 Click the **Add** button to add a Performance Monitor server using the Add or Edit Status Provider Dialog Box, page 11-36.

Step 3 Fill in the information that identifies the Performance Monitor server. The key fields in this dialog box are:

- Provider name, short name—These are the names displayed in Security Manager. They do not need to match anything configured on the device.
- Server—The IP address or fully qualified host name of the Performance Monitor server.
- User name, password, confirm password—A user account that can log into the Performance Monitor server.

You can change the other fields as needed for your installation. Change the polling period if you want it to be more or less frequent.

Click **OK** when finished; the Performance Monitor is added to the Providers list.

Step 4 Click **Save** on the Status page to save your changes.

Tip You can selectively disable or enable Performance Monitor servers on this page by changing the setting in the Status column. This allows you to temporarily discontinue polling a server for status without deleting its registration.

Troubleshooting Performance Monitor Status Collection

If you configure Security Manager to obtain device status from Performance Monitor, as explained in Configuring Status Providers, page 60-9, and the Inventory Status Window is not displaying status from Performance Monitor, ensure that you have configured all required elements to enable this connection:

- **Configure each device for monitoring by Performance Monitor.**

  You must configure the basic settings that Performance Monitor requires for monitoring a device, such as SNMP and syslog. For specific information on the required configurations, see the bootstrapping information in the “Before You Begin” chapter in *User Guide for Cisco Performance Monitor*.

Note Security Manager and Performance Monitor do not support the same devices. You can obtain status information from Performance Monitor only for those devices supported by both applications.

- **Add each device to the Performance Monitor inventory.**

  The "Before You Begin" chapter in *User Guide for Cisco Performance Monitor* explains how to add devices to Performance Monitor.

- **Add each supported monitored device to the Security Manager inventory.**

  See Adding Devices to the Device Inventory, page 3-6 for specific instructions.

- **Register Performance Monitor as a status provider in Security Manager.**

  This procedure establishes communications between Security Manager and the Performance Monitor server, and is described in Configuring Status Providers, page 60-9. You can register up to five Performance Monitor servers in Security Manager.

  Verify that the user account you configure in Security Manager for Performance Monitor is defined on the Performance Monitor server.

If you verify that this configuration is correct, consider the following troubleshooting tips:

- Ensure that you can log into the Performance Monitor server from the Security Manager server. Security Manager establishes an SSL connection with each registered Performance Monitor, and after authenticating the Performance Monitor credentials, Security Manager begins to receive status reports. Being able to log in from your workstation does not test this connection; you must log into Windows on the Security Manager server, then open a browser connection to Performance Monitor.
- If some devices are displaying Performance Monitor status, while others are not, verify that the devices that are missing information are included in the Performance Monitor inventory, and that the devices are not excluded from monitoring in Performance Monitor. If you exclude the device from Performance Monitor polling, the device health and performance reports are no longer available in Security Manager.
- Security Manager displays only the most-recent event of each type. That is, Security Manager does not accumulate the events reported by status providers at different points in time.

  For example, assume that at 12:00 noon, Performance Monitor logs a "Device" event with "Critical" severity and an "Interface" event at "Warning" severity, and no events of either type have occurred since then. In this case, both events are displayed. However, if Performance Monitor then logs a "Device" event at "Warning" severity at 1:00 p.m. and another "Critical" Device event at 2:00 p.m., the "Critical" event at 2:00 p.m. is the only Device event retained and displayed. To see historical events, you must log into Performance Monitor.
- If Performance Monitor fails to get a response from a device within the polling timeout period, polling for all devices stops. Verify that Performance Monitor is still polling devices, and consider increasing the polling timeout value. Refer to the Performance Monitor documentation for more information.

Inventory Status Window

Use the Inventory Status window to view device properties and status for the devices that you are allowed to view. This window summarizes device information so that you do not have to open the device properties for each individual device.

In addition to device property information, you can view summary information about how the policies on each device are configured (whether local, shared, or not configured) and the policy objects that have overrides for each device.

If you are using Performance Monitor to monitor your devices, status information from Performance Monitor is included in the inventory summary. You can also view the status of configuration deployment to the device.

The Inventory Status window contains two panes. Use the upper pane to view a complete listing of all devices, to sort the devices by attribute, or to filter out certain ones. Use the lower pane to view the device property details of the device selected in the upper pane.

Navigation Path

Select **Tools > Inventory Status**.

Related Topics

- Viewing Inventory Status, page 60-9
- Configuring Status Providers, page 60-9
- Troubleshooting Performance Monitor Status Collection, page 60-10
- Filtering Tables, page 1-33
- Table Columns and Column Heading Features, page 1-34

Field Reference

Table 60-2 Inventory Status Window

Element	Description
Device Summary Information for All Devices (Upper Pane)	
Export button	Click this button to export the inventory as a comma-separated values (CSV) file. You are prompted to specify a file name and to select a folder on the Security Manager server. You can use the export file for reference or analysis.
Display Name	The name of the device as it is displayed in Security Manager.
Deployment	The status of the configuration deployment for the device. This column appears only if you enabled Deployment as a status provider (see Status Page, page 11-35).
Performance Monitor	The status for the device as reported by Performance Monitor. This column appears only if you configured the device to be monitored by a Performance Monitor server, and you configured Security Manager to obtain status from that server. For more information, see Status Page, page 11-35.
OS Type	The family of the operating system running on the device, for example, IOS, IPS, ASA, FWSM, or PIX.
Running OS Version	The version of the operating system running on the device.
Target OS Version	The target OS version for which you want to apply the configuration. Configurations are based on the commands supported by this version.
Host Name.Domain Name	The DNS host and domain names for the device.
IP Address	The management IP address of the device.

Table 60-2 Inventory Status Window (Continued)

Element	Description
Device Type	The type of device.
Details for the Selected Device (Lower Pane)	
The detailed information is shown in the tabs in the lower pane. The information is organized into folders; click the +/- icons to open and close folders, or double-click the folder name.	
Inventory	Lists summary information about the selected device's device properties, deployment methods, device group membership, and the parent device for modules.
Policy	Lists the current status of the policies that can be configured for the selected device, whether the policy is unassigned (not defined), a local policy, or a shared policy.
Policy Object Overrides	Lists policy objects that have overrides defined for the selected device. For more information on policy object overrides, see Policy Object Override Pages, page 3-42.
Status	Lists status providers with any status messages for the selected device. Events are organized by event type. Event details include timestamp, description, and recommended action. The time stamp indicates the time of the last change in status for the device, not the time of the latest polling of the device. Also shown is the highest severity level of the status messages. For Performance Monitor, the event statuses are equivalent to the following Performance Monitor event priorities: • Critical events—P1, P2. • Major events—P3. • Minor events—P4. • Warning events—P5.
Navigation buttons	Click the navigation buttons to move through the inventory list. From left to right, buttons mean go to the first device in the list, go to the previous device, go to the next device, and go to the last device. The center field indicates which device is currently selected based on the row number (for example 5/10 means the fifth of 10 devices in the list).

Integrating CS-MARS and Security Manager

While Cisco Security Manager lets you centrally manage security policies and device settings in your network, the Cisco Security Monitoring, Analysis and Response System (CS-MARS) is a separate application that monitors devices and collects event information, including syslog messages and NetFlow traffic records, with much more extensive network monitoring capabilities than Security Manager. CS-MARS aggregates and presents massive amounts of network and security data in an easy-to-use format. Based on information derived from CS-MARS reports, you can edit device policies in Security Manager to counter security threats.

Specifically, if you use Security Manager to configure firewall access rules and IPS signatures, you can configure CS-MARS to collect information related to those policies and make it available to Security Manager users. By registering the CS-MARS servers with Security Manager, users can navigate directly from a specific access rule or IPS signature to a CS-MARS report window, pre-populated with query criteria for that rule or signature.

Similarly, CS-MARS users can view the Security Manager policies related to specific CS-MARS events. This bi-directional mapping of specific events to the policies that triggered them, combined with the ability to immediately modify the policies, can dramatically reduce the time spent configuring and troubleshooting large or complex networks.

To enable this cross-communication, you must register your CS-MARS servers with Security Manager, and register your Security Manager server with the CS-MARS servers. You must also register the specific devices with each application. Then, when working with firewall access rules or IPS signatures for a device, a Security Manager user can quickly view real-time and historical event information related to that rule or signature.

The following sections explain how to enable and use CS-MARS and Security Manager cross-communication:

- Checklist for Integrating CS-MARS with Security Manager, page 60-14
- Looking Up CS-MARS Events for a Security Manager Policy, page 60-19
- Looking Up a Security Manager Policy from a CS-MARS Event, page 60-23

Checklist for Integrating CS-MARS with Security Manager

To enable the cross-communication between CS-MARS and Security Manager (as described in Integrating CS-MARS and Security Manager, page 60-13), you must identify the applications to each other and ensure that devices managed by both applications are configured appropriately. The following table describes the integration steps.

If you have problems with cross-communications, see Troubleshooting Tips for CS-MARS Querying, page 60-18.

Table 60-3 Integrating CS-MARS and Security Manager

Task	Description
Add the devices to Security Manager and CS-MARS	See Adding Devices to the Device Inventory, page 3-6 for information about adding devices to Security Manager. See the *Device Configuration Guide for Cisco Security MARS* for information about adding devices to the CS-MARS inventory. A device must be supported by both applications to provide cross-communication for the device. Supported device types generally are those providing Firewall > Access Rules, or IPS > Signatures policies. (These include: PIX, ASA and FWSM appliances, Cisco IOS routers, Cisco IPS sensors and modules, and Cisco Catalyst switches.)
Configure the devices as required by each application	See Chapter 2, "Preparing Devices for Management" for information about basic configuration requirements for Security Manager. See *Device Configuration Guide for Cisco Security MARS* for the more extensive requirements for CS-MARS.
Register Security Manager with CS-MARS	For information on configuring CS-MARS to communicate with Security Manager, see *User Guide for Cisco Security MARS Local and Global Controllers*. You might want to create a CS-MARS user account specifically for linking with Security Manager. See Configuring the Security Manager Server to Respond to CS-MARS Policy Queries, page 60-16.
Register CS-MARS controllers with Security Manager	For information on registering CS-MARS controllers with Security Manager, see Registering CS-MARS Servers in Security Manager, page 60-16.
Link CS-MARS controllers to the devices in Security Manager	In Security Manager, you can proactively discover the CS-MARS controllers that monitor a particular device by clicking **Discover CS-MARS** on the device's Device Properties page, as described in Discovering or Changing the CS-MARS Controllers for a Device, page 60-17. Otherwise, the appropriate controller is discovered automatically when a user attempts to look up events for the device (the user is prompted to select a controller if more than one monitors the device).

Related Topics

- Viewing CS-MARS Events for an Access Rule, page 60-20
- Viewing CS-MARS Events for an IPS Signature, page 60-22
- Looking Up a Security Manager Policy from a CS-MARS Event, page 60-23

Configuring the Security Manager Server to Respond to CS-MARS Policy Queries

CS-MARS must be allowed access to the Security Manager server so that it can perform policy lookup queries and obtain policy information.

- If you are using Common Services AAA authentication on the server (for example, Cisco Secure ACS), you must update the administrative access settings to ensure that CS-MARS has the necessary client access to the Security Manager server.
- Define a user account in Security Manager that CS-MARS can use to perform queries. A separate account is recommended to provide a specific audit trail on the Security Manager server. This account must be assigned one of the following Common Services roles:
  - Approver
  - Network Operator
  - Network Administrator
  - System Administrator

Users with the Help Desk security level can only view the policy look-up table in CS-MARS; that is, they cannot cross-launch Security Manager to modify policies.

Note When you register a Security Manager server with CS-MARS, if you choose to prompt for Security Manager credentials for policy table look-up, a separate CS-MARS account in Common Services for authentication purposes might not be necessary.

For more information on adding users and associating roles with them in Common Services, see the *User Guide for CiscoWorks Common Services*.

Related Topics

- Registering CS-MARS Servers in Security Manager, page 60-16
- Discovering or Changing the CS-MARS Controllers for a Device, page 60-17

Registering CS-MARS Servers in Security Manager

As described in Checklist for Integrating CS-MARS with Security Manager, page 60-14, you must register your CS-MARS controllers with Security Manager to enable cross-communication between the applications if you intend to use the applications together.

Then, when a user looks up events for a device, Security Manager identifies the CS-MARS controller that is collecting events for that device. If more than one CS-MARS controller is collecting events for a device, the user can select which to use. You can also specify the correct CS-MARS controller to use in the Device Properties window for each device. (See Discovering or Changing the CS-MARS Controllers for a Device, page 60-17 for more information.)

Note For information about the CS-MARS versions explicitly supported by Security Manager, see the *Release Notes for Cisco Security Manager* for this version of the product. If you do try to use a version that is not explicitly supported, you cannot use CS-MARS versions earlier than 4.3.4 or 5.3.4.

Step 1 Choose **Tools > Security Manager Administration** and select **CS-MARS** in the table of contents to display the CS-MARS Page, page 11-4.

Step 2 Click the **Add** button to add a CS-MARS server. The New CS-MARS Device dialog box opens (see New or Edit CS-MARS Device Dialog Box, page 11-5 for detailed information).

Step 3 In the New CS-MARS Device dialog box, enter the IP address or fully qualified DNS host name of the server, and a user name and password for logging into the server. If you add a local controller, the user name you enter can be either a local account or a global account. Choose the type of account from the User Type list.

Tip If you are using CS-MARS Global Controllers, add them instead of individual Local Controllers. By adding Global Controllers, Security Manager can identify the correct Local Controller for a device, without you having to add each Local Controller. When you add a Global Controller, do not add the individual Local Controllers monitored by the Global Controller.

Click **Retrieve From Device** to get the server's authentication certificate. Click **Accept** when the certificate is presented to you.

Click **OK** when finished. The New CS-MARS Device dialog box closes and the server is added to the CS-MARS device list.

Step 4 From the **When Launching CS-MARS** list, choose whether you want users to be prompted to log in to the CS-MARS server when they request event status, or whether Security Manager should automatically log in to CS-MARS using the credentials provided when the user logged in to Security Manager.

If you elect to use Security Manager credentials, the necessary user accounts must be configured in CS-MARS. Refer to the CS-MARS documentation for more information.

Step 5 Click **Save** on the CS-MARS page to save your changes.

Discovering or Changing the CS-MARS Controllers for a Device

If you use the Cisco Security Monitoring, Analysis and Response System (CS-MARS) controllers to monitor devices, you can register them in Security Manager and then view syslogs and events that are related to firewall access or IPS signature rules for individual devices.

Security Manager can automatically discover the CS-MARS controllers that monitor a device when you try to view events related to a rule. If more than one controller monitors a device, you are prompted to select which controller to use.

You can also proactively select the CS-MARS controller for a device in its Device Properties window. Similarly, if you ever need to change the CS-MARS controller assigned to a device, you can change the selection in its Device Properties window. This procedure explains how to discover or change the CS-MARS controller for a device from its Device Properties window.

Before You Begin

The CS-MARS controller that monitors the device must already be registered with Security Manager on the CS-MARS administration page (**Tools > Security Manager Administration > CS-MARS**). For more information, see Registering CS-MARS Servers in Security Manager, page 60-16.

Step 1 In Device view, do one of the following in the Device selector to open the Device Properties dialog box:

- Double-click a device.
- Right-click a device and choose **Device Properties**.
- Select a device and choose **Tools > Device Properties**.

Step 2 Click **General** in the table of contents to open the General properties page (see General Page, page 3-34).

Step 3 In the CS-MARS Monitoring group, click **Discover CS-MARS**. Security Manager determines which registered controller is monitoring the device, if any. If there are more than one, you are prompted to select which CS-MARS controller to use.

Troubleshooting Tips for CS-MARS Querying

Use the following troubleshooting tips to help you identify and resolve problems you might encounter when using CS-MARS and Security Manager together:

- HTTPS is required for communication between the Security Manager server and CS-MARS.
- Interface names are not case-sensitive in Security Manager, but they are in CS-MARS. For example, “outside” and “Outside” are considered exclusive by a CS-MARS appliance, while they are equivalent in Security Manager. Further, syslog messages use lower case for all interface names. As a result, when you perform a query for a Security Manager policy from an event generated in CS-MARS, the interface name logged in the syslog event might not match the interface name in that policy in Security Manager. To avoid this problem, use lower case for all interface names, and in the definition of interface roles, in CS-MARS.
- To query for CS-MARS events from Security Manager policies, the Security Manager client must be on the same side of a network address translation (NAT) boundary as the CS-MARS appliance and the Security Manager server.

  Similarly, when the CS-MARS client is not on the same side of a NAT boundary as the CS-MARS appliance and the Security Manager server, you can look up Security Manager policies, but in read-only mode. However, you cannot start the Security Manager client from the read-only policy look-up table. The Security Manager client must be on the same side of the NAT boundary as the CS-MARS appliance and the Security Manager server if you want to start the client from CS-MARS to modify a matching policy.
- For FWSM, PIX and ASA devices on which multiple independent security contexts exist, to query for CS-MARS events, you must define a unique management IP address in Security Manager for each security context. Also, the host name and reporting IP address for each virtual context must be configured before adding it to CS-MARS. Otherwise, event look-up from policies on these contexts fails.
- For all IPS device and service policies, a default signature policy is assigned to the device when you do not discover IPS policies, or when you remove the configured policies from the device. If you try to perform event look-up from the default signature, a “Policy not found” error message is displayed. However, if you edit the default signature and save it, you can then navigate to events in CS-MARS.
- If object grouping or rule optimization is enabled for an access rule defined in Security Manager and the associated access-list commands on the device do not match the optimized rules, no events are displayed in CS-MARS.
- If logging is not enabled for an access rule, a warning message is displayed, and you can only look up traffic-flow events for those rules.

- When supported by the device, Security Manager uses access-control entry (ACE) hashcodes as additional keywords when querying CS-MARS for syslog messages generated by an ACE, and large access-control lists (ACLs) might contain thousands of such hashcodes. If the number of keywords, or the sum of the number of sources, destinations, and protocols for an ACE or a signature exceeds the query limit of 150, an error message is displayed. The error message indicates the probable cause and recommended action.
- Problems with the synchronization between rules and reported events can occur in the following situations:
  - The device has been added to Security Manager, but the configuration or changes to it have not been saved to the database. This is especially true for access rules that have been changed but not deployed since the device was added to CS-MARS.
  - Access rules exist on the device for which there are no corresponding rules in Security Manager, and vice versa. Be sure all devices are added to Security Manager, and that access rules are configured on them using Security Manager.
  - Traffic in the "wrong" direction triggering events for which there is no defined rule. For example, outbound traffic on a higher-security-level interface on which only inbound-traffic rules have been defined.
- If you perform a policy lookup from CS-MARS and the Security Manager client is active, the query is performed on all policies within the open activity or configuration session plus what is saved in the database (the committed configurations). If the Security Manager client is not active, only committed policies are considered.

Related Topics

- Checklist for Integrating CS-MARS with Security Manager, page 60-14
- Looking Up CS-MARS Events for a Security Manager Policy, page 60-19
- Registering CS-MARS Servers in Security Manager, page 60-16

Looking Up CS-MARS Events for a Security Manager Policy

After you integrate CS-MARS and Security Manager, you can look up events in CS-MARS that relate to specific firewall access rules or IPS signatures.

When CS-MARS receives events, they are parsed, "sessionized," written to an event buffer, and then written to the database. Sessionizing takes two forms: with a session-oriented protocol, such as TCP, the session encompasses the initial handshake to the connection tear-down; with a sessionless protocol, such as UDP, the session start and end times are based more on first and last packets tracked within a restricted time period—packets that fall outside of the time period are considered parts of other sessions.

Because of there is a difference between newly-received and fully processed data, you can look up either real-time or historical events:

- **Real-time**—Because sessionization takes time, keeping an event in cache for up to two minutes, you can use the real-time event query to view events right after parsing, providing access to the most current data received.

  When you query for real-time events, the query is run automatically, based on the policy values obtained from Security Manager, and the results are displayed in the CS-MARS Query Results window. This real-time event viewer lets you monitor CS-MARS traffic in near real-time, as raw events streaming to CS-MARS, before they are sessionized, with a maximum delay of five seconds.

You also can elect to view the sessionized event stream by clicking Edit in the Query Results window and then choosing "Sessionized events" from the Realtime drop-down menu. Note that more delay is possible when there are many events in a session.

- **Historical**—Historical event reports help you identify trends over longer periods of time than is possible with real-time monitoring. When you query for historical events, the CS-MARS Query Criteria: Result window opens. You can either run the query immediately, or save the criteria as a "report" to run at a later time. For historical events, the Result Format is the All Matching Events option, and the Filter By Time value is set to the previous 10 minutes.

The following topics explain event lookup in more detail:

- Viewing CS-MARS Events for an Access Rule, page 60-20
- Viewing CS-MARS Events for an IPS Signature, page 60-22

Viewing CS-MARS Events for an Access Rule

From the **Firewall > Access Rules** policy in Security Manager, you can select an access rule and view related event information in CS-MARS. You can view real-time or historical events matching the rule, the traffic flow, the source address, or the destination address. You can view events for any device that supports access rules, including ASA, PIX, FWSM, routers, and switches.

Firewall access rules are presented in the form of an ordered list or table. When deployed, this policy becomes an access-control list (ACL), with each entry in the list known as an access-control entry (ACE). (For more detailed information, see Understanding Access Rules, page 14-1.)

When deciding whether to forward or drop a packet, a device tests the packet against each access rule in the ordered listed. If you enable logging for an access rule, the results of the test are recording according to your per-rule log settings. Some devices, such as ASA, generate log entries for denied access even if you do not configure logging explicitly. For information on creating access rules, including logging options, see Configuring Access Rules, page 14-7.

You can query CS-MARS for real-time or historical events related to an access rule for the following types of traffic. To use the commands, right-click the rule and select them from the context menu.

- **Flow**—A traffic flow is defined by the rule's source and destination IP addresses, protocol, and ports. The reported flow events include connection set-up and tear-down. Logging need not be enabled for the access rule to record this information.

  To view flow-related events, use the following right-click commands:

  - **Show Events > Realtime > Matching this Flow**—To view real-time query results in CS-MARS for events matching this traffic flow. You can change the query criteria in the CS-MARS window at any time, applying new parameters to alter the real-time results.
  - **Show Events > Historical > Matching this Flow**—Opens the historical query criteria page in CS-MARS with fields populated based on the selected rule's traffic flow. Edit the rule parameters and query criteria as desired, and click **Apply** to continue. Next, in the Query window, you can submit the query or save it for later submission and re-use.

- **Rule**—If logging is enabled for the rule (in the Advanced and Edit Options Dialog Boxes, page 14-13), the device sends syslog messages to CS-MARS to record the logged events (assuming CS-MARS monitors the device). This query includes the access-rule parameters, including available keyword information. Reported events do not include connection set-up and tear-down.

To view rule-related events, use the following right-click commands:

- **Show Events > Realtime > Matching this Rule**—To view real-time query results in CS-MARS for events matching this rule (flow parameters plus keywords); results begin scrolling within five seconds. You can change the query criteria in the CS-MARS window at any time, applying new parameters to alter the real-time results.
- **Show Events > Historical > Matching this Rule**—Opens the historical query criteria page in CS-MARS with fields populated based on the access rule (flow parameters plus keywords). Edit the rule parameters and query criteria as desired, and click **Apply** to continue. Next, in the Query window, you can submit the query, or save it for later submission and re-use.

- **Source or Destination**—If you right-click the Source or Destination cell in an access rule entry, you also can choose to view real-time or historical events matching the rule's source or destination IP address.

  To view events for a source or destination address, right-click the address in the Source or Destination cell and choose one of the following commands (the specific command differs depending on the cell you select):

  - **Show Events > Realtime > Matching this Source/Destination**—To view real-time query results in CS-MARS for events with a matching source or destination address. You can change the query criteria in the CS-MARS window at any time, applying new parameters to alter the real-time results.
  - **Show Events > Historical > Matching this Source/Destination**—Opens the historical query criteria page in CS-MARS with fields populated based on the access rule's source or destination address. Edit the rule parameters and query criteria as desired, and click **Apply** to continue. Next, in the Query window, you can submit the query, or save it for later submission and re-use.

Security Manager provides the following information to CS-MARS as criteria for a traffic-flow or access-rule event queries:

- Device details—General information about the device, such as host name, domain name, management IP address, and display name.
- Source addresses—Source addresses of hosts and the network/host objects expanded to display the networks or collections of IP addresses.
- Destination addresses—Destination addresses of hosts and the network/host objects expanded to display the networks or collections of IP addresses.
- Service—Protocol and port information.
- Event Type—"Built/teardown/permitted IP connection" for permit rules and "Deny packet due to security policy" for deny rules.
- Keyword (rule events only, not provided for traffic-flow queries)—ACL name and ACE hashcode, if available, connected by the logical operator OR.

  On Version 7.0 or later PIX and ASA devices, each access rule is assigned an MD5 hashcode, which is included in the syslogs generated by that rule. Large ACLs can include thousands of access rules. Used as query keywords, these hashcodes can help produce more-accurate event matches. If a device does not support hashcodes, a warning is displayed that query results might be inaccurate because of keyword ambiguity; you can proceed with the query, and then edit the query keyword list and resubmit.

Tips:

- You can query on only one access rule at a time.
- When NAT or PAT is configured on a security device, the source and destination addresses are mapped to pre-translation and post-translation addresses, respectively, and the translated addresses are used when Security Manager sends a query to CS-MARS. For inbound access rules, the destination address is considered the pre-translation address, and for outbound access rules, the source address is considered the post-translation address.
- If the device is monitored by multiple CS-MARS controllers, you are prompted to select the CS-MARS instance to be used.
- Depending on how credentials verification is set up on your system, you might be prompted to log into CS-MARS. For more information, see Registering CS-MARS Servers in Security Manager, page 60-16.

Related Topics

- Access Rules Page, page 14-8
- Looking Up CS-MARS Events for a Security Manager Policy, page 60-19
- Viewing CS-MARS Events for an IPS Signature, page 60-22

Viewing CS-MARS Events for an IPS Signature

When an IPS or IOS IPS device detects and reports a network intrusion by comparing incoming traffic to a configured signature, a syslog message is generated on the device. If the device is monitored by CS-MARS, an incident is generated in CS-MARS after the log associated with the signature is obtained from the device. Looking up the events associated with a specific signature lets you quickly identify attacks and tune your device configuration to minimize or prevent intrusions.

To view reported network intrusion events in CS-MARS, you can select one or more entries in the Signatures policy for a device in Security Manager and navigate to the CS-MARS Query page to view real-time and historical events.

When you look up real-time events for a signature, the query is run automatically and the results displayed in CS-MARS. However, when you look up historical events for a signature, the values sent by Security Manager to CS-MARS are used to populate the query fields. You can modify the query fields as desired, and then run the query, or save it for later use.

Security Manager provides the following signature information to CS-MARS as query criteria:

- Device details—General information about the device, such as host name, domain name, management IP address, and display name.
- Keyword—Signature ID, subsignature ID, and virtual sensor name, if applicable.

  For virtual sensors, the name of the sensor is included as a keyword criterion along with other device information and signature parameters.

Related Topics

- Looking Up CS-MARS Events for a Security Manager Policy, page 60-19
- Viewing CS-MARS Events for an Access Rule, page 60-20

Step 1 (Device view) With an IPS or IOS IPS device selected, select **IPS > Signatures > Signatures** to display the Signatures Page, page 33-4.

Step 2 Right-click the desired entry in the signatures table, or select multiple entries before right-clicking one of them, and choose one of the following commands from the **Show Events** menu:

- **Realtime**—To view real-time query results in CS-MARS for events matching this signature; results begin scrolling within five seconds. Use this option to view raw events as they stream to CS-MARS.

  You can change the query criteria in the CS-MARS Query Results window at any time, applying new parameters to alter the real-time results.

- **Historical**—Opens the historical query criteria page in CS-MARS with fields populated based on the signature parameters. Edit the parameters and query criteria as desired, and click Apply to continue. Next, in the Query window, you can submit the query or save it for later submission and re-use. You can edit the query and save it as a report if you want to run it again later.

Tips:

- If a signature is disabled, you are warned and asked if you want to proceed to event lookup.
- If the device is monitored by multiple CS-MARS controllers, you are prompted to select the CS-MARS instance to be used.
- Depending on how credentials verification is set up on your system, you might be prompted to log into CS-MARS. For more information, see Registering CS-MARS Servers in Security Manager, page 60-16.
- All custom signatures are categorized as "Unknown Device Event Type" events in CS-MARS.
- A default signature is assigned to an IPS device if you elect not to discover IPS policies when adding the device to the Security Manager inventory, or when you remove configured IPS policies from the device. If you try to look up events from the default signature, a "Policy not found" error message is displayed. However, if you edit the default signature and save it, you can then query for related events in CS-MARS.
- Events of type Packet Data and Context Data are not displayed in the query results because these events are not triggered by signature rules.

Looking Up a Security Manager Policy from a CS-MARS Event

The *User Guide for Cisco Security MARS Local and Global Controllers* contains detailed information about how to look up policies based on events shown in CS-MARS. The information includes extensive troubleshooting information to help resolve any problems you might have, plus a checklist of what you must configure in CS-MARS to enable the interaction.

The main reason you would want to perform policy lookup is to adjust a policy based on the events that it is generating. For example, an access rule might be dropping traffic that you actually want to allow. Because you are looking at the event, you know there is a policy that is causing the event, so with a few clicks, you can get from that event to the policy you need to reconfigure.

The general process for looking up a policy based on a device-generated event is as follows. Note that the Security Manager client must be installed on your system to perform policy lookup.

Related Topics

- Viewing CS-MARS Events for an Access Rule, page 60-20
- Viewing CS-MARS Events for an IPS Signature, page 60-22

Step 1 Find the event in CS-MARS in the Query Results or Incident Details pages.

For more information on the syslog and NetFlow events you can use for querying access rules, see the following topics:

- System Log Messages Supported for Policy Look-up, page 60-24
- NetFlow Event Reporting in CS-MARS, page 60-26

Step 2 Click the Security Manager icon in the Reporting Device cell for the event. You might be prompted to log into Security Manager, based on how you configured CS-MARS.

If more than one device in Security Manager matches the event characteristics, you are prompted to select a device.

Step 3 Detailed information is obtained from Security Manager and presented based on whether the event is for an access rule or IPS signature:

- **Access rule**—The access rules are displayed in CS-MARS in a read-only window with the rule that matches the event highlighted.

  If you decide to edit a rule, click the rule number, and you are taken to the rule in the Access Rule policy in the Security Manager client. You can then make your edits, save them, and then deploy configurations. Remember that your changes are not made to the device until you deploy them.

  For more information on configuring access rules, see Configuring Access Rules, page 14-7.

- **IPS Signature**—Signature details are displayed in CS-MARS in a read-only window.

  To edit the signature, click **Edit Signature**, and you are taken to the signature in the Signatures policy, where you can make your changes. For more information, see Editing Signature Parameters (Tuning Signatures), page 33-18.

  If you decide you want to instead remove specific actions from an event, or remove the event entirely, and prevent further processing by the sensor, click **Add Filter**. This opens the Add Event Filter dialog box in Security Manager, where you can configure an event filter. For more information, see Filter Item Dialog Box, page 34-9.

  As with access rules, your changes do not take effect until you deploy the new configuration.

System Log Messages Supported for Policy Look-up

When you configure access rules on security appliances and IOS devices, you can configure logging options in the Advanced and Edit Options Dialog Boxes, page 14-13 that generate system log (syslog) messages. On devices with multiple contexts, each security context includes its own logging configuration and generates its own messages. If Security Manager is configured to interoperate with CS-MARS, these messages are reported to CS-MARS and you can query for the reported information on a per-rule basis.

For additional information about each of these message IDs, see the System Message Guide of the relevant product documentation.

Security-appliance messages

Security-appliance syslog messages begin with a percent sign (%) and are structured as follows:

```
%{ASA | PIX | FWSM}-Level-Message_number: Message_text
```

For example:

```
%ASA-2-302013: Built outbound TCP connection 42210
for outside:9.1.154.12/23 (9.1.154.12/23) to inside:2.168.154.12/4402 (192.168.154.12/4402)
```

Note that additional information, such as date and timestamp, precedes these messages. The specific additional information depends on the type of device.

A unique six-digit number identifies each message (*302013* in the preceding example). The following security-appliance syslog message IDs are supported for Security Manager-to-CS-MARS queries. If you change the logging level of a security appliance, be sure these messages are generated at the new level.

Message ID	Message
106023	An IP packet was denied by the access rule. This message is recorded even if logging is not enabled for the rule; this is the Default Logging option.
106100	An IP packet was permitted or denied by the access rule. Additional information is provided, based on the logging level defined for the rule in the Advanced and Edit Options Dialog Boxes, page 14-13.
302013	A TCP connection between two hosts was created.
302014	A TCP connection between two hosts was torn down.
302015	A UDP connection between two hosts was created.
302016	A UDP connection between two hosts was torn down.
302020	A ICMP connection between two hosts was created.
302021	A ICMP connection between two hosts was torn down.

Router messages

On Cisco IOS routers, syslog messages are also generated for access rules. The first packet that triggers the access list causes an immediate logging message, and subsequent packets are collected over five-minute intervals before they are displayed or logged. Each logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior five-minute interval.

The following IOS syslog message IDs are supported for Security Manager-to-CS-MARS queries.

%SEC-6-IPACCESSLOGP	A packet matching the log criteria for the given access list was detected: TCP and UDP.
%SEC-6-IPACCESSLOGS	A packet matching the log criteria for the given access list was detected: IP address.
%SEC-6-IPACCESSLOGDP	A packet matching the log criteria for the given access list was detected: ICMP.
%SEC-6-IPACCESSLOGNP	A packet matching the log criteria for the given access list was detected: all other IPv4 protocols.

Note If an excessive number of syslog messages are being generated and reported to CS-MARS, use the Advanced and Edit Options Dialog Boxes, page 14-13 to change the logging level for those access rules that are producing the largest number of messages. You can also look at changing the logging policies on the device to limit the types of messages generated.

NetFlow Event Reporting in CS-MARS

Event reporting in CS-MARS can include NetFlow events from an ASA 8.1+ device.

NetFlow Security Event Logging uses NetFlow version 9 fields and templates to efficiently deliver security telemetry in high-performance environments. NetFlow Security Event Logging scales better than syslog messaging, while offering the same level of detail and granularity in logged events. The ASA NetFlow implementation exports only significant events in the life of a flow, rather than exporting data about flows at regular intervals. The following flow events are exported:

- Flow creation
- Flow tear-down
- Flows denied by an access rule

The ASA also exports syslog messages that contain the same information. If you enable NetFlow on a device, you can consider disabling the equivalent syslog messages. Disabling equivalent syslog messages can help avoid the potential performance degradation caused by generating and processing both NetFlow records and syslog messages representing the same event. The following table lists syslog messages with an equivalent NetFlow event; the NetFlow Event IDs and Extended Event IDs are included. For information on how to disable NetFlow equivalent syslog messages, see Server Setup Page, page 44-15.

Syslog ID	Syslog Description	NetFlow Event ID	Extended Event ID
302013 302015 302017 302020	TCP, UDP, GRE, and ICMP connection creation.	1 = Flow Created.	0 = Ignore.
302014 302016 302018 302021	TCP, UDP, GRE, and ICMP connection tear-down.	2 = Flow Deleted.	0 = Ignore, or > 2000 = ASP drop reasons.
710003	An attempt to connect to the device's interface was denied.	3 = Flow Denied.	1003 = To-the-box flow denied due to configuration.
106015	A TCP flow was denied because the first packet was not a SYN packet.	3 = Flow Denied.	1004 = Flow denied because first packet was not a TCP SYN packet.
313001	An ICMP packet to the device was denied.	3 = Flow Denied.	1003 = To-the-box flow denied due to configuration.
313008	An ICMP v6 packet to the device was denied.	3 = Flow Denied.	1003 = To-the-box flow denied due to configuration.
106023	A flow was denied by an access list attached to an interface with the access group command.	3 = Flow Denied.	1001 – Flow denied by Ingress ACL. 1002 – Flow denied by Egress ACL.

Syslog ID	Syslog Description	NetFlow Event ID	Extended Event ID
106100	An access rule was hit.	1 = Flow Created (if ACL permitted the flow). 3 = Flow Denied (if ACL denied the flow).	0 – If Flow permitted by ACL. 1001 – Flow denied by Ingress ACL. 1002 – Flow denied by Egress ACL.

For the Flow Denied NetFlow event, an Extended Event ID indicates the reason for denial, as shown in the following table.

Extended Event ID	Event	Description
1001	FLOW DENIED	The flow was denied by an Ingress ACL.
1002	FLOW DENIED	The flow was denied by an Egress ACL.
1003	FLOW DENIED	The security appliance denied an attempt to connect to the interface service. For example, this message appears (with the service SNMP) when the security appliance receives an SNMP request from an unauthorized SNMP management station.
1004	FLOW DENIED	The flow was denied because the first packet was not a TCP SYN packet.
> 2000	FLOW DELETED	Values above 2000 represent various reasons for a flow being terminated.