CHAPTER 2

Reporting and Mitigation Devices Overview

Revised: November 30, 2007, OL-14647-02

After you complete the initial configuration of Local Controller as described in *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*, you must determine a monitoring strategy to use for your network. You must also determine a mitigation strategy, if you chose to take advantage of the MARS mitigation features. For guidance on how to determine the monitoring and mitigation strategies, see STM Task Flow Overview, page 1-1.

This chapters assumes that you have made corporate-level policy decisions and that you are executing against the Checklist for Provisioning Phase, page 1-2. This chapter provides the following:

- Guidance on selecting and configuring reporting devices and mitigation devices
- Discussion of the levels of operation that MARS supports
- Guidance on selecting a method for adding devices to Local Controller
- Discussion of those features that enable rich data collection

It contains the following sections:

Before configuring the MARS Appliance to recognize reporting devices, you should understand the three levels of operation that MARS can achieve.

Levels of Operation

MARS operates at three discernible levels based on the type of data collected from reporting devices and the features such data enables for the system.These levels focus on the ability to identify attacks from end-to-end, and they are separate from the features enabled by specific types of reporting devices.

- **Basic.** At this level, MARS behaves like a smart syslog server. It collects reporting device logs and support basic queries and reports. To enable basic operation, you must complete the initial configuration of the MARS Appliance as described in *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*. In addition, you must specify the device name and reporting IP addresses of the reporting devices as described in Adding Reporting and Mitigation Devices, page 2-17.
- **Intermediate.** At this level, MARS processes events and performs session-based correlation, including resolving NAT and PAT translations at the IP address layer. To enable intermediate operation, you must provide more details about the devices you want to monitor, including access IP addresses, management access passwords, OS platforms and versions, and running services and applications, see IP Management, page 24-3 for more information.
- **Advanced.** This level is a fully enabled MARS Appliance. When advanced operation is enabled, MARS Appliance discovers and displays the full topology, draws attack paths, and enables MAC address lookups of the hosts involved in an attack. To enable advanced operation, you must provide the SNMP community string information for your network. You must also enable topology discovery, as defined in Scheduling Topology Updates, page 2-40.

Table 2-1 summarizes the levels, their configuration requirements, and the features enabled at that level.

Table 2-1 Levels of Operation

Level Of Operation	Configuration Requirements	Functionality Enabled
Level 1	MARS configured Reporting device names and reporting IP addresses added NetFlow enabled	Basic syslog functionality Event correlation Query, reports, and chart support NetFlow anomaly detection
Level 2	Access IP addresses and information added	Starts performing event and session-based correlation NAT and PAT resolution IP address lookup of attackers and targets
Level 3	Community strings and networks added	MAC address lookup of attackers and targets Topologies enabled

Selecting the Devices to Monitor

All monitoring strategies involve selecting the types of devices to monitor and how much data to provide the MARS Appliance. All devices on your network, be they hosts, gateways, security devices, or servers, provide some level of data that MARS can use to improve the accuracy of security incident identification. However, careful consideration of what data to provide can improve the attack identification response time by ensuring that MARS does not perform necessary or redundant event correlation and analysis. Unnecessary logging and reporting by reporting devices can also reduce the effectiveness of your network.

We recommend analyzing each network segment to identify the most data rich combination that you can achieve, while identifying and refining your configurations to reduce redundant data.

When determining a monitoring strategy, you must also determine the goals behind the monitoring. Is it just for attack detection? Attack detection and mitigation? Regulatory compliance? Your goals affect which devices you must monitor and what features you must configure on those devices.

Consider distinct goals:

- Attack detection
- Attack detection and mitigation
- Regulatory compliance
- Full NAC awareness
- Identify the devices/feature pairs that overlap on the same network segment, where a choice between device can reduce duplicity or prioritize device performance

Last, you must consider an event tuning method for your monitoring strategy. How you tune your MARS affects your overall operational costs proportionally to the number of device of a give type that are monitored. Essentially, if you have the bandwidth available, we recommend that you tune the events at the MARS Appliance, which reduces your operational costs by tuning at a single point in the network. However, if bandwidth is a precious commodity, you may chose to tune the event propagation at the reporting device level, preventing the events from going onto the network.

Table 2-2 identifies the device types, describes what information they can provide, and recommends how to configure these devices within your network.

Table 2-2 Device Types and Data Available

Device Type	Data Available	Recommended Configurations
Router	The device discovery protocol is the one used for administrative access/mitigation. For example, if SSH is used to discover the device, then SSH is the protocol that used to pushed the mitigation command. The following data is pulled from routers: • hostname • static routes • ACL rules • static NAT rules • traffic flows • SNMP RO Community strings • NetFlow data • device status and resource utilization, such as memory, CPU, and interface/port statistics. • ARP cache table. Used to map IP address to MAC address.	Enable the following: • SNMP RO community strings • Syslog traffic • Device discovery via SSH or Telnet access
Switch	During investigation and mitigation, the ARP cache tables are reviewed to resolve the MAC addresses involved in the incident. This data is cached for 6 hours. SNMP RO Community strings Forwarding tables, used to map IP address to MAC address. Device status and resource utilization, such as memory, CPU, and interface/port statistics. NetFlow data 802.1x logs generated during NAC sessions	Enable the following: • SNMP RO community strings • Syslog traffic • Device discovery via SSH or Telnet access • Enable NetFlow data • Administrative access for mitigation push

Table 2-2 Device Types and Data Available (continued)

Device Type	Data Available	Recommended Configurations
Firewall	**Interface configurations.** Used to populate topology view and determine expected routes, which helps refine correlation of traffic traversing the firewall. **NAT and PAT mappings.** Used to identify the point of origin attackers and targets and trace attacks as they spread. **Firewall policies.** When discovering ASA, PIX, and FWSM, MARS parses ACLs and conduits (PIX only). For Check Point firewalls, it collects the firewall policy from policy table. MARS using this information only for path computation and mitigation recommendations. It is not used by any other components, such as rules, reports, and sessionization. **Firewall logs.** Accepted and denied sessions logs are used to identify false positives and determine if potential attacks were blocked before reaching their targets. **Audit logs.** Associates users with authentication sessions and assists in identifying exploited accounts and administrative sessions. **ARP cache tables.** Used to map IP address to MAC address. **Device status and resource utilization information.** Used to identify anomalous network activities based on memory, CPU, and interface and port statistics.	Enable the following: • SNMP RO community strings • Syslog messages • Device discovery
VPN	**Remote user information.** Provides username to IP address mapping. VPN client helps determine the person who logged in and performed specific actions. Clarifies the true point of origin by identifying the host, not the VPN concentrator. **Login/logout records.** Helps identifies worms by tracing outbreaks back to a specific user and provides network access periods. **Device status information.** Identifies whether the device is operational, which allows prediction of possible spread of potential attacks and worms. • SNMP RO Community strings	

Table 2-2 Device Types and Data Available (continued)

Device Type	Data Available	Recommended Configurations
Network IDS/IPS	**Fired signature alerts.** Identifies attacks and threats, which helps determine mitigation response, identify potential false positive information, and target vulnerability assessment probes conducted by MARS. **Trigger packet information.** Provides the payload of the packet that caused the signature to fire. Determine whether an attack was blocked at a specific device. Device status information	
Host IDSes	Provides host-level validation of exploits and blocked attacks, which improves the accuracy of false positive identification, which in turn improves the ability of the administrator to accurately prioritize the work required to contain attacks.	
Anti-Virus	Central anti-virus management servers provide information on which hosts are infected, which hosts have reported attempted infections, etc. The servers also provide the dat or signature file information for managed hosts, which improves the ability to determine whether an attack was likely to have succeeded.	
Vulnerability Assessment	**Host OS and Patch Level.** When a signature fires on an IDS and it is reported to MARS, MARS can either launch a targeted scan using Nessus, or query a vulnerability assessment system that helps determine whether the target was vulnerable.	Enable any vulnerability assessment solutions supported by MARS.

Table 2-2 Device Types and Data Available (continued)

Device Type	Data Available	Recommended Configurations
Host OSes	**Microsoft Windows Hosts** Events found in the security event log as well application event and system event log.	Install and configure SNARE, which pushes events to MARS in near real time, and scales more efficiently than pulling events from hosts.
	Solaris and Linux Hosts Incoming network session logs, via inted, and FTP transfer logs, via xferlog. In addition, any events that are written to the system log by applications and services running on host.	• Enable logging for the xferlog and inetd applications. • Enable syslog daemon. • Identify the MARS Appliance as syslog target.
	Generic Hosts (All OSes) Includes system-level information, such as privilege escalation and buffer overflow. Helps determine what attacks make it to the host layer. If MARS learns of activity at the host level, then it understands that the attack or exploit has successfully traversed the network. MARS correlates this data with the network level data to discover the whole incident and analyze the exploit method so the administrator can build a better defense. In some cases, MARS recommends actions for mitigating the attack. We recommend that you maintain these recommended blocks as long as similar attacks are expected. Typical blocking techniques, such as IPS shunning, often fail to identify the best chokepoint for containment. As part of the recommended action, MARS does identify the optimal chokepoint where the recommended action should be effected.	
Web Server	Same as hosts (SNARE and Perl script agents) need this when the hosts cannot send us the logs via syslog. agent is basically a transport.	
Web Proxy	Mapping from user to site, translations for the IP address mapping, tells us the real address of the host who is likely infected. URLs and also filtering...regulatory compliance.	
Database	Login/logout to determine the actual user (query report tab on the data). Privilege escalation, brute force crack type stuff, or maybe we want to do regulatory compliance.	

Table 2-2 Device Types and Data Available (continued)

Device Type	Data Available	Recommended Configurations
AAA Server	Login/logout and NAC functionality (deny a person due to privileges, it triggers NAC message) • passed authentication log • failed attempts log • RADIUS accounting log, including those events specific to NAC.	Supporting Cisco Secure ACS Server, page 15-2 Supporting Cisco Secure ACS Solution Engine, page 15-2
Generic Syslog	Same as host, provides support for additional customer devices.	
Generic SNMP	Same as host, provides support for additional customer devices.	
Cisco Security Manager	Mapping to any committed policy rules defined in Security Manager that match any ACL rules that could cause the generation of a specific syslog event by a reporting device. This policy lookup feature allows you to debug network issues and understand the cause/effect relationships between event messages and the device policies and traffic that resulted in the generation of the event.	Enable HTTPS on the Security Manager server. Define an administrative level account on the Security Manager server that CS-MARS can use for policy lookups.

Understanding Access IP, Reporting IP, and Interface Settings

When defining a reporting or mitigation device in the web interface, MARS allows (and at times, requires) you to specify several IP addresses. Understanding the purpose of the different addresses is important to effectively defining the devices that you want to monitor and manage. It is also important to understand their relationship to other settings that you can identify.

If a device has a single interface and a single IP address associated with that interface, the access and reporting IP addresses are the same as the address assigned to the interface. MARS collects this information separately to support those devices that have multiple interfaces, multiple IP addresses associated with a single interface, or both.

Note Not all reporting devices support both an access and reporting IP address. Some devices use only access IP addresses to query the device for the required information (e.g., QualysGuard security service), while others have no settings that MARS can discover and only generate event messages for MARS to process (e.g., NetCache appliances). In addition, not all devices require the definition of interfaces.

This section discusses the following three addresses and their relationship to other settings:

- Access IP, page 2-9
- Reporting IP, page 2-9
- Interface Settings, page 2-10

Access IP

MARS uses the access IP address to either connect to the device for network-based administrative sessions or connect to a remote server on which a file containing the device's configuration is stored. The expected value is determined by the access type you select. Most devices also require that you explicitly identify the IP addresses of hosts allowed to administer them. The MARS Appliance must be listed among such hosts as part of the device preparation.

The protocol that MARS uses to connect to the device is defined by the access type value, which is a dependency for enabling administrative access. Once MARS has administrative access, it can perform device discovery, which includes settings such as ARP tables, NAT, routes, and active ACLs, all of which helps MARS understand the topology, perform attack path analysis, and identify false positive incidents. Discovery can be performed to varying degrees using any of the access types. For more information on access types, see Selecting the Access Type, page 2-10.

MARS also uses SNMP RO and SNMPwalk to discover the device settings and topology information. However, the two methods of discovery are distinct and have distinct requirements. SNMPwalk requires the access IP address and the SNMP access type. SNMP RO discovery does not requires the SNMP access type, but it does require the access IP address.

Note MARS does not support the following characters in the SNMP RO community string: ' (single quote), " (double quote), < (less than symbol), and > (greater than symbol).

In addition, both SNMPwalk and SNMP RO are unrelated to SNMP notifications or SNMP traps. SNMPwalk and SNMP RO both require that MARS initiate the information request, where as SNMP notifications are event notifications published by the reporting device, much the same as syslog messages are. As with syslog messages, SNMP notifications are published over the reporting IP address.

Reporting IP

The reporting IP is the source IP address of event messages, logs, notifications, or traps that originate from the device. MARS uses this address to associate received messages with the correct device. For single-homed devices, the reporting IP address is the same as the access IP; for dual- or multi-homed devices, this address must be explicitly associated with the syslog, NetFlow, and SNMP services running on the reporting device. Most devices also require, for each message type, that you explicitly identify the IP addresses of hosts to which messages should be published. These hosts are commonly referred to as target log servers. The MARS Appliance must be listed among such hosts as part of the device preparation.

The role in MARS of the reporting IP address differs from that of the access IP address in that the reporting IP address is treated passively from the MARS perspective. MARS does not query the device using this address. Such operations are performed using the access IP address and the access type.

MARS accepts only one reporting IP address per device. For devices supporting two message formats, such as NetFlow and syslog, you must ensure that both message formats are bound to the same source IP address (the reporting IP). In Cisco IOS devices, this common association is not the default so you must change either the syslog or the NetFlow reporting IP address to match the other. If the message types do not originate from a common IP address, one of them is seen as originating from an unreported device and MARS does not parse those events correctly.

The supported format of event data varies among reporting devices. Just because the device is able to generate syslog, NetFlow, and SNMP notifications does not mean that MARS processes all three formats. The document, *Supported Devices and Software Versions for Cisco Security MARS Local Controller 4.3.x and 5.3.x*, identifies the event retrieval protocol supported by each device type.

Interface Settings

Interface settings are exclusive to hosts and software applications running on hosts. While MARS can discover the settings of a reporting device that is a software application running on a host, it cannot discover settings about the host itself. The role of interface settings in MARS is different from that the access IP address and reporting IP address. Interface settings represent static information, not discovered or learned, about the host.

When correlating events specific to a host or reporting devices running on that host, MARS needs to understand the number of interfaces installed in the host, their names, and the IP addresses and networks associated with them. MARS uses the interface settings to guide discovery operations, to determine attack path vectors, and to perform Nessus vulnerability assessments.

Selecting the Access Type

The access type refers to the administrative protocol that MARS uses to access a reporting device or mitigation device. For most devices monitored by MARS, you can choose from among four administrative access protocols:

- **SNMP.** SNMP access provides administrative access to the device using a secured connection. It allows for the discovery of the settings using SNMPwalk, such as routes, connected networks, ARP tables, and address translations. If granted read-write access, SNMP also allows for mitigation on any L2 devices that support MIB2.

Note MARS uses SNMP v. 1 to perform device discovery. If MARS is unable to discover a device and you are confident that the configuration settings are correct, verify that the device is not expecting the authentication from MARS to occur over an encrypted channel.

- **Telnet.** Telnet provides full administrative access to the device using an unsecured connection. It allows for the discovery of the settings, such as routes, connected networks, ARP tables, and address translations. It also allows for mitigation on L2 devices.
- **SSH.** SSH provides full administrative access to the device using a secured connection. It allows for the discovery of the settings, such as routes, connected networks, ARP tables, and address translations. It also allows for mitigation on L2 devices. This access method is recommended for DTM support; however, Telnet access can achieve the same results.

Note Device discovery based on an SSH connection does not support 512-byte keys. The OpenSSH client (OpenSSH_3.1p1) used by MARS does not support a modulus size smaller than 768.

- **FTP.** FTP passive discovery of settings by providing MARS access to a file copy of the configuration running on the router. FTP does not support mitigation, DTM, or discovery of dynamic settings, such as NAT and ARP tables. In addition, if you select the FTP access type for device types, such as Cisco ASA and FWSM, you can only discover settings for the admin context.

This access method is the least preferred and most limited access method. To enable configuration discovery using FTP access, you must place a copy the device's configuration file on an FTP server to which the MARS Appliance has access. This FTP server must have users authentication enabled.

Note TFTP is not supported. You must use an FTP server.

You can use any access scheme in conjunction with an SNMP RO community string. The division between Access IP and Reporting IP is clearly illustrated by an FTP access type example. Assume that you have SNMP RO access to a router, but your configuration discovery (access type) is restricted to a file stored on an FTP server.

When you define a device in MARS, the Access IP is the IP address of the FTP server (not the router), and the authentication information is used to access the FTP server. The Access Method is set to FTP. The Reporting IP is the IP address of the interface over which SNMP traps are published by the router.

The following topics describe how to configure each access type, identifying the fields that should be completed when a specific access type is selected. For efficiencies sake, these procedures are referenced throughout the specific device configuration topics, as they related to a specific device type.

- Configure SNMP Access for Devices in MARS, page 2-11
- Configure Telnet Access for Devices in MARS, page 2-12
- Configure SSH Access for Devices in MARS, page 2-12
- Configure FTP Access for Devices in MARS, page 2-12

Configure SNMP Access for Devices in MARS

This procedure assumes you are defining a reporting device or mitigation device and that you were referred to this procedure after selecting SNMP in the Access Type list. To select SNMP as the access type, you must provide MARS with SNMP read-write access.

Note The SNMP access type is not required to enable the SMPO RO strings. In fact, no access type is required to support SNMP RO. SNMP RO uses a shared, read-only community string; it does not require a read-write community string as does the SNMP access type.

If you selected SNMP as the access type, follow these steps:

Step 1 In the Login field, enter the username of the administrative account to use when accessing the reporting device.

Note MARS uses SNMP v. 1 to perform device discovery. If MARS is unable to discover a device and you are confident that the configuration settings are correct, verify that the device is not expecting the authentication from MARS to occur over an encrypted channel.

Step 2 In the Password field, enter the password associated with the username specified in the Login field.

Step 3 If this device supports an enable mode, enter that password in the Enable Password field.

Configure Telnet Access for Devices in MARS

This procedure assumes you are defining a reporting device or mitigation device and that you were referred to this procedure after selecting TELNET in the Access Type list.

If you selected TELNET as the access type, follow these steps:

Step 1 In the Login field, enter the username of the administrative account to use when accessing the reporting device.

Step 2 In the Password field, enter the password associated with the username specified in the Login field.

Step 3 If this device supports an enable mode, enter that password in the Enable Password field.

Configure SSH Access for Devices in MARS

This procedure assumes you are defining a reporting device or mitigation device and that you were referred to this procedure after selecting SSH in the Access Type list.

Note Device discovery based on an SSH connection does not support 512-byte keys. The OpenSSH client (OpenSSH_3.1p1) used by MARS does not support a modulus size smaller than 768.

If you selected SSH as the access type, follow these steps:

Step 1 From the list box to the right of the Access Type list, select **3DES**, **DES**, or **BlowFish** as the encryption cipher for SSH sessions between the MARS Appliance and the reporting device.

Step 2 In the Login field, enter the username of the administrative account to use when accessing the reporting device.

Step 3 In the Password field, enter the password associated with the username specified in the Login field.

Step 4 If this device supports an enable mode, enter that password in the Enable Password field.

Configure FTP Access for Devices in MARS

This procedure assumes you are defining a reporting device or mitigation device and that you were referred to this procedure after selecting FTP in the Access Type list.

If you selected **FTP** as the access type, follow these steps:

Step 1 In the Login field, enter the username of the FTP server account to use when accessing the configuration file of the reporting device.

Step 2 In the Password field, enter the password associated with the username specified in the Login field.

Step 3 In the Config Path field, enter the path to the reporting device's configuration file residing on the FTP server.

This path begins at the root of the FTP server's published folder, not at the root directory of server.

Step 4 In the File Name field, enter the name of the reporting device's configuration file residing on the FTP server.

Note If you select **FTP,** you cannot enter an enable password.

Bootstrap Summary Table

Table 2-3 summaries the settings that you must configure for reporting devices and mitigation devices. It also provides links to any required agent downloads and to detailed configuration information.

Table 2-3 Reporting and Mitigation Device Bootstrap Summary

Device Type/Name	Bootstrap Summary	Reference Information
Router/Switch		
Cisco Router	1. Access to IP address/interface by MARS. 2. FTP, SNMP, Telnet or SSH access by MARS. 3. Define SNMP RO community string. 4. Turn on syslog, define log level, and define MARS as target of syslog messages. 5. Enable NAC features.	Cisco Router Devices, page 4-1
Cisco Switch (IOS)		Cisco Switch Devices, page 4-9
Cisco Switch (CatOS)		
Extreme ExtremeWare	1. Access to IP address/interface by MARS. 2. (ExtremeWare only) Turn on syslog, define log level, and define MARS as target of syslog messages. 3. SNMP access by MARS. 4. Define SNMP RO community string.	Extreme ExtremeWare 6.x, page 4-17
Generic Router		Generic Router Device, page 4-19
Firewall Devices		
Cisco PIX	1. Access to access and reporting IP address/interface by MARS. 2. FTP, Telnet, or SSH access by MARS. 3. Define SNMP RO community string. **Note** SNMP settings should be defined for the admin context on ASA and FWSM. You do not need to define these settings for each security context. 4. Turn on syslog, define log level, and define MARS as target of syslog messages.	Bootstrap the Cisco Firewall Device, page 5-2
Cisco Adaptive Security Appliance (ASA)		
Cisco Firewall Services Module (FWSM)		
Cisco IOS Firewall Feature Set		
Juniper Netscreen		NetScreen ScreenOS Devices, page 5-20

Table 2-3 Reporting and Mitigation Device Bootstrap Summary (continued)

Device Type/Name	Bootstrap Summary	Reference Information
Checkpoint Opsec NG and Firewall-1 Nokia Firewall (running Checkpoint)	1. Add the MARS Appliance as a host. 2. Create and install an OPSEC Application object for the defined host. 3. Define policies to permit SIC traffic between the MARS Appliance, the Check Point management server, and any remote servers. 4. Define the log settings to push the correct events to the defined host. 5. Install the policies.	Bootstrap the Check Point Devices, page 5-31
VPN Devices		
Cisco VPN Concentrator		Cisco VPN 3000 Concentrator, page 6-1
Network IDS		
Cisco Network IDS Cisco IDSM	1. Enable RDEP for IDS modules. 2. Configure the following signature actions: • Alert • (Optional) To view trigger packets, enable the "produce-verbose-alert". • (Optional) To view IP logs, enable the alert or "produce-verbose-alert" and "log-pair-packets".	Cisco IDS 3.1 Sensors, page 7-1 Cisco IDS 4.0, IPS 5.x, and IPS 6.x Sensors, page 7-5
Cisco Intrusion Prevention System (IPS), Network IPS	1. Enable SDEE for IPS modules. 2. Configure the following signature actions: • Alert • (Optional) To view trigger packets, enable the "produce-verbose-alert". • (Optional) To view IP logs, enable the alert or "produce-verbose-alert" and "log-pair-packets".	Cisco IDS 4.0, IPS 5.x, and IPS 6.x Sensors, page 7-5
Cisco IPS ASA module	1. Enable SDEE for IPS modules. 2. Configure the following signature actions: • Alert • (Optional) To view trigger packets, enable the "produce-verbose-alert". • (Optional) To view IP logs, enable the alert or "produce-verbose-alert" and "log-pair-packets".	Cisco IPS Modules, page 8-16

Table 2-3 Reporting and Mitigation Device Bootstrap Summary (continued)

Device Type/Name	Bootstrap Summary	Reference Information
Cisco IOS IPS module	1. Enable SDEE for IPS modules. 2. Configure the following signature actions: • Alert • (Optional) To view trigger packets, enable the "produce-verbose-alert". • (Optional) To view IP logs, enable the alert or "produce-verbose-alert" and "log-pair-packets".	Cisco IPS Modules, page 8-16
McAfee Intrushield		IntruVert IntruShield, page 8-37
Juniper Netscreen IDP		NetScreen IDP Device and Server Support, page 8-46
Symantec Manhunt		Symantec ManHunt, page 8-44
ISS RealSecure		ISS RealSecure 6.5 and 7.0, page 8-32
Snort		Snort 2.0, page 8-43
Enterasys Dragon		Enterasys Dragon 6.x, page 8-49
Host IDS		
Cisco Security Agent		Cisco Security Agent 4.x and 5.x Device, page 8-4
McAfee Entercept		Entercept Entercept 2.5 and 4.0, page 8-1
ISS RealSecure Host Sensor		ISS RealSecure 6.5 and 7.0, page 8-32
Anti-virus		
Symantec AntiVirus		Symantec AntiVirus Configuration, page 9-1
Cisco Incident Control System (Cisco ICS), Trend Micro Outbreak Prevention Service (OPS)		Cisco Incident Control Server, page 9-15
McAfee ePolicy Orchestrator		McAfee ePolicy Orchestrator Devices, page 9-10
Network Associates VirusScan		McAfee ePolicy Orchestrator Devices, page 9-10
Vulnerability Assessment		
eEye REM		eEye REM 1.0, page 10-3
Qualys QualysGuard		Qualys QualysGuard Devices, page 10-6
Foundstone Foundscan		Foundstone FoundScan 3.0, page 10-1
Host Operating Systems		

Table 2-3 Reporting and Mitigation Device Bootstrap Summary (continued)

Device Type/Name	Bootstrap Summary	Reference Information
Windows	Do one of the following: • Install and configure the SNARE agent • Create or edit an administrative account to ensure that it has permissions to pull the event data	Syslog (pushed by SNARE agent) or event data pull using MS-RPC Push Method: Configure Generic Microsoft Windows Hosts, page 11-5 Pull Method: Configure the Microsoft Windows Host, page 11-6
Solaris	—	Syslog (from Device) Sun Solaris and Linux Hosts, page 11-2
Redhat Linux	—	Syslog (from Device) Sun Solaris and Linux Hosts, page 11-2
Web Server		
Microsoft Internet Information Server	—	Syslog (from SNARE agent) Install and Configure the Snare Agent for IIS, page 13-1
Sun iPlanet	—	HTTP (from MARS Agent) Install and Configure the Web Agent on UNIX or Linux, page 13-7
Apache	—	HTTP (from MARS Agent) Install and Configure the Web Agent on UNIX or Linux, page 13-7
Web Proxy		
NetApp NetCache	—	HTTP Network Appliance NetCache Generic, page 14-1
Database Server		
Oracle	TCP	SQLnet (from Host) Oracle Database Server Generic, page 12-1
AAA Server		
Cisco Secure Access Control Sever (ACS)	—	Syslog (from MARS Agent) Install and Configure the PN Log Agent, page 15-7 (Cisco Secure ACS)
Cisco Secure ACS Appliance	Install and configure remote log agent.	Syslog (from MARS Agent) on secondary host Supporting Cisco Secure ACS Solution Engine, page 15-2 Install and Configure the PN Log Agent, page 15-7 (Cisco Secure ACS)
SNMP and Syslog Servers		

Table 2-3 Reporting and Mitigation Device Bootstrap Summary (continued)

Device Type/Name	Bootstrap Summary	Reference Information
Generic Syslog Server	Publish syslog messages to MARS Appliance. Enable SNMP access by MARS Appliance.	Adding Generic Devices, page 11-1
Generic SNMP Server	Enable SNMP access by MARS Appliance.	Adding Generic Devices, page 11-1
Other		
Cisco Security Manager	Enable HTTPS access by MARS Appliance	Checklist for Policy Table Lookup from MARS, page 17-13 Bootstrapping Security Manager Server to Communicate with MARS, page 17-15 Adding a Security Manager Server to MARS, page 17-16

Adding Reporting and Mitigation Devices

Three methods exist for adding reporting devices and mitigation devices to MARS:

- Manually add the devices one at a time.
- Add multiple devices using a seed file.
- Discover devices automatically using SNMP RO community strings.

From the Security and Monitor Devices page, you can add or edit the reporting devices and mitigation devices that MARS monitors. To access this page, click **Admin > System Setup > Security and Monitor Devices**. You can search for, add, edit, delete, change display status, and load devices from the seed file.

The device support is categorized into three categories:

- **HW-Based Security Devices.** Hardware-based devices represent routers, switches, and other dedicated security appliances. You can add such reporting devices by selecting the appropriate device.
- **SW-Based Security Devices.** Software-based devices represent applications that reside on a host, rather than a dedicated appliance. You can add reporting device on a new host by selecting **Add SW security apps on new host** or on an existing host by selecting **Add SW security apps on existing host**.

Note You can only define one SW security application for each reporting device. For example, if you have multiple Oracle databases running on a server, you cannot add separate instances to the same host. To work around this issue, use multiple servers or have the different applications report to MARS using unique reporting IP addresses. When using unique IP addresses, each one represents a unique host in MARS on which you can define a single SW security application.

- **On-Demand Security Services.** Security services represent subscription-based services provided by vendors using a central security operations center (SOC) with remote monitoring nodes. These services, such as Qualys QualysGuard, represent systems from which MARS periodically pulls data. You can add such reporting devices by selecting the appropriate service. These devices also require you to define a schedule for pulling data (see Scheduling Topology Updates, page 2-40).

The complete list of supported devices is presented in the *Supported Devices and Software Versions for Cisco Security MARS Local Controller 4.2.x and 5.2.x* document. Devices are added to this list on an ongoing basis via software upgrade packages. See *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System* for details on how to upgrade your MARS Appliance.

MARS can also support any syslog or SNMP devices, even if they do not appear on the list of devices supported by the MARS. You can enter any syslog or SNMP device into the network topology, configure it to report data to the MARS, and query it using a free-form query. (See To Run a Free-form Query, page 21-2.)

For more information on adding devices, see:

- Add Reporting and Mitigation Devices Individually, page 2-18
- Add Multiple Reporting and Mitigation Devices Using a Seed File, page 2-21
- Adding Reporting and Mitigation Devices Using Automatic Topology Discovery, page 2-26

Regardless of the method that you have used to add the devices, you should also perform the following tasks:

- Verify Connectivity with the Reporting and Mitigation Devices, page 2-27
- Activate the Reporting and Mitigation Devices, page 2-28

Add Reporting and Mitigation Devices Individually

In general, you have two choices for adding devices that you want to monitor into your MARS. You can create a seed file or you can add each device manually. Seed file support is limited to a few device types, see Column E, page 2-24 for the devices supported.

When manually configuring devices, select the devices that are most interesting to you. Once added, you can come back and edit them as necessary. Manual configuration is also useful when you add or change a single security device on your network.

Note Remember that you do not have to add all of the devices configuration information at once. You can start by adding the device's name and its access IP address. You can always return later, when the MARS starts to report to you, and provide more details.

To add a device manually, follow these steps

Step 1 Click **Admin > System Setup > Security and Monitor Devices > Add**.

Step 2 Select the device from the list.

Step 3 Enter the information needed to communicate with the device.

Step 4 Click **Submit**.

Step 5 Once add a device, you must click **Activate** for MARS to correctly process events received from that device. For more information, see Activate the Reporting and Mitigation Devices, page 2-28.

Edit a Device

Step 1 Check the box next to the device.

Step 2 Edit the device's settings.

Step 3 Click **Submit**.

Upgrade the Device Type to a Newer Version

You can change the Device Type version setting of a hardware-based security device. You cannot upgrade the version for software applications running on a host. To upgrade the software appliance version, you must remove the application from the host and add the newer one.

This version change feature applies only to device types with the same vendor and model but different versions. Specifically, you can change the version for the following device types:

- Cisco IDS
- Cisco PIX
- Cisco VPN Concentrator
- NetScreen ScreenOS

For example, you could change the settings for the device type Cisco PIX 6.1 to Cisco PIX 7.0 without having to delete the device and add it again. The benefit of matching the version setting to the deployed device is that it allows MARS to correlate any event types introduced in the more recent version. It also allows you to incrementally upgrade your reporting devices without having to worry about when to add that reporting device to MARS. The events that are correlated under one device type will be associated with the newer device type version when you make the change in MARS.

To change the version of a device, follow these steps:

Step 1 Click **Admin > System Setup > Security and Monitor Devices**.

Step 2 Select the checkbox to the left of the device for which you want to change the version, and click **Change Version**.

The Change the Device Type Version page appears, displaying the device name, vendor, model, and old version type information.

Step 3 Select the new version in the New Device Type Version list.

Step 4 To change the version of the device to the new version, click **Submit**.

If any additional changes are available due to the version change, the Edit page appears.

Step 5 If the Edit page appears, make any desired changes and click **Submit**.

Step 6 Once you change the version setting for a device, you must click **Activate** for MARS to correctly process events received from that device. For more information, see Activate the Reporting and Mitigation Devices, page 2-28.

Delete a Device

When you define a reporting device in MARS, this device is added in two separate pages of the web interface. It appears where you have defined it, on the Admin > Security and Monitoring Devices page, as well as under the general device identification page under Management > IP Management. This duplication of content is based on the different functions that each of these pages serves.

The Security and Monitoring Devices page configures the contact and device type information, whereas the IP Management page is used by the parser module to correlate known devices versus unknown devices. Typically when you delete a device from the Security and Monitoring Device page, you still want to retain the knowledge of that device in MARS so that historical incidents and events and cases can resolve to a known device; therefore, the device is not deleted from the IP Management page.

Note Deleting a device does disassociate any historical incidents and events from the IP address. In other words, once you delete the device, you will not be able to find historical events for that device even if you re-add the device at a later date.

However, if you need to delete and re-add a device to MARS, you must delete the device from both pages before you attempt to re-add the device.

In addition, as devices are discovered on your network, they are added to the list of devices in the IP Management page. If you want to add a reporting device and find that you cannot, review the list of devices in the IP Management page to ensure that the device has not been auto-populated. If it has, you must first delete that device, then you can add it as a reporting device on the Security and Monitoring Devices page.

To delete a device, follow these steps:

Step 1 Select one of the following pages:

- Admin > Security and Monitoring Devices
- Management > IP Management

Step 2 Check the box next to each device you want to delete.

Step 3 Click **Delete**.

Step 4 On the confirmation page, click **Submit**.

The device is deleted from the selected page.

Delete All Displayed Reporting Devices

You can perform this procedure from the Admin > Security and Monitoring Devices page.

To delete all devices displayed on a page, follow these steps:

Step 1 On the Admin > Security and Monitoring Devices, select the checkbox to the left of the Device Name column heading at the top left of the table.

All displayed devices are selected.

Step 2 Click **Delete**.

A page appears prompting you to confirm that you want to delete the list of devices.

Step 3 Click **Submit** to delete all the selected devices.

Add Multiple Reporting and Mitigation Devices Using a Seed File

The seed file is a comma-delimited file with the file extension .csv (comma-separated value). Most spreadsheet programs let you import and export files as CSV files.

The following is a sample seed file as exported from a popular spreadsheet program:

```
10.1.1.1,,,,PIX,TELNET,,,cisco,,,,,,,,,,
192.168.229.241,,,,IOS,TELNET,,,csRv$12*,EcsRv$12$,,,,,,,,,
10.1.1.83,,,,PIX,SSH,pix,Vpnspn12,,vPfw1ne,,,,,,,,,
192.168.151.169,,,,PIX,SSH,pix,lpt$12,,pot$1*d1,,,,,,,,,
10.4.2.4,,,,NETSCREEN,SSH,netscreen,nt*$scn25,,,,,,,,,,,
10.4.2.3,,,,NETSCREEN,SSH,netscreen,nt*$scn10,,,,,,,,,,,
10.1.1.241,,,,IOS,TELNET,,,cisco,cisco,,,,,,,,,
10.4.2.1,,,,IOS,TELNET,,,Qa$1*5ft,gt$*j15,,,,,,,,,
10.4.2.2,,,,IOS,TELNET,,,Qa$1*5ft,gt$*j15,,,,,,,,,
wanRouter,public,,,IOS,SNMP,,,,,,,,,,,,,
myPix63,,,,PIX,SSH,pix,test1,,test1234,,,,,,,,,,10.2.3.1
MyPc,,,,WINDOWS,RPC,myname,mypass,,,,,,,,,,,
myPix70,,,,PIX7X,SSH,,,,,,,,,,,,,
myids40,,,,CiscoIDS4x,SSL,,,,,,,,,,,,,
myids50,,,,CiscoIPS5x,SSL,,,,,,,,,,,,,
myASA70,,,,ASA,SSH,,,,,,,,,,,,,
myWindowsNT,,,,WindowsNT,RPC,,,,,,,,,,,,,
myFWSM23,,,,FWSM,SSH,,,,,,,,,,,,,
```

With the CSV file, you can enter the values, passwords, and information for each device that you want the MARS Appliance to monitor in its appropriate row and column. While the seed file is useful for getting the MARS Appliance started processing event data for most devices, you may need to use the Admin > System Setup > Security and Monitoring Devices page to fine-tune the device manually. In addition, you must Activate the devices that you add using a seed file (see Activate the Reporting and Mitigation Devices, page 2-28).

Devices that Require Custom Seed Files

Some reporting devices represent the management consoles for the actual host- or node-based reporting devices. These consoles often represent centralized log servers for the devices they manage. However, for MARS to correctly correlate the logs for these centralized log servers, you must identify those host- or node-based reporting device. In some cases, MARS is able to dynamically learn of the hosts or nodes by parsing the logs. In other cases, you must use a seed file generated by management console to identify each of the managed reporting devices.

Once you generate the seed file, you must import that seed file under the host that represents the management console in the MARS web interface to load the sensor module information from the CSV or seed file. The device types that use a custom seed file are as follows:

- **Entercept**. For more information, see Extracting Entercept Agent Information into a CSV file (for Entercept Version 2.5), page 8-2.
- **IntruVert IntruShield**. For more information, see Extracting Intruvert Sensor Information from the IntruShield Manager, page 8-37.

- **Cisco Security Agent**. While MARS can learn of the CSA agents dynamically, you can also import the initial list of agents using a custom seed file. For more information, see Export CSA Agent Information to File, page 8-6.
- **Symantec AntiVirus**. While MARS can learn of the Symantec AntiVirus agents dynamically, you can also import the initial list of agents using a custom seed file. For more information, see Export the AntiVirus Agent List, page 9-8.

Devices that Require Updates After the Seed File Import

When you add specific reporting devices using a seed file, you must edit them to complete the definition of the device before you can monitor them. Typically, these devices are IDS/IPS devices that monitor specific networks. The device types that you must update are as follows:

- **Cisco IDS 4.x Devices**. These sensors are defined by importing a MARS-specific seed file as defined in Load Devices From the Seed File, page 2-25. However, once you import a sensor, you must identify the monitored networks that it monitors. For more information, see Specify the Monitored Networks for Cisco IPS or IDS Device Imported from a Seed File, page 7-9.
- **Cisco IPS 5.x Devices**. These sensors are defined by importing a MARS-specific seed file as defined in Load Devices From the Seed File, page 2-25. However, once you import a sensor, you must identify the monitored networks that it monitors. For more information, see Specify the Monitored Networks for Cisco IPS or IDS Device Imported from a Seed File, page 7-9.
- **IntruShield Senors**. These sensors are defined by importing a custom seedfile; however, once you import the sensors, which appear as children of the IntruShield Manager host, you must identify the monitored networks for each sensor. For more information, see Add IntruShield Sensors Using a Seed File, page 8-42.

Seed File Header Columns

Table 2-4 describes the columns in the seed files and identifies valid values. If you do not enter a value for a given column, you must enter a comma to delineate that column.

Note Remember that you do not have to add all of the devices' configuration information at once. You can start by adding the device's name and its access IP address. You can always return later, when the MARS starts to report to you, and provide more details.

Table 2-4 Seed File Column Description

Column	Type	Entry
Column A	NAME OR IP	The device's name or IP address. (Mandatory) If the device name is provided and Column U is empty, MARS performs a DNS lookup to identify the address which will be used to populate the Access and Reporting IP fields **Note** If an IP address appears in Column U, that address overrides any address or derived address specified in Column A. However, the name value specified in Column A is used.
Column B	SNMP RO/RW Community	The device's SNMP RO community name here. **Note** MARS does not support the following characters in the SNMP RO community string: ' (single quote), " (double quote), < (less than symbol), and > (greater than symbol).
Column C	EMPTY	Empty placeholder column.
Column D	EMPTY	Empty placeholder column.

Table 2-4 Seed File Column Description (continued)

Column	Type	Entry
Column E	DEVICE TYPE	The device type designator. (case insensative) **Note** Some of the devices supported in the GUI cannot be entered via a CSV file. Use the following strings represent the desired device type: • `ASA`: for Cisco ASA devices • `CiscoIDS4x`: for applaince running Cisco IPS 4.x (not modules) • `CiscoIPS5x`: for appliance running Cisco IPS 5.x (not modules) • `FWSM`: for Cisco FWSM 2.3 • `FWSM3`: for Cisco FWSM 3.1 • `PIX`: for Cisco PIX 6.0, 6.1, 6.2, and 6.3 devices • `PIX7X`: for Cisco PIX 7.0 devices • `IOS`: for Cisco IOS 12.2 (default) • `SWITCH-CATOS`: for Cisco Switch in Hybrid Mode • `SWITCH-IOS`: for Cisco Switch in Native Mode • `EXTREME`: for Extreme ExtremeWare 6.x • `NETSCREEN`: for ScreenOS 4.0 and 5.0 • `WINDOWS`: for Window host • `Windows2000`: for Windows 2000 host • `Windows2003`: for Windows 2003 host • `WindowsNT`: for Windows NT 4.x host. • `SOLARIS`: for Solaris host • `LINUX`: for Linux host **Note** In the case of host files, Linux, Solaris, and Windows, MARS is configured by default to receive events from the hosts specified in a seed file. However, for a Windows host where the RPC settings are also specified in the seed file, MARS will both pull and receive logs from the host by default.
Column F	ACCESS TYPE	The Access Type for this device. Your choices are: • TELNET • FTP • SSH • SNMP (default) • RPC (Windows only) In the RPC case, the username field (Column G) should be non-empty. The password can be provided in Column H. If RPC access type and username are given, the PULL flag is set by the backend in addition to the default RECEIVE flag.

Table 2-4 Seed File Column Description (continued)

Column	Type	Entry
Column G	USER NAME	The TELNET, SSH, FTP, or RPC user name. This column is only valid if you have used TELNET, SSH, or FTP in Column F.
Column H	SSH/FTP/RPC PASSWORD	The SSH or FTP Password for the device. This column is only valid if you have used SSH or FTP in Column F.
Column I	TELNET PASSWORD	The Telnet password for the device.
Column J	ENABLE PASSWORD	The enable password (applicable only with FWSM, PIX, or IOS devices).
Columns K	EMPTY	Emplty placeholder column.
Column L	EMPTY	Emplty placeholder column.
Column M	EMPTY	Emplty placeholder column.
Column N	EMPTY	Emplty placeholder column.
Column O	EMPTY	Emplty placeholder column.
Column P	EMPTY	Emplty placeholder column.
Column Q	EMPTY	Emplty placeholder column.
Column R	EMPTY	Emplty placeholder column.
Column S	EMPTY	Emplty placeholder column.
Column T	FTP LOCATION [if Access Type =FTP]	The location for the FTP file. This location starts from the FTP root, not the sysroot. If, for example, the file is at `<ftproot>/configdata/router1.txt`, using `./configdata/router1.txt` is correct.
Column U	Access/Reporting IP [optional]	The Access IP and Reporting IP address to use when populating this device. The MARS Appliance uses this address to communicate with the device. See Understanding Access IP, Reporting IP, and Interface Settings, page 2-8

Load Devices From the Seed File

Once you have completed the seed file, you must place the CSV file on to the FTP server from which the MARS Appliance will load it.

To load the file into the MARS, follow these steps:

Step 1 Click **Admin > System Setup > Security and Monitor Devices > Load From Seed File**.

Step 2 Enter the FTP Server's IP address, the user name and password for the FTP server, the path, and the file name for the seed file.

The FTP path starts from the FTP root, not from the sysroot for the configuration path.

Step 3 Click **Submit**.

Once you have loaded devices from the seed file, return to each device. Continue to configure the devices and to add information such as reporting IP addresses, and SNMP information.

Step 4 Once add a device, you must click **Activate** for MARS to correctly process events received from that device. For more information, see Activate the Reporting and Mitigation Devices, page 2-28.

Note Using a seed file to define the reporting devices replaces the manual definition of the device; however, the topology information will not be available. After adding the reporting devices via a seed file, you must either manually discover each device by selecting the device, clicking Edit, and then clicking the Discover button or by scheduling a topology discovery. In addition, some device types required that you define additional settings (see Devices that Require Updates After the Seed File Import, page 2-22).

Adding Reporting and Mitigation Devices Using Automatic Topology Discovery

On the Admin page, under the Topology Discovery Information section, three links exist, allowing you to define the settings required to discover reporting and mitigation devices automatically. These links are:

- **Community String and Networks.** Allows you to define SNMP RO community strings on a per network or IP range basis. Networks and SNMP RO stings can overlap. At least one SNMP string must be defined before discovery is attempted.
- **Valid Networks.** Identifies the set of networks and IP ranges that you want to discover. You should also define one or more SNMP targets. If no SNMP targets are defined, MARS uses it's own gateway as the SNMP target. SNMP targets should be layer 3 gateway devices, such as a router or firewall with SNMP RO community strings defined and discovery permitted; they should also be defined on a per network or per range basis if you wish to separate the discovery using schedule rules. At least one valid network must be defined before discovery is attempted.
- **Topology/Monitored Device Update Scheduler.** While not required for discovery, it does allow you to increase the frequency of topology discovery and further refine the potential depth of a discovery based on a particular schedule rule. The default schedule rule is once a month for all valid networks. However, if no valid networks are defined, the process wakes up, sees no valid networks are defined, and quits. Each schedule rule allows you to select which networks, as defined within the list of valid networks and ranges, that should be discovered according to frequency also specified in the rule. As connected networks often exist, you can refine which networks are discovered by ensuring that separate schedule rule exists for each network that you do not want to be automatically discovered as part of a connected network.

Based on the networks defined within the schedule rules, MARS starts with the first SNMP target associated with those networks or ranges as defined under Valid Networks and attempts to discover that device using SNMP discovery. The discovery process continues as long as the target device provides additional routes and the addresses of such routes are part of the networks in another schedule rule. The process also iterates through each SNMP target that is defined. The entire discovery process is limited based on the schedule rule's bounding networks, the SNMP targets, the valid network and IP ranges, and the SNMP RO community strings, which are defined on a per network basis. Networks and SNMP RO community stings can overlap, in which case MARS tries each string against the gateway addresses discovered within that network. The discovery process only discovers Layer 3 gateway devices, such as routers and firewalls. It does not discover hosts, unless those hosts are defined as the explicit target within a schedule rule (see Scheduling Topology Updates, page 2-40).

As the discovery process identifies supported reporting and mitigation devices, it adds those devices to the Monitoring and Security Devices list (Admin > Monitoring and Reporting Devices), identifying them by the Reporting IP. You can later edit these discovered devices to provide Access IP information and perform more thorough device-level discovery. Once a device is listed under Monitoring and Reporting Devices, it may be rediscovered, but it will not be added again unless it has been properly deleted (see Delete a Device, page 2-20).

For more information on these settings, see:

- Configuring Layer 3 Topology Discovery, page 2-38
- Scheduling Topology Updates, page 2-40

Note Once the discovery process is complete, you must click **Activate** for MARS to correctly process events received from that device. For more information, see Activate the Reporting and Mitigation Devices, page 2-28.

Verify Connectivity with the Reporting and Mitigation Devices

After loading the seed file or manually adding devices, you can verify that the devices were loaded by clicking **Admin > System Setup > Security and Monitor Devices**. You should see the devices that you have added populating this page.

You can test the devices by checking the box next to the name of the device and clicking **Edit**. On the device's page, click **Discover** or **Test Connectivity**. The UI displays a "holding pattern" screen while it connects to the device. When complete, it shows you the device's discovery screen.

Note Some devices cannot be checked for connectivity nor can be discovered. The next section, Discover and Testing Connectivity Options, page 2-27, contains a list of devices that can be checked or discovered.

Discover and Testing Connectivity Options

When you add a device, you should check its connectivity or perform the discovery. Checking a device's connectivity or discovery analyzes the device's configuration, checks that MARS can process its events, and that MARS can understand its NAT information.

You can test these devices for connectivity or perform discovery:

- Cisco IOS
- Cisco PIX
- Cisco ASA
- Cisco Switch CatOS
- Cisco Switch IOS
- Cisco IDS
- Cisco IPS 6.x
- Cisco IDSM
- Cisco FWSM
- Cisco Security Manager server
- Cisco VPN Concentrator 4.x
- Check Point
- Extreme ExtremeWare 6.x
- NetScreen

Run a Reporting Device Query

Another method to see the added devices, is to run a query with the display format: **Reporting Device Ranking**.

Note You might not see all of the devices that you loaded using the seed file right away because of lag, network size and traffic. If you do not see a device after waiting, it could be due to input error.

To run a reporting device ranking query, follow these steps:

Step 1 Click the **Queries / Reports** tab.

Step 2 On the Queries page, in the Query Event Data table, click **Event Type** in the Display Format column.

Step 3 Select **Reporting Device Ranking**.

Step 4 Click **Apply**.

Step 5 Click **Submit** to run the query.

Activate the Reporting and Mitigation Devices

After you have added reporting devices and mitigation devices to MARS, you must activate those devices before MARS begins to fully process the data provided by those devices. This processing is different from those devices discovered on the network, where the logs sent to the appliance are stored, but your ability to interact with that data is limited to queries and reports. Typically, MARS runs inspection rules and generates notifications only against the data retrieved from activated devices.

Once a device is known to the MARS Appliance, all data provided by that particular device can be normalized and sessionized, which enables that device's data to be used to fire an incident

Note Default installations of MARS do not fire incidents based on data received from unknown devices. However, you can still enable this by creating one or more rules that use keyword search. A device must be defined for the MARS to be able to parse and sessionize the event data. The act of parsing the event data correctly is what ensures rules fire more accurately.

Tip You must click Activate whenever you add or modify rules, drop rules, reports, or add or modify any options or settings under in the Admin tab other than those on the User Management subtab. Otherwise, the changes that you make will not take effect.

To activate added devices, follow these steps:

Step 1 For each device that you want to add, provide the device details and click **Submit** to add the device.

The Submit action stores the device details in the database. Once you click Submit, your work is saved, even if you drop the administrative connection before clicking Activate.

Step 2 Once you have all of the devices desired for this administrative session, click **Activate**.

The Activate action differs from Submit in that MARS begins to inspect and generate notifications about the data provided by the devices.

Tip If you are adding or editing several devices, it is better for the system to click **Activate** for several changes rather than for each individual change.

Data Enabling Features

Adding a the reporting devices and mitigation devices is the primary method of providing MARS with the data required to study the activities on your network. However, other features, both within the web interface and as part of configuring the devices, can provide MARS with additional data, which is used to refine the views it provides and to assist in the improving the overall effectiveness of the system. We think of these features as data enabling features.

This section contains the following topics:

- Layer 2 Discovery and Mitigation, page 2-30

  Enable SNMP community strings to support the discovery the network topology. Allows for mapping to the port level for switches. Combined with 802.1x support required by NAC, this setting can resolve MAC address level settings for attached and wireless nodes on the network.

- Networks for Dynamic Vulnerability Scanning, page 2-30

  Enables a Nessus-based scan of the targeted hosts. Nessus also uses nmap for OS fingerprinting and port scanning during a vulnerability assessment scan. These scans are conducted in response to suspicious activity to determine whether the attempted attack is successful or likely to succeed based on information such as target operating system type, patch level, and open ports on the host.

- Understanding NetFlow Anomaly Detection, page 2-31

  By enabling NetFlow, MARS can detect anomalies in traffic and network usage by comparing new events with summary data. When anomalies are detected, MARS begins to store full NetFlow data. By default, full NetFlow data is not stored by MARS unless an incident is identified.

- Host and Device Identification and Detail Strategies, page 2-37

  Details about reporting devices and the hosts that are on your network aids in the elimination of false positives, as well as improves the performance of MARS in assessing events.

- Configuring Layer 3 Topology Discovery, page 2-38

  Layer 3 topology discovery aids in attack path analysis, as well as the population of the topology graph in the web interface.

- Scheduling Topology Updates, page 2-40

  Topology update schedules are a critical part of many of the data enabling features, including discovery of Layer 2 and Layer 3 devices, as well as pulling information from specific reporting devices.

- Configuring Resource Usage Data, page 2-42

  MARS can collect additional data from a select set of reporting devices, which is used to provide reports about CPU utilization, memory utilization, and device saturation. This data can be helpful in detecting anomalies as well in network capacity planning.

- Configuring Network Admission Control Features, page 2-53

  Describes how to accomplish full NAC awareness, what it provides, and what products are required.

Layer 2 Discovery and Mitigation

Make sure that all the L2 devices have the SNMP RO community strings specified in the web interface for L2 mitigation, even if the access type is not SNMP. (See False Positive Confirmation, page 20-6 for more information on mitigating an attack.)

The SNMP RO community string is *always* required on Layer 2 devices for L2 mitigation. L2 devices must be added manually—there is no automatic discovery for these device.

Note MARS does not support the following characters in the SNMP RO community string: ' (single quote), " (double quote), < (less than symbol), and > (greater than symbol).

MARS does not discover L2 devices automatically as it does with L3 devices.

Note *L2 devices must be added manually; there is no automatic discovery for these devices.* Make sure all the L2 devices (switches) have the SNMP RO community strings specified in the web interface, even if the access type is not SNMP. The SNMP RO community string is always required on L2 devices for L2 mitigation.

You can specify which L3 devices to discover by specifying networks and SNMP RO community values, as defined in Configuring Layer 3 Topology Discovery, page 2-38.

The reason is MARS does not scan the network for devices. Therefore, you must manually add L2 devices using the web interface or a CSV file. Assuming that device discovery permission has been provided, L3 devices are discovered automatically using the route information provided by monitored gateways. Once devices are loaded/added in the web interface, user can use the topology scheduler feature to update the configuration of both L2 and L3.

For L2 devices SNMP access type is sufficient with RO community. But for mitigation, MARS requires SNMP RW community access. If SNMP RW community is not possible, select TELNET/SSH access type with SNMP RO Community.

Networks for Dynamic Vulnerability Scanning

With dynamic vulnerability scanning, the MARS probes the networks that you have specified for weaknesses. These automatic scans commence after a rule has fired that indicates an attack is in progress. Once an attack is underway, these scans accomplish the following:

- return information that determines if the attack failed
- return information that determines if the attack likely succeeded
- return false positive information
- assign severity to firing events and incidents

Select a Network for Scanning

To select a network for scanning, follow these steps:

Step 1 Click the **Select** radio button.

Step 2 Click a network to scan.

Step 3 Click **Add**.

Step 4 Repeat Step 1 through Step 3.

Step 5 Click **Submit** when ready.

Create a Network IP Address for Scanning

To create a network address that you can use to define the scan settings, follow these steps:

Step 1 Click the **Network IP** radio button.

Step 2 Enter the Network IP address and Mask.

Step 3 Click **Add**.

Create a Network IP Range for Scanning

To create a range of network addresses that you can use to define the scan settings, follow these steps:

Step 1 Click the **IP Range** radio button.

Step 2 Enter the range of IP addresses.

Step 3 Click **Add**.

Understanding NetFlow Anomaly Detection

NetFlow is a Cisco technology that supports monitoring network traffic and is supported on all basic IOS images. NetFlow uses an UDP-based protocol to periodically report on flows seen by the Cisco IOS device. A *flow* is a Layer 7 concept that consists of a session set up, data transfer, and session teardown. For every flow, a NetFlow-enabled device record several flow parameters including

- Flow identifiers, specifically source and destination addresses, ports, and protocol
- Ingress and egress interfaces
- Packets exchanged
- Number of bytes transferred

Periodically, a collection of flows and its associated parameters are packaged in an UDP packet according to the NetFlow protocol and sent to any identified collection points. Because data about multiple flows is recorded in a single UDP packet, NetFlow is an efficient method of monitoring high volumes of traffic compared to traditional methods, including SYSLOG and SNMP.

The data provided by NetFlow packets is similar to that provided by SYSLOG, SNMP, or Checkpoint LEA as reported by enterprise-level firewalls, such as Cisco PIX, NetScreen ScreenOS, and Checkpoint Firewall-1. The difference being that NetFlow much more efficient. To receive comparable syslog data from a firewall device, the syslog logging level on the firewall must be set to DEBUG, which degrades firewall throughput at moderate to high traffic loads.

If NetFlow-enabled reporting devices are positioned correctly within your network, you can use NetFlow to improve the performance of the MARS Appliance and your network devices, without sacrificing MARS's ability to detect attacks and anomalies. In fact, NetFlow data and firewall traffic logs are treated uniformly as they both represent traffic in the network.

This section contains the following topics:

How MARS Uses NetFlow Data

When MARS is configured to work with NetFlow, you can take advantage of NetFlow's anomaly detection using statistical profiling, which can pinpoint day zero attacks like worm outbreaks. MARS uses NetFlow data to accomplish the following:

- Profile the network usage to determine a usage baseline
- Detect statistically significant anomalous behavior in comparison to the baseline
- Correlate anomalous behavior to attacks and other events reported by network IDS/IPS systems

After being inserted into a network, MARS studies the network usage for a full week, including the weekend, to determine the usage baseline. Once the baseline is determined, MARS switches to detection mode where it looks for statistically significant behavior, such as the current value exceeds the mean by 2 to 3 times the standard deviation.

By default, MARS does not store the NetFlow records in its database because of the high data volume. However, when anomalous behavior is detected, MARS does store the full NetFlow records for the anomalous entity (host or port). These records ensure that the full context of the security incident, such as the infected source and destination port, is available to the administrator. This approach to data collection provides the intelligence required by an administrator without affecting the performance of the MARS Appliance. Storing all NetFlow records consumes unnecessary CPU and disk resources.

Note MARS only supports NetFlow version 5 and version 7.

Guidelines for Configuring NetFlow on Your Network

Ideally NetFlow should be collected from the core and distribution switches in your network. These switches, together with the NetFlow from Internet-facing routers or SYSLOG from firewalls, typically represent the entire network. With this in mind, review the following guidelines before deploying NetFlow in your network:

- MARS normalizes NetFlow and SYSLOG events to prevent duplicate event reporting from the same reporting device.
- Review VLANS in switches and pick several VLANs for which the traffic volume is low. This approach allows you to slowly integrate NetFlow and become comfortable with using it in your environment.
- Be aware of existing CPU utilization on NetFlow capable devices. For more information on understanding how NetFlow affects the performance of routers and network throughput, see the following link:

  http://www.cisco.com/en/US/tech/tk812/technologies_white_paper0900aecd802a0eb9.shtml
- Consider using a sampling of NetFlow data 10:1 100:1 ratio's in highly utilized VLANS.
- Be selective in using NetFlow, you to not need to enable it on all NetFlow-capable devices. In fact, such usage can create duplicate reporting of events, further burdening the MARS Appliance.
- MARS uses NetFlow versions 5 and 7. Ensure that the version of Cisco IOS software or Cisco CatOS running on your reporting devices supports at least one of these NetFlow versions.

Note For releases 4.2.3 and earlier of MARS, you cannot define drop rules for a NetFlow-based event. For these releases, tuning of NetFlow events must be performed on the reporting device.

The taskflow for configuring NetFlow to work with MARS is as follows:

1. Identify the reporting devices on which to enable NetFlow.
2. Enable NetFlow on each identified reporting device and direct the NetFlow data to the MARS Appliance responsible for that network segment.
3. Verify that all reporting devices are defined in the MARS web interface.
4. Enable NetFlow processing in the MARS web interface.
5. Allow MARS to study traffic for a week to develop a usage baseline before it beings to generate incidents based on detected anomalies.

The following tasks provide guidance on the required device configuration:

- Enable Cisco IOS Routers and Switches to Send NetFlow to MARS, page 2-33
- Enable NetFlow Processing in MARS, page 2-35

Enable Cisco IOS Routers and Switches to Send NetFlow to MARS

For more information on NetFlow and configuring the settings in Cisco IOS, refer to:

http://www.cisco.com/en/US/docs/ios/netflow/configuration/guide/12_4/nf_12_4_book.html

Before you configure NetFlow from MARS, you must first configure it on the router or switch.

To enable NetFlow on a Cisco IOS router or switch and to push those events to the MARS Appliance, follow these steps:

Step 1 Log in to the Cisco IOS router or switch with administrator's privileges.

Step 2 Enter the following commands:

Command	Purpose
enable	Turn on enable mode.
configure terminal	Enter global configuration mode. **Note** Commands in this mode are written to the running configuration file as soon as you enter them (using the Enter key/Carriage Return).
ip flow-export destination *<MARS_IP_address>* *<UDP_port>*	Enables the data export to the MARS Appliance on UDP port 2055 (assuming the default port is used). *MARS_IP_address* is the IP address of the MARS Appliance that is responsible for processing the NetFlow events for this reporting device. *UDP_port* is the default UDP port to send NetFlow (the default port is 2055).
ip flow-export source <*syslog_interface_name*>	• Set the source IP for the interface to send the NetFlow. The *syslog_interface_name* value should be the interface attached to the network through which the MARS Appliance is reachable, and it must equal the syslog source interface name.
ip flow-export version <*version_number*>	Identifies which version of NetFlow, 5 or 7, to use when generating events. Cisco recommends using version 5 if supported. *version_number* is either 5 or 7. MARS only supports NetFlow versions 5 and 7.
ip flow-cache timeout active 5	Configures the flow timeout. This timeout value breaks up long-lived flows into 5-minute segments. You can choose any number of minutes between 1 and 60; however, selecting the default of 30 minutes will result in spikes appearing in utilization reports.
ip flow-cache timeout inactive 15	Ensures that those flows that have finished are exported in a timely manner.

Step 3 For each interface in the device, enter the following commands:

Command	Purpose
interface <*interface_name*>	Specifies the interface for which you want to enable NetFlow and it enters the interface configuration mode. *interface_name* is the name of the interface to which the MARS is connected. This command varies based on the device type. For example, **interface** *type slot/port-adapter/port* (Cisco 7500 series routers) **interface** *type slot/port* (Cisco 7200 series routers)
ip route-cache flow	Enables NetFlow for the selected interface.

Step 4 To verify that NetFlow is enabled correctly, enter the following commands:

show ip flow export

show ip cache flow

Step 5 To exit enable mode, enter the following command:

exit

Configuring Cisco CatIOS Switch

Some Cisco Catalyst switches support a different implementation of NetFlow that is performed on the supervisor. With the cache-based forwarding model, which is implemented in the Catalyst 55xx running the Route Switch Module (RSM) and NetFlow Feature Card (NFFC), the RSM processes the first flow and the remaining packets in the flow are forwarded by the Supervisor. This support is also implemented in the early versions of the 65xx with MSFC. The deterministic forwarding model used in the 65xx with MSFC2 do not use NetFlow to determine the forwarding path, the flow cache is only used for statistics as in the current IOS implementations. In all of these configurations, flow exports arrive from both the RSM/MSFC and the Supervisor engines as distinct streams.

The router-side running IOS is configured as specified in Enable Cisco IOS Routers and Switches to Send NetFlow to MARS, page 2-33. However, to configure the he CatIOS NetFlow Data Export, use the following commands:

set mls flow full

set mls nde version 5

set mls nde <*MARS_IP_address***> 2055**

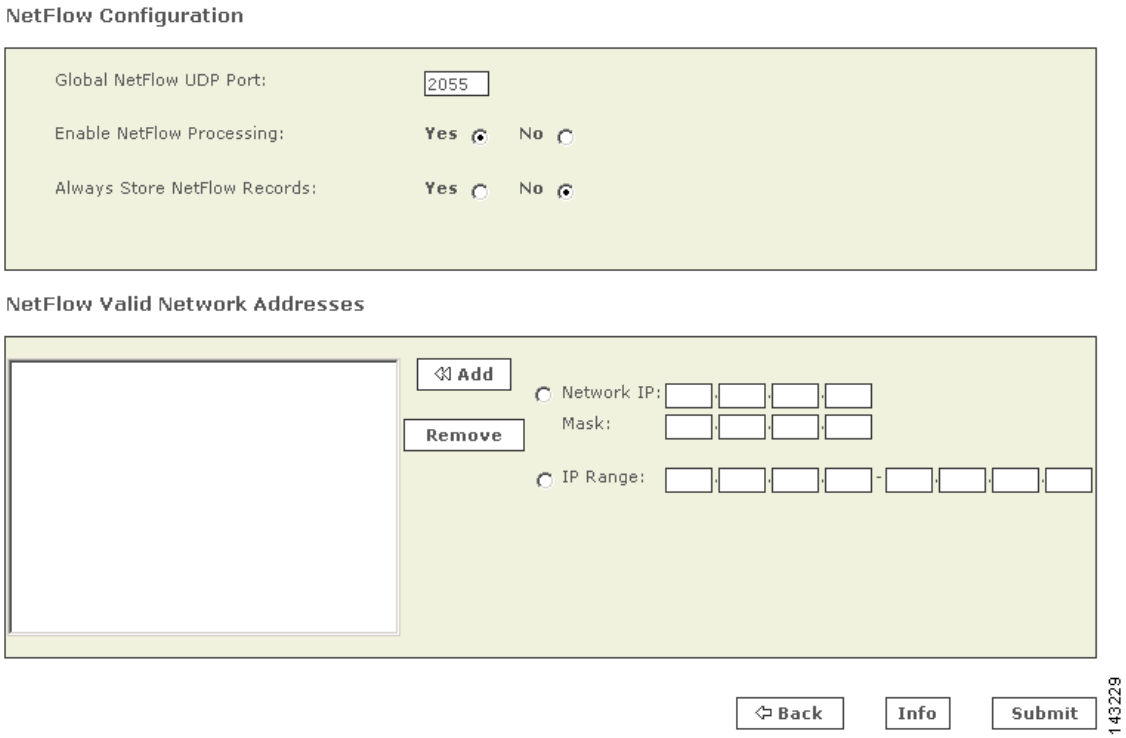
set mls nde enable

From a user's perspective, the switch is only running IOS when the 65xx is running in Native mode.

Enable NetFlow Processing in MARS

Once you have enabled NetFlow on your routers or switches and you have directed those devices to publish NetFlow data to the MARS Appliance, you must configure the appliance to process that data. This configuration involves determining how to store data, as well as identifying which networks you want to process for anomalous behavior. Both of these options can affect the rate at which MARS can process events: storing the full event data rather than summary data burdens the system with writing large volumes of data rather than processing new incoming events. Also, by not specifying a select set of networks, MARS studies all networks.

Step 1 Click **Admin > System Setup > NetFlow Config Info**.



Step 2 Under **NetFlow Configuration**, enter the NetFlow **Global NetFlow UDP Port**. This is the default port for MARS to listen for NetFlow; the default value is 2055.

Note This value must match the value you entered in the "`ip flow-export destination`" command when configuring the router (see Enable Cisco IOS Routers and Switches to Send NetFlow to MARS, page 2-33. Also, verify you have enabled this traffic to flow between the router or switch and the MARS Appliance on any intermediate gateways, such as routers and firewalls.

Step 3 Choose whether to **Enable NetFlow Processing**.

- **Yes** tells MARS to process the NetFlow logs.
- **No** disables the processing of NetFlow data into the MARS.

Step 4 Choose whether to **Always Store NetFlow Records**.

- **Yes** tells MARS to store all of the NetFlow events in the database. Selecting this option can slow down the system by greatly decreasing the number of events per second that MARS is able to process.
- **No** tells MARS to store only anomalies. The MARS detects anomalies by using two dynamically generated watermarks comparing the previous data against current data. When the data breaches the first watermark, MARS starts to save that data. When the data rises above the second watermark, MARS creates an incident.

Step 5 Under **NetFlow Valid Network Addresses**, you can enter one or more for networks you want to monitor and use the **<< Add** button to add them.

- Specifying one or more networks causes MARS to generate NetFlow-based anomalies that occur only on the specified networks. If empty, then entire network is examined for anomalies. If the Local Controller is monitoring a specific zone (as defined by theGlobal Controller-Local Controller relationship), then this field should include only those networks for which this Local Controller is responsible.

Note To reduce the memory usage and increase performance of the appliance, you can configure MARS to profile hosts belonging to a set of valid networks.

- Leaving this value blank (not specifying any networks) causes MARS to examine all networks for anomalous behavior based on the NetFlow events.

Step 6 Click **Submit** to save your changes.

Step 7 To enable NetFlow processing by the MARS Appliance, click **Activate**.

Before MARScan start detecting anomalies based on NetFlow data, it must first develop a baseline for network behavior. It takes a full week, including the weekend, for MARS to develop such a baseline. After this period has elapsed, MARS can start generating incidents based on NetFlow's anomaly detection.

Host and Device Identification and Detail Strategies

MARS studies many events at the network layer, relying on firewalls, routers, and IPS devices to identify anomalies and suspected incidents at a layer above the endpoint hosts that are the source or destination of network sessions. If operating exclusively at this network layer, MARS can generate a number of false positive incidents that must be manually investigated. However, several features exist that allow you to provide host-level details to MARS:

- Enable event reporting from the hosts on your network. MARS can receive, and in some cases, pull event data directly from the hosts on your network. This additional data allows MARS to verify the success of some attacks, as well as to report issues with the operation of the host, such as including them in "device down" reports if they are inaccessible. For more information on configuring the hosts and MARS to pull or receive data from those hosts, see the following topics:
  - Adding Generic Devices, page 11-1
  - Sun Solaris and Linux Hosts, page 11-2
  - Microsoft Windows Hosts, page 11-4
- Manually identify the operating system type and network services running on discovered hosts. For more information, see Define Vulnerability Assessment Information, page 11-12 and Identify Network Services Running on the Host, page 11-14
- Manually identify common hosts and nodes in your network by adding other devices via Management > IP Management. This additional data allows you to identify those hosts that are likely to be involved in network sessions without having to configure the hosts to provide event data directly to MARS. This open allows you to provide vulnerability assessment information to assist in the reduction of false positives. For more information on adding hosts manually, see Add a Host, page 24-5.

Configuring Layer 3 Topology Discovery

For the MARS to reach full operability, you must specify its community strings and select the networks that you want to discover. Once the appliance discovers these networks, you get a more accurate view of MAC addresses, end-point lookup (attack paths), and network topology. Topology discovery enables operation level three, see Levels of Operation, page 2-1 for more information.

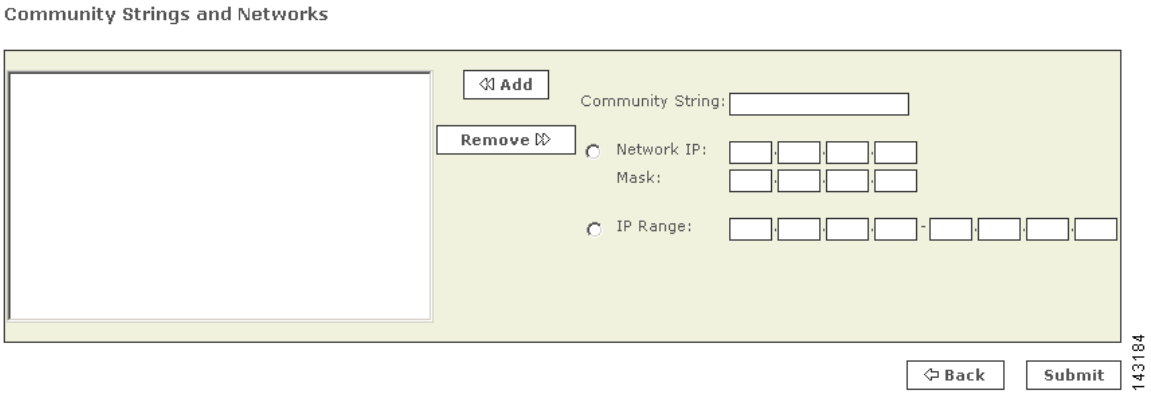
See Figure 18-20 on page 18-12 for a view of the topologies.

Note Remember to activate additions and changes to your community strings and valid networks by clicking **Activate**.

Add a Community String for a Network

To add a community string for a network IP, follow these steps:

Step 1 To open the Community Strings and Networks page, click **Admin > Community Strings and Networks**.



Step 2 Click the **Network IP** radio button.

Step 3 Enter the Community String, Network IP address, and Mask.

Step 4 Click **Add**.

Step 5 Repeat Step 2 through Step 4 for all the community strings that you want to add.

Step 6 Click **Submit** to commit these additions.

Add a Community String for an IP Range

To add a community string for an IP range, follow these steps:

Step 1 To open the Community Strings and Networks page, click **Admin > Community Strings and Networks**.

Step 2 Click the **IP Range** radio button.

Step 3 Enter the Community String and its IP Range.

Step 4 Click **Add**.

Step 5 Repeat Step 2 through Step 4 for all the community strings that you want to add.

Step 6 Click **Submit** to commit these additions.

You can add multiple community strings for the same network by adding similar entries.

Add Valid Networks to Discovery List

Adding valid networks confines the MARS to discover the networks that you want. MARS uses this information to create topologies, find MAC addresses, and for end-point lookup (attack paths).

Note You can only specify networks for the zone where the MARS Appliance operates.

To add valid networks, follow these steps:

Step 1 Click **Admin** > **Valid Networks** to open the Valid Networks page.

Step 2 Enter the **SNMP Target**'s IP address.

The SNMP target is the entry-point where the MARS starts discovering devices on a network. It typically identifies an address on a default gateway of the network.

Step 3 Click either **Network IP** or **Network Range** to define the scope of the scan.

Step 4 Enter the appropriate information.

Step 5 Click **Submit**.

Remove Networks from Discovery List

To remove a network, follow these steps:

Step 1 Click **Admin** > **Valid Networks** to open the Valid Networks page.

Step 2 Click the network that you want to remove.

Step 3 Click **Remove**.

Discover Layer 3 Data On Demand

You can schedule topology discovery, as defined in Scheduling Topology Updates, page 2-40. However, you can also initiate an on-demand discovery.

To perform an on-demand discovery, follow these steps:

Step 1 Click **Admin** > **Valid Networks** to open the Valid Networks page.

Step 2 Verify that the list of Valid Network Addresses contains the networks that you want to discover.

Step 3 Click **Discover Now**.

Scheduling Topology Updates

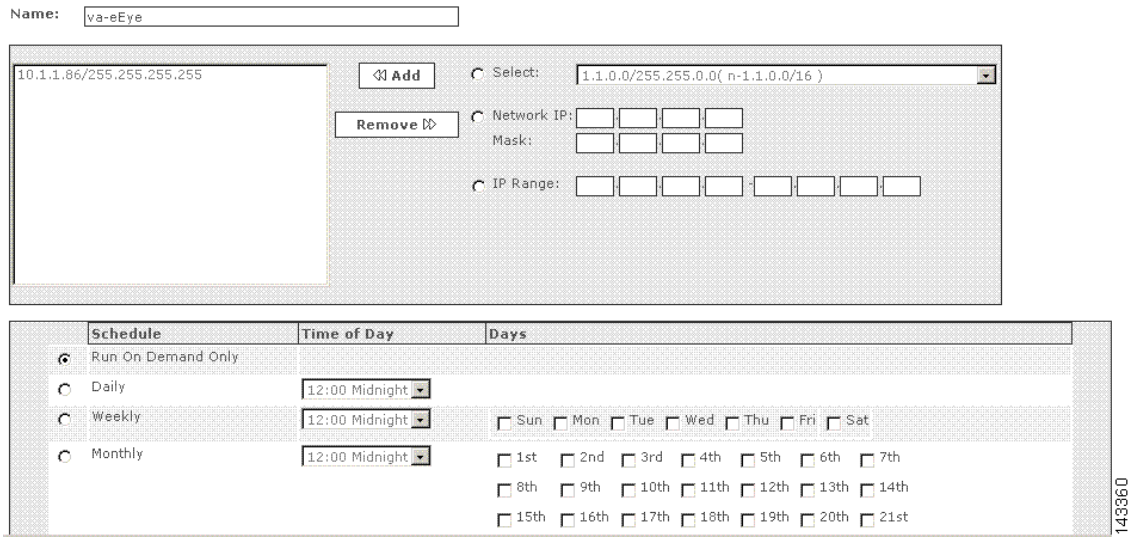
You can configure MARS to run automatic topology updates on devices, networks, and groups of networks. Scheduling topology updates is a critical part of keeping the MARS Appliance abreast of changes in the network and of changes to the configuration settings of the reporting devices and mitigation devices. This operation is similar to clicking Discover when defining a reporting device.

Configuration discovery depends on the device type, proper authorization, an access type, such as Telnet or SSH, and an access IP address. When device discovery is performed, MARS contacts the device and conducts a topology and configuration discovery. This discovery collects all of the route, NAT, and ACL-related information for the device or admin context. In addition, the name of the device may change to `hostname.domain` format if it was not already entered as such. If discovering a device that supports them, MARS also discovers information about modules, admin contexts, and security contexts. Another effect of scheduled updates is that MARS keeps the network diagram and attack paths current in the Dashboard.

This feature also allows you to pull data from those devices that require interval-based polling. The list to devices that require such polling are:

- Qualys QualysGuard
- eEye REM
- FoundStone FoundScan
- Check Point log servers

Figure 2-1 Example Scheduled Update for eEye REM



Schedule a Network Discovery

To add a network for scheduled discovery, follow these steps:

Step 1 Click **Admin > Topology/Monitored Device Update Scheduler**.

The Topology/Monitored Device Update Scheduler page displays.

Step 2 Click **Add**.

Step 3 Enter a name for the network (or group of networks).

Step 4 Select or enter your networks:

- Click the **Select** radio button, and select a network from the list.
- Click the **Network IP** radio button, and enter the IP address and Mask.
- Click the **IP Range** radio button, and enter the IP ranges.

Step 5 Click **Add** to move the network into the selected field.

- To remove an item in the selected field, click it to highlight it, and click **Remove**.

Step 6 In the schedule table, select the appropriate radio button and its time criteria:

- **Run On Demand Only**
- **Daily** and the Time of Day
- **Weekly**, the Time of Day, and the Days
- **Monthly**, the Time of the Day, and the Dates

Step 7 Click **Submit**.

To edit a scheduled topology discovery

Step 1 Check the box next to the Topology Group.

Step 2 Click **Edit**.

Step 3 Click **Add** to move the network into the selected field.

- To remove an item in the selected field, click it to highlight it, and click **Remove**.

Step 4 In the schedule table, select the appropriate radio button and its time criteria:

- **Run On Demand Only**
- **Daily** and the Time of Day
- **Weekly**, the Time of Day, and the Days
- **Monthly**, the Time of the Day, and the Dates

Step 5 Click **Submit**.

To delete a scheduled topology discovery

Step 1 Check the box next to the Topology Group.

Step 2 Click **Delete**.

To run a topology discovery on demand

Note You can run any scheduled or on-demand topology discoveries at any time.

Step 1 Check the box next to the Topology Group.

Step 2 Click **Run Now**.

Configuring Resource Usage Data

While the Monitor Resource Usage box appears on every host and reporting device, only three device types actually provide resource usage data to MARS:

- Cisco IOS routers running 12.2
- Cisco IOS switches running 12.2
- Cisco PIX 6.0, 6.1, 6.2, 6.3, 7.0
- Cisco ASA 7.x
- Cisco FWSM 2.x and 3.x
- Check Point devices (Opsec NG FP3)

For these six devices, MARS can provide data about CPU utilization, memory utilization, and device saturation. For FWSM, MARS monitors system context level resources (CPU, memory, connections) via the CLI and per-context resources (CPU, memory, connections, interface utilization, and errors) via SNMP. Therefore, you can monitor three views of the FWSM module: base platform (IOS switch hosting the module), module level (system context), and security context level.

To enable the collection of resource usage data, you must ensure that the resource usage-specific events are logged by the reporting devices, that the SNMP RO community string is set, that those devices forward the events to MARS, and that the device is defined in the web interface as a reporting device or mitigation device. In addition, you must select **Yes** in the Monitor Resource Usage box of the General tab for each supported reporting device.

Once configured, MARS uses SNMP to poll the device every 5 minutes for the following SNMP OIDs:

- Bytes in/out of every interface on the device (Cisco IOS, Cisco PIX)
- Number of current connections (Cisco PIX, Check Point)
- CPU of last second and last 60 seconds (Cisco IOS, Cisco PIX)
- Memory free/used (Cisco IOS, Cisco PIX)

It also detects anomalous resource utilization if the consumption is significantly higher than the hourly average.

The following resource usage data reports are available:

- Resource Utilization: Bandwidth: Inbound - Top Interfaces
- Resource Utilization: Bandwidth: Outbound - Top Interfaces
- Resource Utilization: CPU - Top Devices
- Resource Utilization: Concurrent Connections - Top Devices
- Resource Utilization: Errors: Inbound - Top Interfaces
- Resource Utilization: Errors: Outbound - Top Interfaces
- Resource Utilization: Memory - Top Devices

You can define custom rules, reports, and queries about resource usage based on the following events:

- CPU Utilization Higher Than 50%
- CPU Utilization Higher Than 75%
- CPU Utilization Higher Than 90%
- CPU Utilization Abnormally High
- Memory Utilization Higher Than 50%
- Memory Utilization Higher Than 75%
- Memory Utilization Higher Than 90%
- Memory Utilization Abnormally High

There is also is pre-defined resource utilization inspection rule:

- System Rule: DoS: Network Device - Success Likely
- System Rule: DoS: Network - Success Likely
- System Rule: Resource Issue: Network Device

Enabling the Required SNMP OIDs for Resource Monitoring

Table 2-5 lists the OIDs to enable, on a per device basis, for the supported model and versions.

Table 2-5 SNMP OIDs Required for Resource Monitoring

Vendor, Model, and Version	OID Descriptor	OID
Cisco IOS 12.2	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.2.1.56.0
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
	DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i
	DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i

Table 2-5 SNMP OIDs Required for Resource Monitoring (continued)

Vendor, Model, and Version	OID Descriptor	OID
Cisco Switch-IOS 12.2	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.2.1.56.0
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
	DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i
	DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i
Cisco PIX 6.0	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
	DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i
	DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i

Table 2-5 SNMP OIDs Required for Resource Monitoring (continued)

Vendor, Model, and Version	OID Descriptor	OID
Cisco PIX 6.1	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
	DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i
	DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i

Table 2-5 SNMP OIDs Required for Resource Monitoring (continued)

Vendor, Model, and Version	OID Descriptor	OID
Cisco PIX 6.2	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.1.3.1
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
	DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i
	DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i

Table 2-5 SNMP OIDs Required for Resource Monitoring (continued)

Vendor, Model, and Version	OID Descriptor	OID
Cisco PIX 6.3	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.1.3.1
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
	DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i
	DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i

Table 2-5 SNMP OIDs Required for Resource Monitoring (continued)

Vendor, Model, and Version	OID Descriptor	OID
Cisco PIX 7.0	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.1.3.1
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
	DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i
	DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i

Table 2-5 SNMP OIDs Required for Resource Monitoring (continued)

Vendor, Model, and Version	OID Descriptor	OID
Cisco FWSM 2.2	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.1.3.1
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
	DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i
	DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i

Table 2-5 SNMP OIDs Required for Resource Monitoring (continued)

Vendor, Model, and Version	OID Descriptor	OID
Cisco FWSM 2.3	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.1.3.1
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
	DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i
	DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i

Table 2-5 SNMP OIDs Required for Resource Monitoring (continued)

Vendor, Model, and Version	OID Descriptor	OID
Cisco FWSM 3.1	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.1.3.1
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
	DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i
	DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i

Table 2-5 SNMP OIDs Required for Resource Monitoring (continued)

Vendor, Model, and Version	OID Descriptor	OID
Cisco ASA 7.0	DEVICE_RES_OID_CPU	.1.3.6.1.4.1.9.9.109.1.1.1.1.3.1
	DEVICE_RES_OID_MEMORY_FREE	.1.3.6.1.4.1.9.9.48.1.1.1.6.1
	DEVICE_RES_OID_MEMORY_USED	.1.3.6.1.4.1.9.9.48.1.1.1.5.1
	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.9.9.147.1.2.2.2.1.5.40.6
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0
	DEVICE_RES_OID_INTERFACE_IN_BYTES	.1.3.6.1.2.1.2.2.1.10.i
	DEVICE_RES_OID_INTERFACE_OUT_BYTES	.1.3.6.1.2.1.2.2.1.16.i
	DEVICE_RES_OID_INTERFACE_IN_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_OUT_BANDWIDTH	.1.3.6.1.2.1.2.2.1.5.i
	DEVICE_RES_OID_INTERFACE_IN_ERROR	.1.3.6.1.2.1.2.2.1.14.i
	DEVICE_RES_OID_INTERFACE_OUT_ERROR	.1.3.6.1.2.1.2.2.1.20.i
	DEVICE_RES_OID_INTERFACE_IN_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.11.i
	DEVICE_RES_OID_INTERFACE_IN_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.12.i
	DEVICE_RES_OID_INTERFACE_OUT_UCAST_PACKET	.1.3.6.1.2.1.2.2.1.17.i
	DEVICE_RES_OID_INTERFACE_OUT_NUCAST_PACKET	.1.3.6.1.2.1.2.2.1.18.i
	DEVICE_RES_OID_INTERFACE_DESCRIPTOR	.1.3.6.1.2.1.2.2.1.2.i
	DEVICE_RES_OID_INTERFACE_IN_DISCARDS	.1.3.6.1.2.1.2.2.1.13.i
	DEVICE_RES_OID_INTERFACE_IN_UNKNOWN_PROTOS	.1.3.6.1.2.1.2.2.1.15.i
	DEVICE_RES_OID_INTERFACE_OUT_DISCARDS	.1.3.6.1.2.1.2.2.1.19.i
CheckPoint OpSec NG FP3	DEVICE_RES_OID_CONNECTION	.1.3.6.1.4.1.2620.1.1.25.3.0
	DEVICE_RES_OID_INTERFACE_NUMBER	.1.3.6.1.2.1.2.1.0

Configuring Network Admission Control Features

Network Admission Control (NAC) is a Cisco Systems sponsored industry initiative that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from viruses and worms.

Using NAC, organizations can provide network access to endpoint devices such as PCs, PDAs, and servers that are verified to be fully compliant with established security policy. NAC can also identify noncompliant devices and deny them access, place them in a quarantined area, or give them restricted access to computing resources.

MARS supports the NAC initiative by storing and reporting about the NAC-based events generated by the various reporting devices on your network. The devices include:.

- Cisco Trust Agent. While CTA does not report to MARS, it does report discovered settings to the Cisco network devices, from which MARS collects events.
- 3rd-party 802.1x Supplicants.
- Cisco IOS routers running Cisco IOS Software, Release 12.3(8)T with security.
- Cisco VPN 3000 Concentrators

- Cisco Secure ACS
- Cisco Security Agent

To enable NAC reporting on your network, you must ensure that the NAC-specific events are logged by the reporting devices, that those devices forward the events to MARS, and that the device is defined in the web interface as a reporting device or mitigation device.

The following reports are available to support NAC:

- Activity: AAA Failed Auth - All Events (Total View)
- Activity: AAA Failed Auth - Top NADs (Total View)
- Activity: AAA Failed Auth - Top Users (Total View)
- Activity: Security Posture: Healthy - Top Users (Total View)
- Activity: Security Posture: NAC - Top NADs (Total View)
- Activity: Security Posture: NAC - Top NADs and Tokens (Total View)
- Activity: Security Posture: NAC - Top Tokens (Total View)
- Activity: Security Posture: NAC Agentless - Top Hosts (Total View)
- Activity: Security Posture: NAC Agentless - Top NADs (Total View)
- Activity: Security Posture: NAC Agentless - Top Tokens (Total View)
- Activity: Security Posture: NAC Audit Server Issues - All Events (Total View)
- Activity: Security Posture: NAC End Host Details - All Events (Total View)
- Activity: Security Posture: NAC Infected/Quarantine - All Events (Total View)
- Activity: Security Posture: NAC Infected/Quarantine - Top Hosts (Total View)
- Activity: Security Posture: NAC L2 802.1x - Top Tokens (Total View)
- Activity: Security Posture: NAC L2IP - Top Tokens (Total View)
- Activity: Security Posture: NAC Static Auth - Top Hosts (Total View)
- Activity: Security Posture: NAC Static Auth - Top NADs (Total View)
- Activity: Security Posture: NAC Static Query Failure - Top Hosts (Total View)
- Activity: Security Posture: Not Healthy - All Events (Total View)
- Activity: Vulnerable Host Found (Total View)
- Activity: Vulnerable Host Found via VA Scanner (Total View)

The following system rules are available to support NAC:

- System Rule: Security Posture: Audit Server Issue - Network Wide
- System Rule: Security Posture: Audit Server Issue - Single Host
- System Rule: Security Posture: Excessive NAC Status Query Failures - Network Wide
- System Rule: Security Posture: Excessive NAC Status Query Failures - Single Host
- System Rule: Security Posture: Excessive NAC Status Query Failures - Single NAD
- System Rule: Security Posture: Infected - Network Wide
- System Rule: Security Posture: Infected - Single Host
- System Rule: Security Posture: Quarantine - Network Wide
- System Rule: Security Posture: Quarantine - Single Host

- System Rule: Security Posture: Vulnerable Host Found

For information on configuring reporting devices and mitigation devices with NAC support, see Enable NAC-specific Messages, page 4-4.

Integrating MARS with 3rd-Party Applications

MARS provides multiple integration methods with 3rd-party applications. The following topics describe how to integrate using these methods:

Forwarding Alert Data to 3rd-Party Syslog and SNMP Servers

You can forward alert data from MARS to third-party syslog and SNMP servers. The data is forwarded on a per rule basis. In other words, you must configure those rules for which you want to forward alert data to include either SNMP, syslog, or both as a notification methods. When a rule fires, the notifications will be sent in the selected formats to the specified recipients, which should be the desired servers in the case of SNMP and syslog.

For more information on configuring notification methods for a rule, see Setting Alerts, page 22-23. To learn more about the SNMP MIB format sent by MARS, see MARS MIB Format, page 2-58.

Syslog Relay Support

In 4.3.1/5.3.1, MARS can act as a relay for the syslog messages received from reporting devices to a single collector.

- A *reporting device* is a source host that generates a syslog message and sends that message to a Local Controller.
- A *relay* is a Local Controller that receives a syslog message from a reporting device and forwards it to a collector.
- A *collector* is a host that receives a syslog message, but the collector does not relay it to another host.

Note This feature is not supported on Global Controller models.

The Local Controller can now act as a relay; it processes the incoming syslog messages locally before it forwards them to the designated collector. The destination port number is 514 for incoming and relayed syslog messages. MARS adheres to *RFC 3164: The BSD syslog Protocol* while relaying the syslog messages with the following exceptions:

- MARS can only forward to a single collector IP address
- Because MARS supports exactly one collector, you cannot specify that events originating from one device address be forwarded to one collector while those originating from a different device address are forwarded to a different collector. All events are forwarded to the same collector.

- Forwarded syslog can be up to 1024 bytes in length. Logs longer than 1024 bytes are truncated.

Tip Using this feature, you can *daisy chain* Local Controllers. Configure the first Local Controller to forward to the second. In the web interface of the second Local Controller, identify the first Local Controller as **Generic Syslog Relay Any** in the Security and Monitoring Devices list. This configuration mirrors the data on both appliances.

The Local Controller generates internal events for the dropped packets, and it does not relay internal system and operating system event logs. Dropped packets result when one of the following condition exist:

- the forward queue is full
- a reporting device is down
- the collector is down.

You configure the syslog relay feature using the MARS CLI interface; no web interface exists to configure these settings. The configuration process is summarized as follows:

1. Access the MARS console.
2. Define the collector.
3. Define the list of devices for which events should be forward.
4. If you chose to select the ANY option, define the list of devices you want to exclude.

Note Syslog forwarding is disabled until you specify the collector and at least one source host.

To configure and use this feature, see the following topics:

- Enable the Syslog Relay Feature, page 2-56
- Disable the Syslog Relay Feature, page 2-57
- MARS Events, System Rule, and Report Details for the Syslog Relay Feature, page 2-57
- Troubleshooting the Syslog Forwarding Feature, page 2-57

For more information on using this feature, see the following commands:

- syslogrelay setcollector
- syslogrelay src
- syslogrelay list

Enable the Syslog Relay Feature

To enable the relay forward, follow these steps:

Step 1 Log in to the Local Controller that will act as the relay. For more information, see Log In to the Appliance via the Console.

Step 2 At the [pnadmin]$ prompt, enter **syslogrelay setcollector** *ip_address*, where *ip_address* is the IP address value for the host to which you want to forward the syslog messages that this MARS Appliance receives from reporting devices.

Result: The the [pnadmin]$ prompt returns. To verify the address, enter **syslogrelay list collector**.

Step 3 At the [pnadmin]$ prompt, enter one of the following commands:

- **syslogrelay src include** *ip_address*, where *ip_address* is one or more IP addresses that represent the reporting devices for which syslog messages should be forwarded to the collector.
- **syslogrelay src include ANY** to specify that MARS should forward the syslog messages for all reporting devices that do not appear in the exclude list.

  If you use ANY, then you may define an exclude list using **syslogrelay src exclude** *ip_address*, where *ip_address* is one or more IP addresses that represent the reporting devices for which syslog messages should not be forwarded.

Step 4 To verify your settings, enter **syslogrelay list all**.

Disable the Syslog Relay Feature

You can disable the syslog relay feature using either of two approaches:

- Clear the list of syslog relay sources
- Clear the syslog collector address

To disable the relay forward feature, follow these steps:

Step 1 Log in to the Local Controller acting as the relay. For more information, see Log In to the Appliance via the Console.

Step 2 At the [pnadmin]$ prompt, enter one of the following commands:

- **syslogrelay src reset**

  This the list of syslog relay sources so that messages are forwarded.
- **syslogrelay unsetcollector** *ip_address*, where *ip_address* is the IP address value for the collector to which syslog messages are currently forwarded.

Step 3 To verify your settings, enter **syslogrelay list all**.

MARS Events, System Rule, and Report Details for the Syslog Relay Feature

Two internal events are defined in the Info/HighUsage/CS-MARS event group in support or this feature:

- MARS-2-100026: MARS Dropped Syslog Relay Event Since Capacity is Reached - First Event in the Hour
- MARS-2-100027: MARS Dropped Syslog to be Relayed Event Since Capacity is Reached - Drop Count in the Hour

The System Rule: Resource Issue: CS-MARS rule includes the MARS-2-100026 event. The Resource Issues: CS-MARS - All Events system report, which includes the Info/HighUsage/CS-MARS event group, summarizes data for the new event types.

Troubleshooting the Syslog Forwarding Feature

The following techniques can assist you in troubleshooting the syslog forwarding feature:

- If incoming syslog messages that should be forwarded are not being forwarded, verify the pnparser service is running on the Local Controller.
- If pnparser is having problems, you can use the **pnstop** and then **pnstart** command to restart the processes.

```
[pnadmin]$ pnstatus
    Module                      State               Uptime
    …
    pnesloader                  RUNNING           3-16:18:29
    pnmac                       RUNNING           3-16:18:29
    pnparser                    RUNNING           3-16:18:23
    process_event_srv           RUNNING           3-16:18:28
    process_inlinerep_srv       RUNNING           3-16:18:28
    process_postfire_srv        RUNNING           3-16:18:28
    process_query_srv           RUNNING           3-16:18:29
    superV                      RUNNING           3-16:18:30
```

- At least one source and one destination must be configured to enable syslog forwarding. Use the **syslogrelay list** command to verify the configuration.
- Source devices must send syslog message to destination port 514 on the Local Controller. Use the **tcpdump** command on the Local Controller to verify the configuration:

  ```
  [pnadmin]$ tcpdump src host 192.168.3.2 and dst host 192.168.3.4 and udp dst port 514
  ```

  where 192.168.3.4 is the IP address of the Local Controller and 192.168.3.2 is configured as a syslog source.
- MARS forwards syslog message to destination port 514 only. Use **tcpdump** command on the syslog collector (192.168.1.1) to verify the configuration

  ```
  tcpdump src host 192.168.3.4 and dst host 192.168.1.1 and udp dst port 514
  ```

  where 192.168.3.4 is the Local Controller and 192.168.1.1 is configured as the syslog collector.

MARS MIB Format

The MARS management information base (MIB) is defined for all MARS releases. The SNMP notification contains the same content as the syslog generated by MARS.

The MARS MIB definition is as follows:

enterprises.16686.1.0 string “MARS-1-101”
enterprises.16686.2.0 string “<alert_content>”
enterprises.16686.3.0 string "<optional_port_list_for_sudden_traffic_increase_incident>"

The MARS private enterprise number is 16686 and <alert_content> is defined as follows:

```
<<priorityInfo>> <current_time> %MARS-1-101: Rule <ruleid> (<rulename>) fired and caused
<color> Incident <incidentId>, starting from <starttime> to <endtime>.
```

In the following two examples of the SNMP notification output, 10.1.1.1 is the IP address of the MARS Appliance:

```
SNMPv2-SMI::enterprises.16686 10.1.1.1 SNMPv2-SMI::enterprises.16686.1.0 "MARS-1-101"
SNMPv2-SMI::enterprises.16686.2.0 "<34>Mon Apr 28 20:11:43 2003 %MARS-1-101: Rule 45513
(Nimda Attack) fired and caused red Incident 12265001, starting from Mon Apr 28 19:58:47
2003 to Mon Apr 28 20:11:21 2003"

SNMPv2-SMI::enterprises.16686 10.1.1.1 SNMPv2-SMI::enterprises.16686.1.0 "MARS-1-101"
```

```
SNMPv2-SMI::enterprises.16686.2.0 "<34>Wed Mar 14 12:28:24 2007 %MARS-1-101: Rule 489722
(System Rule: Sudden Traffic Increase To Port) fired and caused red Incident 204368256,
starting from Wed Mar 14 12:28:14 2007 to Wed Mar 14 12:28:14 2007"
SNMPv2-SMI::enterprises.16686.3.0 "sudden traffic increase to ports: 445 "
```

Note Notifications are sent only from the Local Controller.

Relaying Syslog Messages from 3rd-Party Syslog Servers

You can rapidly deploy MARS by forwarding messages from existing syslog-ng or Kiwi syslog servers. This feature eliminates the network and device changes required to insert MARS into an operational network. You are no longer required to configure each network device to publish its syslog messages directly to MARS, which saves time, avoids device change approval processes, preserves packet processing performance of the network devices, and ensures daily network operations proceed without interruption. This relay feature also allows the correlation and inspection of syslog messages from reporting devices, such as those on the DMZ, for which corporate policies might prohibit the existence of or connection to configuration information.

If your network devices already publish syslog messages to syslog-ng or Kiwi syslog servers, you can configure those servers to forward messages to the MARS Appliance and identify the syslog servers in MARS. Currently, MARS parses the syslog messages generated by the following devices: Cisco PIX, Cisco IOS, Cisco CatOS, Cisco ICS, Cisco ASA, Cisco FWSM, Cisco VPN 3000, Cisco Secure ACS, Snort IDS, Juniper/Netscreen firewalls, Solaris, Linux, and Microsoft Internet Information Server (ISS), Microsoft Windows running the SNARE agent. For other devices, you can define custom log parsers.

The MARS Appliance can begin processing and storing the events while you define the reporting devices using the MARS user interface. You are still required to define the reporting device by IP address and device type in MARS to ensure proper event correlation; however, you are not required to configure device to publish syslog messages directly to MARS.

To configure MARS to work with a syslog relay server, perform the following tasks:

1. Configure the syslog relay server to forward correctly formatted messages to MARS. See Configure Syslog-ng Server to Forward Events to MARS, page 2-59 or Configure Kiwi Syslog Server to Forward Events to MARS, page 2-60.
2. Identify the MARS Appliance as a forward target.
3. Add the syslog relay server to the MARS user interface. See Add Syslog Relay Server to MARS, page 2-61.
4. Add the reporting devices monitored by the syslog relay server to the MARS user interface. See Add Devices Monitored by Syslog Relay Server, page 2-62.

Configure Syslog-ng Server to Forward Events to MARS

We recommend the following settings in the configuration options of the syslog-ng.conf file to ensure good integration of syslog-ng with MARS:

options { long_hostnames(off); use_dns(0); keep_hostname(yes); };

where

- The long_hostnames(off) setting conforms to RFC 3164, which recommends that the HOSTNAME does not contain domain name.

- The use_dns(0) setting ensures that the IP address is used in HOSTNAME rather than the hostnames.
- The keep_hostname(yes) setting preserves the original sending device's HOSTNAME even when it is relayed more than once.

In addition to configuring the message format, you must specify that the MARS Appliance is a destination loghost on UDP port 514. The following lines must appear in the syslog-ng.conf file:

```
destination loghost { udp("IP address of MARS Appliance" port(514)); };
log { source(src); destination(loghost); };
log { source(net); destination(loghost); };
```

Configure Kiwi Syslog Server to Forward Events to MARS

We recommend the following settings in the configuration options of the Kiwi Syslog Daemon to ensure good integration of Kiwi with MARS:

Step 1 Expand the **File > Setup > Rules > Actions tree.**

Step 2 Right on **Actions** and click **Add an Action**.

Step 3 Enter a name for the action, such as "Forward to pncop".

Step 4 For the following fields, enter the following values:

- **Destination IP address or hostname** — Enter the IP address of the MARS Appliance.
- **Protocol** — UDP
- **New Facility** — No Change
- **New Level** — No Change
- **Port** — 514
- **Send with RFC 3164 header information** — Selected if the syslog server receives syslog messages directly from the source devices only. Clear if the syslog server also receives syslog messages from relays. Do not configure mixed relays.

  This additional header is necessary for the supported device types that do *not* have HOSTNAME in the syslog messages; thereby allowing MARS to correctly identify the original sending device. However, this option cannot be used on a Kiwi relay of relay. To support a Kiwi relay of relay in MARS, the first relay must have this option selected and must receive syslog messages only from the source devices, and all other relays must have this option cleared and must only receive syslog messages from other Kiwi relays, not directly from devices.
- **Retain the original source address of the message** — Cleared.

Step 5 If you are using SNARE agents, click **Setup > Modifiers** and clear "Replace non printable characters with <ASCII value>"

If this value is selected, tabs appear as `<009>` in the Windows event logs, which prevents MARS from parsing the events correctly.

Step 6 Save your changes.

Add Syslog Relay Server to MARS

In addition to representing each of the potential reporting devices, you must define the syslog relay server so that MARS knows for which messages it should attempt to discover the true reporting device. To add a syslog relay server, you must add it as a security software application running on a host.

To add a syslog relay server, follow these steps:

Step 1 Select **Admin > System Setup > Security and Monitor Devices > Add**.

Step 2 Do one of the following:

- Select **Add SW Security apps on a new host** from the Device Type list, and continue with Step 3
- Select **Add SW security apps on existing host** from the Device Type list. Select the device to which you want to add the software application and click Add. Continue with Step 6.

Step 3 Specify values for the following fields:

- **Device Name** — Enter the hostname of the syslog relay server. MARS maps this name to the reporting IP address. This name is used in topology maps, queries, and as the primary management station in the Security and Monitoring Device list.
- **Reporting IP** — Enter the IP address of the interface in the syslog relay server from which MARS will receive syslog messages.

  This address represents the physical IP address of the syslog relay server. To learn more about the reporting IP address, its role, and dependencies, see Understanding Access IP, Reporting IP, and Interface Settings, page 2-8.

Step 4 Under Enter interface information, enter the interface name, IP address, and netmask value of the interface in the syslog relay server from which syslog messages will be received.

This address represents the physical IP address of the syslog relay server. To learn more about the interface settings, its role, and dependencies, see Understanding Access IP, Reporting IP, and Interface Settings, page 2-8.

Step 5 Click **Apply** to save these settings.

Step 6 Click **Next** to access the Reporting Applications tab.

Step 7 Select **Generic Syslog Relay ANY** from the Select Application list, and click **Add**.

Step 8 Click **Submit** to add this application to the host.

Result: Generic Syslog Relay ANY appears in the Device Type list.

Step 9 Click the **Vulnerability Assessment Info** link to define the host information that MARS uses to determine false positive attacks against this host. Continue with Define Vulnerability Assessment Information, page 11-12.

Step 10 Click **Done** to save the changes.

Result: The host appears in the Security and Monitoring Information list.

Step 11 To activate the device, click **Activate**.

Add Devices Monitored by Syslog Relay Server

While you do not have to configure each reporting device to forward syslog messages to the MARS Appliance, you must define the device to MARS so that when it parses the syslog messages forwarded by the relay server, then it is able to match the true reporting IP address to that of a known reporting device type. By knowing the reporting device type, MARS can correctly parse the events.

The process for adding these reporting devices is the same as if there were no syslog relay server except that you do not configure the reporting device to forward events to the MARS Appliance. In the MARS web interface, you should still configure the reporting devices so that MARS can discover their settings and to perform any mitigation operations.