Configuring the Security Appliance for Use with MARS

MARS centrally aggregates logs and events from various network devices, including security appliances, which you can analyze for use in threat mitigation. MARS supports the following PIX and ASA adaptive security appliance versions: 7.0(7), 7.2(2), 7.2(3), and 8.0(2).

This appendix describes how to configure the security appliance and add it to MARS as a reporting device, and includes the following sections:

For more information about configuring devices and software to work with MARS, see the *Supported and Interoperable Devices and Software for Cisco Security MARS Local Controller* document and the *User Guide for Cisco Security MARS Local Controller*.

Taskflow for Configuring MARS to Monitor Security Appliances

The taskflow for configuring MARS to monitor the security appliance includes the following steps:

1. Configure the security appliance to accept administrative sessions from MARS to discover settings. Configure this setting in the admin context.

2. Configure the security appliance to publish its system log messages to MARS. Configure this setting for the admin context and for each security context defined.

> **Note** Each context requires a unique, routable IP address for sending system log messages to MARS, and each context must have a unique name (usually in the *hostname.domain* name format).

3. To enable MARS to accept system log message event data and to collect configuration settings from the security appliance, perform the following tasks:

    – Enable logging for one or more interfaces.

- Select the logging facility and queue size.
- Specify the logging severity level as debugging (7) or indicate the desired severity level.
- Identify the target MARS appliance, and the protocol and port pair on which it listens.

4. Within the MARS web interface, perform the following steps:

- Define the security appliance by providing the administrative connection information.
- Define security contexts. For more information, see Adding Security Contexts, page E-4.
- Add discovered contexts. For more information, see Adding Discovered Contexts, page E-4.
- Edit discovered contexts. For more information, see Editing Discovered Contexts, page E-5.

Enabling Administrative Access to MARS on the Security Appliance

To enable administrative access to MARS on the security appliance, perform the following steps:

Step 1   To enable the MARS appliance to discover the security appliance settings through SSH access, enter the following commands:

```
hostname# crypto key generate rsa modulus modulus
```

where *modulus* is the RSA modulus size specified in bits

```
hostname# ssh mars_ip netmask of the mars_ip interface name
```

where *mars_ip* is the IP address of the MARS appliance, *netmask of the mars_ip* is the netmask of the MARS appliance, and *interface name* can be inside, outside, or DMZ.

Step 2   To enable the MARS appliance to discover the security appliance settings through Telnet access, enter the following command:

```
hostname# telnet mars_ip netmask of the mars_ip interface name
```

where *mars_ip* is the IP address of the MARS appliance, *netmask of the mars_ip* is the netmask of the MARS appliance, and *interface name* can be inside, outside, or DMZ.

Step 3   To enable the MARS appliance to discover the security appliance settings through FTP access, make sure that you have added the MARS appliance configuration file to an FTP server.

> **Note**   If you choose the FTP access type, the MARS appliance cannot discover the non-admin context settings. Therefore, we do not recommend this access type.

Step 4   To enable MARS to act as a target logging host, configure the security appliance to publish system log messages to MARS by entering the following commands:

```
hostname# logging host interface name mars_ip
```

where *mars_ip* is the IP address of the MARS appliance and *interface name* can be inside, outside, or DMZ.

```
hostname# logging trap 7
```

```
hostname# logging enable
```

> ✏️
>
> **Note**   Make sure that you set the logging severity level to 7 (debugging), or configure the security
> appliance to generate the desired set of system log messages. The logging severity level
> generates the system log message details that are required to track session-specific data.
>
> Debugging messages are recommended for troubleshooting. The debugging logging severity
> level includes all emergency, alert, critical, error, warning, notification, and informational
> messages. This logging severity level also generates logs that identify the commands that are
> issued during FTP sessions and the URLs that are requested during HTTP sessions. If the
> security appliance cannot sustain debugging-level messages because of performance
> considerations, use the informational logging severity level (6). For more information, see
> Setting the Logging Severity Level for System Log Messages, page E-5.
>
> **In addition, do not** use the EMBLEM format for system log messages.

Step 5   To allow MARS to discover CPU usage and related information, enable the SNMP RO community string
for the security appliance by entering the following command:

```
hostname# snmp-server host interface mars_ip poll community community
```

where *interface* can be inside, outside, or DMZ, *mars_ip* is the IP address of the MARS appliance, and
community is the SNMP RO community string.

Step 6   Repeat Step 4 for each admin context and security context defined.

Adding a Security Appliance to Monitor

Events that are published by a reporting device (the security appliance) to MARS are not inspected until
the reporting IP address of the security appliance is defined in the MARS web interface.

To add a PIX or ASA adaptive security appliance to monitor, perform the following steps:

Step 1   In the MARS web interface, click **Admin > System Setup > Security and Monitor Devices > Add**.

Step 2   Choose the correct version of the ASA adaptive security appliance from the Device Type drop-down list.
The basic device type represents the admin context.

Step 3   Specify values for the following Device Access fields:

> 🔍
>
> **Tip**   To enable SSH discovery, the MARS appliance must authenticate to the security appliance. The
> default username is "pix" and the password is the one that you specified for the **password**
> command (unless you use AAA).

- Device Name, which MARS maps to the reporting IP address
- Access IP, which is usually the same as the reporting IP address
- Reporting IP, which is the interface that publishes system log messages or SNMP notifications, or
  both
- Access Type
- Login

- Password

- Enable Password

- (Optional) SNMP RO, which allows MARS to retrieve MIBs that are related to CPU usage and network usage

- (Optional) Monitor Resource Usage (requires the SNMP RO setting), which allows MARS to monitor for anomalous consumption of resources, such as memory and CPU

Step 4   Click **Discover** to determine the security appliance settings, including any security contexts and their settings.

Step 5   Click **Submit** to save these settings in the MARS database.

Step 6   Click **Activate to load these settings into the MARS appliance working memory**.

Step 7   Click **Summary > Dashboard**.

Step 8   Under the Hotspot Graph, click **Full Topology Graph**, and verify that the selected security appliance appears.

Adding Security Contexts

To add security contexts, perform the following steps:

Step 1   In the MARS web interface, click **Add Module**.

Step 2   Choose the correct version of the security appliance from the Device Type drop-down list.

Step 3   Enter the name of the security appliance in the Device Name field.

Step 4   Enter the name of the security context in the Context Name field. This name must match the context name defined on the security appliance.

Step 5   Enter the IP address of the security context from which system log messages or SNMP notifications, or both are published in the Reporting IP field.

Step 6   (Optional) Enter the security appliance read-only community string in the SNMP RO Community field.

Step 7   Click **Discover** to discover the settings of the defined security context. MARS collects all route, NAT, and ACL-related information.

Step 8   Click **Submit** to save these settings in the MARS database.

Adding Discovered Contexts

To add discovered contexts, perform the following steps:

Step 1   In the MARS web interface, click **Add Available Module**.

Step 2   Choose the security context from the Select drop-down list, and click **Add**.

Step 3   Click **Submit** to save these settings in the MARS database.

Step 4   Repeat these steps for each discovered context.

Editing Discovered Contexts

To edit discovered contexts, perform the following steps:

Step 1 In the MARS web interface, choose the discovered context that you want to edit according to the selected device type.

Step 2 Click **Edit Module**.

Step 3 Enter the IP address from which the system log messages of the security context are sent in the Reporting IP field.

Step 4 (Optional) Enter the security appliance read-only community string in the SNMP RO Community field.

Step 5 (Optional) To enable MARS to monitor this context for anomalous resource usage, click **Yes** from the Monitor Resource Usage list.

Step 6 Click **Submit** to save these settings in the MARS database.

Step 7 Repeat these steps for each discovered context.

Setting the Logging Severity Level for System Log Messages

You can change the logging severity level of the required system log messages or turn off specific system log messages using the **logging message** command. For more information, see Chapter 44, "Monitoring the Security Appliance."

System Log Messages That Are Processed by MARS

MARS can correctly parse system log messages at customized logging severity levels. Therefore, you can set system log messages to a lower logging severity level (for example, logging severity level 6). By changing the logging severity level for system log messages, you can reduce the logging load on the security appliance by 5-15%. However, the primary consumer of resources are the session detail events.

MARS processes the following system log messages, which are required for correct sessionization. If you change the logging severity level of the security appliance, make sure that these system log messages are generated at the new logging severity level so that the MARS appliance can receive them.

Table E-1 lists the system log message classes, their definitions, and the ranges of system log message numbers that are processed by MARS.

Table E-1 System Log Message Classes and Associated Message Numbers

Class	Definition	System Log Message Numbers
auth	User Authentication	109001-109003, 109005-109008, 109010-109014, 109016-109034, 113001, 113003-113020, 114001-114020, 611101-611104, 611301-611323
bridge	Transparent Firewall	110001
ca	PKI Certification Authority	717001-717019, 717021-717038

Table E-1   System Log Message Classes and Associated Message Numbers (continued)

Class (continued)	Definition	System Log Message Numbers
config	Command Interface	111001, 111003-111005, 111007-111009, 111111, 112001, 208005, 308001-308002, 504001-504002, 505001-505013, 506001
e-mail	E-mail Proxy	719001-719026
ha	High Availability (Failover)	101001-101005, 102001, 103001-103005, 104001-104004, 105001-105011, 105020-105021, 105031-105032, 105034-105040, 105042-105048, 210001-210003, 210005-210008, 210010, 210020-210022, 311001-311004, 709001-709007
ip	IP Stack	209003-209005, 215001, 313001, 313003-313005, 313008, 317001-317005, 322001-322004, 323001-323006, 324000-324007, 324300-324301, 325001-325003, 326001-326002, 326004-326017, 326019-326028, 327001-327003, 328001, 329001, 331001-331002, 332003-332004, 333001-333010, 334001-334008, 335001-335014, 408001-408003, 410001-410004, 411001-411004, 412001-412002, 413001-413004, 416001, 417001, 417004, 417006, 417008-417009, 418001, 419001-419002, 421001-421007, 422004-422006, 423001-423005, 424001-424002, 431001-431002, 450001, 507001-507002, 508001-508002, 509001
ips	Intrusion Protection Service	400000-400050, 401001-401005, 415001-415020, 420001-420003
np	Network Processor	319001-319004
npssl	NP SSL	725001-725014
ospf	OSPF Routing	318001-318009, 409001-409013, 409023, 503001, 613001-613003
rip	RIP Routing	107001-107003, 312001
rm	Resource Manager	321001-321004
session	User Session	106001-106002, 106006-106007, 106010-106027, 106100-106101, 108002-108003, 108005, 201002-201006, 201008-201013, 202001, 201005, 202011, 204001, 302001, 302003-302004, 302007-302010, 302012-302023, 302302, 303002-303005, 304001-304009, 305005-305012, 314001, 405001-405002, 405101-405107, 405201, 405300-405301, 406001-406002, 407001-407003, 500001-500004, 502101-502103, 502111-502112, 607001-607002, 608001-608005, 609001-609002, 616001, 617001-617004, 620001-620002, 621001-621003, 621006-621010, 622001, 622101-622102, 703001-703002, 710001-710006, 726001
snmp	SNMP	212001-212006

Table E-1   System Log Message Classes and Associated Message Numbers (continued)

Class (continued)	Definition	System Log Message Numbers
sys	System	199001-199003, 199005-199009, 211001, 211003, 216003, 217001, 218001-218004, 219002, 315004, 315011, 414001-414002, 604101-604104, 605004-605005, 606001-606004, 610001-610002, 610101, 612001-612003, 614001-614002, 615001-615002, 701001-701002, 711001-711002
vpdn	PPTP and L2TP Sessions	213001-213004, 403101-403104, 403106-403110, 403500-403507, 603101-603109
vpn	IKE and IPSec	316001, 320001, 402101-402103, 402106, 402114-402120, 402123, 404101-404102, 501101, 602101-602104, 602201-602203, 602301-602304, 702201-702212, 702301-702303, 702305, 702307, 713004, 713006, 713008-713010, 713012, 713014, 713016-713018, 713020, 713022, 713024-713037, 713039-713043, 713047-713052, 713056, 713059-713063, 713065-713066, 713068, 713072-713076, 713078, 713081-713086, 713088, 713092, 713094, 713098-713099, 713102-713105, 713107, 713109, 713112-713124, 713127-713149, 713152, 713154-713172, 713174, 713176-713179, 713182, 713184-713187, 713189-713190, 713193-713199, 713203-713206, 713208-713226, 713228-713251, 713900-713906, 714001-714007, 714011, 715001, 715004-715009, 715013, 715019-715022, 715027-715028, 715033-715042, 715044-715072, 715074-715079
vpnc	VPN Client	611101-611104, 611301-611323, 722001-722038
vpnfo	VPN Failover	720001-720073
vpnlb	VPN Load Balancing	718001-718081, 718084-718088
webvpn	Web-based VPN	716001-716056, 723001-723014, 724001-724002

Configuring Specific Features

You can configure security appliances to act as reporting devices and manual mitigation devices, because they perform multiple roles on your network. MARS can benefit from configuration of the following features:

- The built-in IDS and IPS signature matching features can be critical in detecting an attempted attack.

- The logging of accepted, as well as denied sessions, aids in false positive analysis.

- Administrative access ensures that MARS can obtain critical data, including the following:

  - *Route and ARP tables*, which aid in network discovery and MAC address mapping.

  - *NAT and PAT translation tables*, which aid in address resolution and attack path analysis, and expose the actual instigator of attacks.

  - *OS settings*, from which MARS determines the correct ACLs to block detected attacks, which you can use in a management session with the security appliance.