



CHAPTER 2

Deployment Planning Guidelines

Revised: May 9, 2007, OL-13543-01

This chapter presents information to assist you in deploying one or more MARS Appliances. It contains the following sections:

- [MARS Components, page 2-1](#)
- [Supporting Devices, page 2-1](#)
- [Required Traffic Flows, page 2-2](#)

MARS Components

When planning a deployment, you must consider the ability of a MARS Appliance to process the traffic expected from reporting devices on your network. Which models you purchase and where you place them on your network depends on the anticipated, sustained events per second (EPS) and NetFlow flows per second (FPS) predicted for that network or segment.

For details on the supported EPS and FPS rates per model, see the [Cisco Security Monitoring, Analysis and Response System: Data Sheet](#). This datasheet also provides detailed technical specifications on the each appliance model, such as form factor, power consumption requirements, and disk type.

Supporting Devices

Supporting devices are network devices or hosts that provide network services used by MARS. The supporting devices, both optional and required, are listed in [Table 2-1](#) to help you plan your deployment.

Table 2-1 Supporting Devices and Their Role

| Supporting Device Type | Is It Required? | Comment |
|-------------------------|--|---|
| E-mail Server | Yes | MARS uses e-mail servers to deliver administrative reports and notifications. |
| NTP Server | Not for single device deployment. Yes for any scenario involving a Global Controller. | You must specify the timezone and UTC settings on all appliances. The timestamps applied to received messages is critical to accurate incident correlation. |
| DNS Server | Yes | MARS uses DNS to resolve the hostnames for monitored devices, which improves the readability of reports and queries. |
| Internal Upgrade Server | No | For more information on configuring and using such a server, see Checklist for Upgrading the Appliance Software, page 6-7 . |
| GUI Client | Yes | This host is one from which you run the GUI to managed the appliance. |

Required Traffic Flows

Required traffic flows identify traffic that must be allowed by gateways if they separate the MARS Appliance from a reporting device, mitigation device, or a supporting device (as listed in [Supporting Devices](#)). Also, traffic flows between a Global Controller and any monitored Local Controllers must be allowed.

The following table identifies categories of traffic flows, the protocols required, and how long they must be allowed:

Table 2-2 Required Traffic Flows and Ports

| Category | Protocols | Allow Only As Needed? | Comments |
|----------------|--------------------------|-----------------------|--|
| Management GUI | HTTPS/SSL (TCP port 443) | No | You cannot effectively use the appliance and block GUI-based management traffic. This traffic must be enabled for Global Controller-to-Local Controller, as well as from the MARS Appliance to the computer you are using to manage the appliance. |
| Management CLI | SSH (TCP 22) | Yes | — |

Table 2-2 Required Traffic Flows and Ports (continued)

| Category | Protocols | Allow Only As Needed? | Comments |
|--|---|-----------------------|--|
| Support Servers and Services | DNS (TCP and UDP port 53) NTP (TCP/UDP port 123) SMTP (TCP port 25) ICMP (IP level service) NFS | | SMTP is used for outgoing mail services. ICMP is useful for diagnostics and troubleshooting and is required by the dynamic vulnerability scanner. NFS is used for network-attached storage (NAS) servers to retain data archives for MARS. Because NFS ports are negotiated, it is recommended that the NAS server be located on the same network segment as the MARS Appliance. |
| Upgrade from GUI | HTTPS or FTP (TCP port 20 and 21) | Yes | Your options from within the GUI require that you |
| Upgrade from CLI | HTTPS, HTTP (TCP port 80), or FTP | Yes | At the command line, you can also upgrade from the DVD drive, which does not require any extra opened ports. |
| Discovery of reporting device or mitigation device | Telnet (TCP port 23) SSH FTP SNMP (TCP 161) | No | MARS Appliance periodically contacts the devices to ensure they are operational. |
| Monitoring of reporting device or mitigation device | HTTPS SSH SNMP Telnet FTP PostOffice (UDP port 45000) RDEP (SSL) SDEE (SSL) syslog (UDP port 514) | No | |
| Policy query to Cisco Security Manager | HTTPS | Yes | You must enable HTTPS access to the Common Services 3.0 server by the MARS Appliance. . |
| Global Controller and Local Controller data synchronization. | Proprietary (port 8444) | No | This port must remain open on the outside and inside interfaces to ensure accurate data correlation operations of the Global Controller. |

Table 2-2 Required Traffic Flows and Ports (continued)

| Category | Protocols | Allow Only As Needed? | Comments |
|----------|---|-----------------------|---|
| | NetFlow (TCP port 2055) | | You must enable Spanning Trees between switches (distribution and access switch, not the core). You can change the port on which the appliance listens for NetFlow traffic on the Admin > NetFlow Config page. |
| | OPSEC-LEA (TCP port 18184) OPSEC-CA (TCP 18210) SSLCA (TCP port 18184) OPSEC-CPMI (TCP port 18190) | | Used by Check Point devices only. CA is used for pulling a certificate for the OPSEC application. |
| | Oracle Database Listener (TCP port 1521) | | Used by Oracle only |
| | MS SQL (TCP port 1433) | | Used by FoundStone and eEye. |