



# CHAPTER 1

## Introduction to MARS

---

This chapter delineates basic components of the Cisco Security Monitoring, Analysis, and Response System (MARS), introduces the Global Controller and the Local Controller, and presents a basic understanding of features and deployment options.

This chapter contains the following topics:

- [System Description, page 1-1](#)
- [Basic Functions of the Global Controller, page 1-4](#)
- [Deployment, page 1-5](#)

## System Description

Cisco Security MARS is a security threat mitigation (STM) system. It delivers a range of information about your networks' health as reported by devices in your network. Cisco Security MARS processes raw events from your reporting devices, sessionizes them across different devices, evaluates for matching inspection rules (system and user-defined), identifies false positives, and consolidates information using diagrams, charts, queries, reports, and rules.



Tip

---

*Sessionize* refers to correlating the reported network data, logs, and events into a higher-level interpretation to identify those packets as part of a single session, or a communication, that has a beginning, a body, and an end.

---

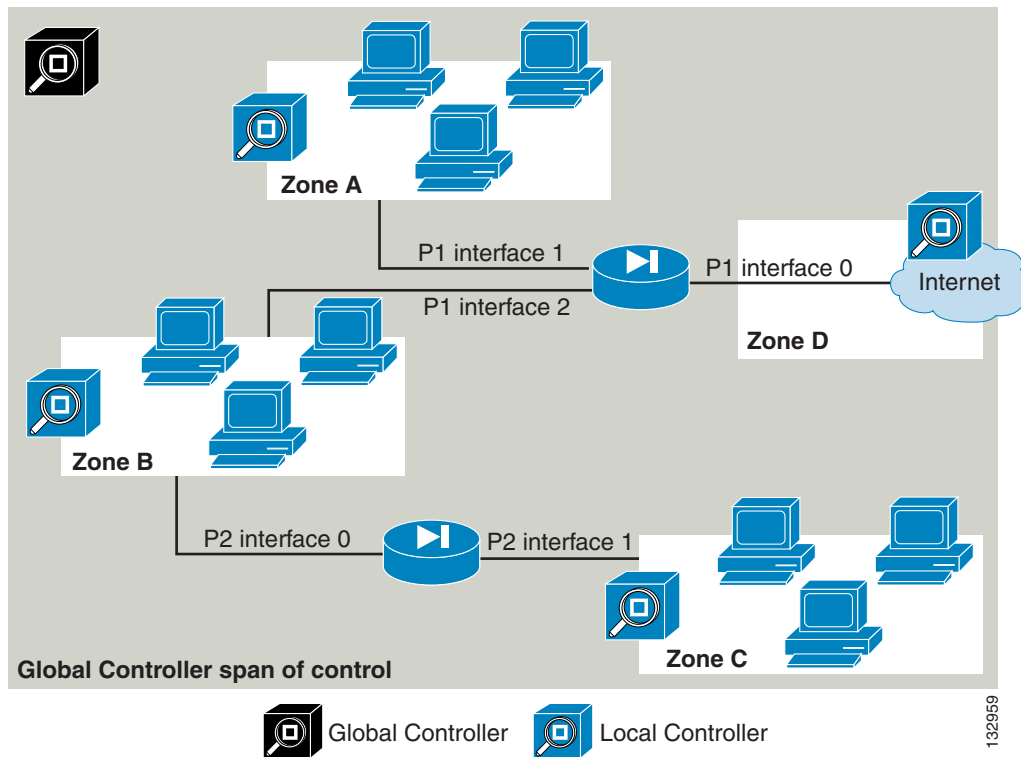
MARS enables you to be more productive by:

- Reducing the amount of raw data that requires manual review
- Enabling an evolving view of the network security posture
- Identifying hot spots of malicious activity
- Blocking undesirable traffic from the network

The MARS system operates at distinct and separate levels based on how much information is provided about your network's reporting devices. At its most basic level, MARS functions as a syslog server. As you add information about reporting devices, MARS begins to sessionize the raw data, and after you configure additional reporting devices and enable the more verbose reporting features, it presents a much more comprehensive view of your network, from which you can quickly drill-down to a specific MAC address, for example.

While it is possible to employ a single MARS appliance, many find that a distributed system preferable. In such a design, a Global Controller controls and communicates with a series of Local Controllers, thereby monitoring events from multiple local zones within the network. [Figure 1-1](#) presents an example deployment of MARS, which identifies these components and their relationships.

**Figure 1-1** Relationship of Global Controller to Local Controller to Reporting/Mitigation Device



This section contains the following topics:

- [Local Controller](#), page 1-2
- [Global Controller](#), page 1-3
- [Advantages of a Distributed Global/Local Architecture](#), page 1-3
- [MARS Web Interface](#), page 1-4
- [Reporting and Mitigation Devices](#), page 1-4

## Local Controller

The Local Controller models are as follows:

- Gen 1: MARS 20, MARS 20R, MARS 50, MARS 100, MARS 100e, and MARS 200.
- Gen 2: MARS 25, MARS 25R, MARS 55, MARS 110R, MARS 110, and MARS 210.

Each model differs in its ability to process and store events from reporting devices, enabling you to accurately address your needs based on the size of your network and the traffic volume.

Local Controllers receive and pull data from reporting devices, which may include firewalls, routers, intrusion detection/prevention systems, and vulnerability assessment systems. Based on the data obtained from those devices, and the established level of integration with them, MARS can present you with suggested mitigation rules for detected attacks and, in some cases, push those rules to the mitigation device, which is a network device that contains the attack by restricting network access to the infected hosts.

A Local Controller summarizes information about the health of your network based on data it receives from the reporting devices that it monitors.

The Local Controller performs the following functions:

- Collects all raw events
- Sessionizes events across different devices
- Fires inspection rules for incidents
- Determines false positives
- Delivers consolidated information in diagrams, charts, queries, reports, and notifications
- Detects inactive reporting devices

## Global Controller

A Global Controller summarizes the findings of two or more Local Controllers. In this way, the Global Controller enables you to scale your network monitoring without increasing the management burden. The Global Controller provides a single user interface for defining new device types, inspection rules, and queries, and it enables you to manage the Local Controllers under its control. This management includes defining administrative accounts and performing remote, distributed upgrades of the Local Controllers. The Global Controller is available in the following models:

- MARS GCm and MARS GC
- Gen 2: MARS GC2 and MARS GC2R

A Global Controller monitors two or more local zones. Each zone consists of a cluster of monitored devices and is managed by a Local Controller.

## Advantages of a Distributed Global/Local Architecture

The Global Controller/Local Controller architecture has the following advantages:

- It allows for centralized, distributed management of network topology.
- It lets remote sites view their own data while keeping data private between Global Controller and Local Controllers.
- It enables you to view the entire network from the Global Controller.
- It provides linear scalability using a multi-layer hierarchy.
- It enables you to use multiple Local Controllers to isolate departmental functions such as host logging, NIDS, compliance, and for network profiling and anomaly detection.
- It preserves the WAN link by pushing up correlated information instead of raw data from monitoring device.

## MARS Web Interface

The MARS web interface operates on a client computer. With many features common to both the Local Controller and Global Controller, the web interface uses a tabbed, hyperlinked, browser-based user interface. You access the web interface from any computer that can access the MARS Appliance on your network. For more information on client requirements, see the *Web Browser Client Requirements* section in the [Deployment Planning Guidelines](#) chapter of the *Cisco Security MARS Initial Configuration and Upgrade Guide, 6.X*.

From the web interface, you can perform most of your administrative functions, including all functions that are not supported at the command line.

## Reporting and Mitigation Devices

If you consider the MARS system from a top-down perspective, you see that the Global Controller monitors Local Controllers and that Local Controllers monitor one or more reporting devices. Reporting devices provide MARS with a variety of data about the network, from traffic flows (in the case of a router) to the configuration of possible attack targets (such as from a vulnerability assessment system).

A reporting device that can deny a traffic flow is called a *mitigation device* (for example, a switch). MARS provides mitigation support in two forms:

- For supported Layer 3 devices (based on the OSI Network Model), MARS provides you with a suggested device and set of commands that can be used to halt an ongoing, detected attack. You can use this information to manually block the attack.
- For supported Layer 2 devices, MARS recommends a device, a set of commands to halt the ongoing, detected attack, and provides a method for making the configuration changes on your behalf.

How you configure your reporting devices and mitigation devices greatly affects the ability of MARS to detect ongoing attacks.

## Basic Functions of the Global Controller

The Global Controller centrally manages a group of Local Controllers. Its user interface displays a listing of all the zones with their respective Local Controllers.

The Global Controller monitors and manages the network with a powerful suite of functions:

- Incidents
- Rules
- Queries and reports
- Centralized maintenance (for example, software upgrades of managed Local Controllers)

A Global Controller Admin user has the ability to create, edit or delete information on the Global Controller and its monitored Local Controllers. Information such as:

- Rules
- Reports and queries
- User, IP and service management
- Management grouping (for example, event and user groupings)

## Incidents

The Global Controller can monitor any Local Controller at any time to receive data. It receives summarized information from all its Local Controllers and produces a merged summary of this data. The summary consists of global topologies and incidents reflecting network activities in each of its zones. You can drill down on topologies and incidents to reach their subsets of paths and events at the zonal level.

The summaries provides an account of high-, medium-, and low-priority incidents. All network, port, protocol, applications, and events have to be global in scope to be on the Global Controller.

## Rules

The Global Controller uses rules to monitor the zones that report to it. Rules that apply to multiple Local Controllers can be created on the Global Controller and pushed down to them from a central location. These rules trigger incidents that you can review at the global level.

**Note**

---

Rules created on the Local Controller remain local. Incidents generated from these rules do not get pushed up to the Global Controller.

---

## Centralized Maintenance

The Global Controller leaves most data archiving to the Local Controller. However, some basic archive/restore capability is provided at the global level.

The Global Controller centrally manages all upgrades to the Local Controllers. Global Controller manages Local Controller(s) that are running the same version of the software as it is.

## Deployment

The Global Controller system's flexible architecture supports two basic types of deployment: incremental and greenfield. Each of these are discussed in the sections that follow.

This section contains the following topics:

- [Incremental Deployment, page 1-5](#)
- [Green-field, Multi-box Deployment, page 1-6](#)
- [Zone Planning, page 1-6](#)

## Incremental Deployment

In this scenario, an administrator deploys one or more Local Controller systems as standalone units. At a later date, the administrator decides to add a Global Controller. You must then ensure that the previously deployed Local Controllers can communicate with the new Global Controller. To enable this communication, you must:

1. Create a zone for each Local Controller
2. Ensure that the reporting devices do not overlap among zones

3. Upgrade the Local Controller version to be the same as that of the Global Controller
4. Add the Local Controller as a monitored controller in the Global Controller.
5. The Global Controller is then configured to communicate with each Local Controller by exchanging security certificate information.

After this communication has been enabled, the Global Controller is able to receive information, such as incidents and rules, from the Local Controller.

## Green-field, Multi-box Deployment

In this scenario, the network administrator decides from the very start to deploy two or more Local Controllers and a Global Controller to monitor them. In this case, the administrator defines the zones and their monitored devices ahead of time to complete a smooth installation.

## Zone Planning

A zone is a logical collection of one or more subnetworks that are home to the reporting devices monitored by a Local Controller. Zones allow a Global Controller to distinguish among events that are correlated by Local Controllers that monitor unique subnetworks with common network addresses. For example, consider the case where a managed security service provider (MSSP) uses a Global Controller to monitor the Local Controllers of their clients. That MSSP cannot prevent its clients from using the same private network addresses, however, it can use zones to distinguish among those networks and clients.

The requirements for planned zones are few:

- Each zone must be uniquely named.
- A Local Controller cannot belong to more than one zone.
- Each Local Controller corresponds to a single zone.