



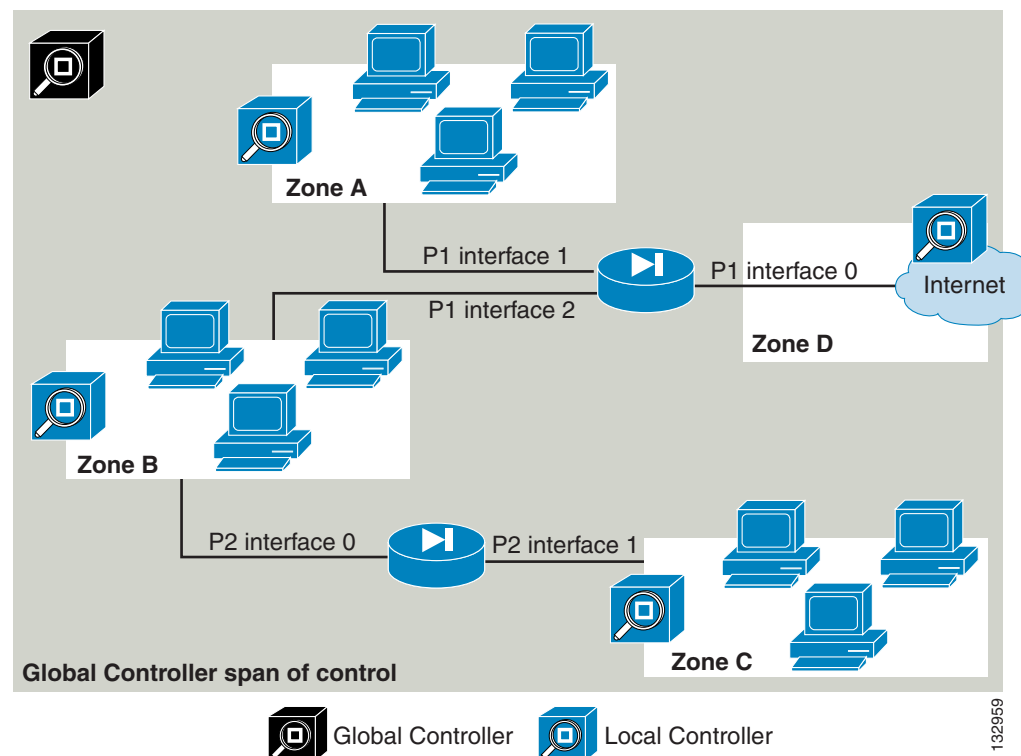
CHAPTER 1

Introduction

The MARS Global Controller is a security threat mitigation (STM) appliance. Once you deploy multiple Local Controllers, you can deploy a Global Controller that 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 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 two models—MARS GCm and MARS GC.

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. The following diagram shows the relationship between the Global Controller and multiple local zones.

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



For more information about the architecture of a distributed MARS system, refer to the [System Description](#), in the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*.

Advantages

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.
- You can view the entire network from the Global Controller.
- It enables linear scalability using a multi-layer hierarchy.
- You can 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.

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. The topologies and incidents can be drilled down to 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 is running the same version of the software as it is.

Deployment

The Global Controller system's flexible architecture supports two types of deployment:

- [Incremental Deployment, page 1-3](#)
- [Green-field, Multi-box Deployment, page 1-3](#)

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 to the scenario. The previously deployed Local Controllers must be upgraded to 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.

Once this communication is 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 must define the zones and their monitored devices ahead of time to complete a smooth installation.

