



## CHAPTER 10

# Monitoring, Analysis, and Correlation

---

The Cisco SAFE defense-in-depth approach results in the implementation of multiple layers security safeguards throughout the network, and the leverage of the network infrastructure as a security tool. Different forms of network telemetry present on each safeguard are leveraged to obtain a consistent and accurate view of the network activity. Logging and event information generated by routers, switches, firewalls, intrusion prevention systems, and endpoint protection software are globally collected, trended, and correlated using CS-MARS. Given the complexity of today's network environments, without central correlation and analysis capabilities troubleshooting and identifying security incidents and threats in the network would require hours if not days. The Cisco SAFE design blueprints leverage CS-MARS to quickly identify and react to threats before they affect the rest of the network.

CS-MARS allows for infrastructure-wide security intelligence and collaboration, enabling the designs to effectively:

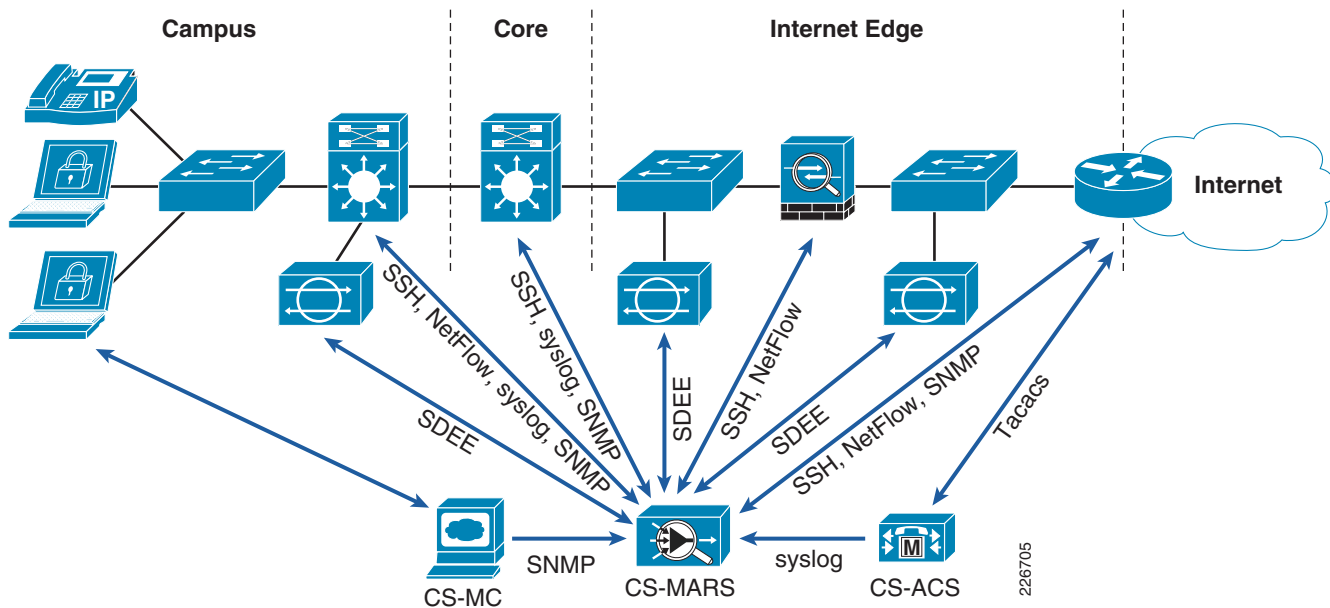
- *Identify threats*—Collecting, trending, and correlating logging, flow, and event information help identify the presence of security threats, compromises, and data leak.
- *Confirm compromises*—By being able to track an attack as it transits the network, and by having visibility on the endpoints, the architecture can confirm the success or failure of an attack.
- *Reduce false positives*—Endpoint and system visibility help identify whether a target is in fact vulnerable to a given attack.
- *Reduce volume of event information*—Event correlation dramatically reduces the number of events, saving security operator's precious time and allowing them to focus on what is most important.
- *Determine the severity of an incident*—The enhanced endpoint and network visibility allows the architecture to dynamically increase or reduce the severity level of an incident according to the degree of vulnerability of the target and the context of the attack.
- *Reduce response times*—Having visibility over the entire network makes it possible to determine attack paths and identify the best places to enforce mitigation actions.

## Key Concepts

CS-MARS analysis and correlation is based on the processing of event and log information provided by the various reporting and mitigation devices. In Cisco SAFE blueprints, reporting and mitigation devices include Cisco ASA security appliances, Cisco IOS routers and switches, Cisco IPS appliances and modules, Cisco Security Agent Management Console (CSA-MC), and Cisco Secure Access Control Server (CS-ACS). This is illustrated in Figure 10-1 below. CS-MARS also has the ability to leverage non-Cisco products. The list of Cisco and non-Cisco supported products can be found at the following URL:

[http://www.cisco.com/en/US/products/ps6241/products\\_device\\_support\\_tables\\_list.html](http://www.cisco.com/en/US/products/ps6241/products_device_support_tables_list.html)

**Figure 10-1** Event Monitoring, Analysis and Correlation



One important concept is that event information generated by the reporting devices is collected by CS-MARS in two different ways: it is either pushed to CS-MARS from the device, or is pulled by CS-MARS from the device. The collection type depends on the characteristics of the reporting device such as the access protocols supported and the configuration choices. These and other important concepts are explained next.



### Note

CS-MARS implements a customer parser that can be used to add support to unsupported applications or systems. The parser uses regular expressions to interpret Simple Network Management Protocol (SNMP) and syslog messages, and to map them into CS-MARS known message types.

## Access and Reporting IP address

As some reporting and mitigation devices may have multiple interfaces and IP addresses, CS-MARS allows the configuration of separate IP addresses for the collection of event information that is either pulled by or push to CS-MARS. To that end, when adding a reporting or mitigation device in the web interface, the user may specify an access IP address and a reporting IP address. For devices with a single IP address, both access and reporting IP addresses should be configured as the same.

The access IP address is used by CS-MARS to either connect to the device with a remote administrative session or connect to a remote server on which a file containing the device's configuration is stored. In contrast, CS-MARS uses the reporting IP address to associate received messages with the correct device. The reporting IP is the source IP address of event messages, logs, notifications, or traps that originate from the device. The fundamental difference between the two types of IP addresses is that the reporting IP address is treated passively by CS-MARS. CS-MARS does not query the device using this address; such operations are performed using the access IP address.

If following the best practices discussed in the [“Infrastructure Device Access Best Practices” section on page 2-2](#), the reporting and mitigation devices should not grant access to CS-MARS unless the appliance is configured as a trusted system from which administrative access should be allowed. At the same time, the devices should be configured to treat the CS-MARS appliance as a trusted destination for log, event, and trap information.

**Note**

Only one reporting IP address is accepted per device. In order for CS-MARS to parse and correlate events properly, all message types (NetFlow, syslog, etc) originating from the same device should come from a common source IP address. If messages do not originate from a common IP address, one of the message types is seen as coming from an unreported device, affecting correlation. In the case of Cisco IOS devices, ensure that services such as NetFlow and syslog are bounded to the same IP address.

## Access Protocols

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

- *SNMP*—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, Address Resolution Protocol (ARP) tables, and address translations. If granted read-write access, SNMP also allows for mitigation on any Layer-2 devices that support MIB2.

**Note**

CS-MARS uses SNMP v1 to perform device discovery. If CS-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 CS-MARS to occur over an encrypted channel.

- *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 Layer-2 devices.
- *Secure Shell (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 Layer-2 devices. This access method is recommended for mitigation device 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 CS-MARS does not support a modulus size smaller than 768.

- *Trivial File Transfer Protocol (TFTP)*—Allows passive discovery of settings by providing CS-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 Network Address Translation (NAT) and ARP tables. In addition, if the FTP access type for device types is selected, such as Cisco ASA and Firewall Service Module (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 CS-MARS appliance has access. This FTP server must have user authentication enabled.

## Reporting Protocols

CS-MARS leverages a variety of reporting protocols for the reception of event information. Depending on the platform, the following options may be available:

- *Syslog*—System logging (syslog) may be used to provide information on session activity (setup, teardown, and deny), NAT transactions, resource usage, and system status.
- *SNMP*—SNMP traps may be used to send CS-MARS information indicating session activity (setup, teardown, and deny), NAT transactions, resource usage, and system status.
- *NetFlow*—NetFlow data is used to profile the network usage, detect statistically significant anomalous behavior, and to correlate anomalous behavior. NetFlow security event logging (NSEL) provides information on session activity (setup, teardown, and deny) and NAT transactions.
- *Security Device Event Exchange (SDEE)*—SDEE is a protocol developed by a consortium led by Cisco and designed for the secure exchange of network event information. Cisco IPS appliances and modules, and Cisco IOS IPS use SDEE to communicate security events. At the same time, CS-MARS leverages SDEE to pull configuration information, logs, and other information from Cisco IPS appliances and modules.

## Events, Sessions and Incidents

To facilitate the analysis of security incidents, CS-MARS interprets each security incident as a collection of sessions, each one composed by one or more security events:

- *Events*—An event refers to a single alarm or message pushed to CS-MARS by the monitoring reporting devices (syslogs, SNMP traps) or pulled by CS-MARS, the monitoring reporting devices (IPS alerts, Windows log, etc)
- *Sessions*—A set of messages (events) that are correlated by the CS-MARS across NAT boundaries.
- *Incidents*—A set of sessions that match defined inspection rules. Rules are either included in the CS-MARS system or defined by the administrator. An incident is a chain of correlated events that describe an attack scenario.

Some examples of incidents are as follows:

- Reconnaissance activity followed by a penetration attempt, and further, followed by malicious activity on the target host.
- Reconnaissance activity followed by denial-of-service (DoS) attempt.

# CS-MARS Monitoring and Mitigation Device Capabilities

This section explains the access protocols and mitigation capabilities supported by the platforms in the Cisco SAFE designs.

## Cisco IPS

CS-MARS extracts the logs from Cisco IPS 5.x and 6.x devices and modules using SDEE. SDEE communications are secured with Secure Sockets Layer/Transport Layer Security (SSL/TLS). Therefore, CS-MARS must have HTTPS access to the Cisco IPS sensor. This requires configuration of the Cisco IPS sensor as well as CS-MARS.

To allow access, HTTPS access must be enabled on the Cisco IPS sensor, and the IP address of CS-MARS must be defined as an allowed host, one that can access the sensor to pull events. In addition, an administrative account to be used by CS-MARS should be configured locally on the Cisco IPS sensor. As a best practice, this account should be set with a user role of viewer to ensure only the minimum necessary access privileges are granted. This account should not be used for any other purposes.

## Event Data Collected from Cisco IPS

There are three types of event data that CS-MARS may extract from a Cisco IPS sensor:

- *Event alerts*—Alarm messages generated every time the Cisco IPS sensor identifies a match to a signature. Information contained in the event alerts include signature ID, version and description, severity, time, source and destination ports and IP addresses of the packets that triggered the event.
- *Trigger packet data*—Information of the first data packet that triggered a signature. This information is useful for a deeper analysis and to help diagnose the nature of an attack. The trigger packet data helps to visualize the data that was transmitted the instant the alarm was triggered. Trigger packet data is available for those signatures configured with the "produce-verbose-alert" action.
- *Packet data (IP logging)*—IP packet log, by default contains 30 seconds of packet data. This information is useful for a much deeper analysis. The IP packet log provides a view of the packets transmitted during and instants after the signature was triggered. IP packet logging is available for signatures configured with the *produce-verbose-alert* action and the *log-pair-packets* action. In addition, the pull IP logs option should be enabled for the Cisco IPS sensor under **Admin > System Setup > Security and Monitor Devices**.

Note that, while trigger packet data and IP logging provide valuable information for the analysis of security incidents, configuring IP logging and verbose alerts on the sensor is system-intensive and does affect the performance of the sensor. In addition, it affects the performance of the CS-MARS appliance. Because of these effects, be cautious in configuring signatures to generate IP logs.

## Verify that CS-MARS Pulls Events from a Cisco IPS Device



The first step for verifying if CS-MARS can pull events from a Cisco IPS sensor is to confirm both are able to communicate. To that end, select the test connectivity option under the Cisco IPS device configuration (**Admin > System Setup > Security and Monitor Devices**). A "Connectivity Successful" message indicates both systems are able to communicate.













The second step is to perform an action to knowingly trigger a signature on the Cisco IPS sensor. As an example, type the following URL on a browser, replacing *x.x.x.x* by the IP address or hostname of a web server located on a subnet monitored by the Cisco IPS sensor.

http://x.x.x.x/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

This action should be interpreted as a WWW IIS unicode directory traversal attack, triggering Cisco IPS signatures numbers 5114 and 5081. The event shown in [Figure 10-2](#) should be seen at the incidents page.

**Figure 10-2 Security Incident**

Incident ID: 40453163   Expand All Collapse All

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	Tune
3	S:131998401, I:40453163 	WWW IIS Unicode Directory traversal  WWW WinNT cmd.exe Exec 	10.240.100.2  17277 	10.245.255.250  80 	TCP 	Mar 11, 2009 3:29:25 AM GMT	sfx12-ips4270-1/vs0  		 	False Positive Tuning

Copyright © 2003–2008 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

226706

## IPS Signature Dynamic Update Settings

In Release 6.0 and later, Cisco IPS supports dynamic signature updates. CS-MARS can discover the new signatures and correctly process and categorize received events that match those signatures. If this feature is not configured, the events appear as unknown event type in queries and reports, and CS-MARS does not include these events in inspection rules. These updates provide event normalization and event group mapping, and they enable CS-MARS appliance to parse day-zero signatures from the IPS devices.

The downloaded update information is an XML file that contains the IPS signatures. However, this file does not contain detailed information, such as vulnerability information. Detailed signature information is provided in later CS-MARS signature upgrade packages just as with third-party signatures.

The screenshot in [Figure 10-3](#) shows the configuration of dynamic IPS signature updates.

**Figure 10-3 PS Signature Dynamic Update**

Copyright © 2003–2008 Cisco Systems, Inc.  
All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

226707

## Cisco ASA Security Appliance

CS-MARS requires administrative access to be able to discover the Cisco ASA firewall configuration settings. Administrative access is possible via Telnet (not recommended) or SSH.

The following data is learned by CS-MARS as a result of the discovery operation:

- 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, exposing the real instigator of attacks.
- OS Settings, from which CS-MARS determines the correct ACLs to block detected attacks, which paste into a management session with the Cisco firewall device.

In order to access the device, the Telnet/SSH access rules on the Cisco ASA firewall need to be configured to grant access to the IP address of the CS-MARS appliance. Administrative access also requires the use of an administrative account. The best practice is to use AAA and use a separate user account dedicated for this sort of access. It is also recommended to define a local account on the Cisco ASA for fallback access in case the AAA service is unavailable. Note that CS-MARS device configuration only allows the definition of a single set of username and password credentials. Therefore, fallback access will not succeed unless the local account is maintained up-to-date with the same credentials as the ones configured on CS-MARS.

In the case of SSH access, keys should be generated with a minimum modulus size of 768.

On Cisco ASA appliances configured with multiple contexts, it is important to discover each one of the contexts. Failing to do so affects the ability of CS-MARS to adequately learn the network topology. Virtual contexts should be identified by CS-MARS automatically after the initial discovery of the Cisco ASA appliance. Then, the reporting and access information of each context needs to be provided individually.

## Event Data Collected from Cisco ASA

The following information may be collected by CS-MARS from a Cisco ASA security appliance:

- *Resource usage*—Using SNMP read-only access, CS-MARS may monitor the device's CPU and memory usage, network usage, and device anomaly data. SNMP read-only access is also used to discover device and network settings. SNMP access requires the definition of an access IP address for the monitored device.
- *Accept/deny logs*—Syslog/SNMP trap information indicating session setup, teardown and deny, as well as NAT translations. This information is useful for false-positive analysis. CS-MARS support SNMPv1.
- *NetFlow security event logging (NSEL)*—Available on software Version 8.1 for ASA5580 and Version 8.2 for other ASA platforms, provides the same type of information as syslog but more efficiently, saving CPU cycles on both the Cisco ASA appliance and CS-MARS. Both connection information and NAT translation data are combined in the same NSEL records, reducing the overall number of records exported compared to syslog.

Cisco ASA appliances should take advantage of NSEL for higher efficiency and scalability. NSEL requires the configuration of CS-MARS as a NetFlow collector on the Cisco ASA appliance.

There are some system status and other messages that are logged with syslog and not with NSEL. The Cisco ASA appliance can be configured to disable the logging of any redundant messages generated by syslog and NSEL. This is done by configuring the **logging flow-export-syslogs disable** command on the Cisco ASA appliance.

Table 10-1 lists the disabled syslog messages

**Table 10-1 Syslog Messages**

Syslog Message	Description	Severity Level
106015	A TCP flow was denied because the first packet was not a SYN packet.	Informational (6)
106023	A flow that is denied by an ingress ACL or an egress ACL that is attached to an interface through the <b>access-group</b> command.	Warning (4)
106100	A flow that is permitted or denied by an ACL.	Warning (4)
302013 and 302014	A TCP connection and deletion.	Informational (6)
302015 and 302016	A UDP connection and deletion.	Informational (6)
302017 and 302018	A GRE connection and deletion.	Informational (6)
302020 and 302021	An ICMP connection and deletion.	Informational (6)
313001	An ICMP packet to the security appliance was denied.	Error (3)
313008	An ICMPv6 packet to the security appliance was denied.	Error (3)
710003	An attempt to connect to the security appliance was denied.	Error (3)



### Note

To be able to query events triggered with NetFlow, CS-MARS needs to be configured to *always store* ASA NetFlow security event logs. Note that this may have an impact on the CS-MARS performance.



**Note**

When monitoring a failover pair of Cisco firewall devices (PIX or ASA), designate the primary Cisco firewall device as the device to be monitored. If failover occurs, the secondary device assumes the IP address of the primary, which ensures that session correlation is maintained after the failover. The same focus on the primary is true for performing any bootstrap operations. The secondary device will synchronize with the configuration settings of the primary.

## Verify that CS-MARS Pulls Events from a Cisco ASA Security Appliance

The first step is to ensure CS-MARS is able to communicate with the Cisco ASA Security appliance. This can be verified by forcing a device discovery. Discovery is triggered under the Cisco ASA device configuration (**Admin > System Setup > Security and Monitor Devices**).

An easy way to verify CS-MARS is receiving events from the Cisco ASA appliance is to generate packets or connections expected to be blocked by the firewall's policies. That should trigger "*Denied TCP/UDP request to Firewall*" message as shown in [Figure 10-4](#).

**Figure 10-4** Denied TCP/UDP Request

I:404531860	Denied TCP/UDP request to Firewall	System Rule: Network Errors - Likely Routing Related	Mar 11, 2009 4:04:49 AM GMT - Mar 11, 2009 4:16:56 AM GMT	226708
-------------	------------------------------------	--	---	--------

## Cisco IOS

CS-MARS requires administrative access to be able to discover routers and switches running Cisco IOS software. Administrative access is possible via Telnet (not recommended), SNMP or SSH (most recommended).

In order to access the device, Telnet/SSH access needs to be allowed to the IP address of the CS-MARS appliance. In the case of SSH access, keys should be generated with a minimum modulus size of 768.

Administrative access also requires the use of an administrative account. The best practice is to use AAA and use a separate user account dedicated for this sort of access. It is also recommended to define a local account on the Cisco ASA for fallback access in case the AAA service is unavailable. Note that CS-MARS device configuration only allows the definition of a single set of username and password credentials. Therefore fallback access will not succeed unless the local account is maintained up-to-date with the same credentials as the ones configured on CS-MARS.

## Event Data Collected from a Cisco IOS Router or Switch

The following information may be collected by CS-MARS from a Cisco router or switch running Cisco IOS software:

- *Resource usage*—Using SNMP read-only access, CS-MARS may monitor the device's CPU and memory usage, network usage, and device anomaly data. SNMP read-only access is also used to discover device and network settings. SNMP access requires the definition of an access IP address for the monitored device. CS-MARS supports SNMPv1.
- *Syslog messages*—The syslog messages provide information about activities on the network, including accepted and rejected sessions. This information is useful for false-positive analysis.

- *NetFlow*—CS-MARS can leverage NetFlow Versions 1, 5, 7, and 9 data to profile the network usage, to detect statistically significant anomalous behavior, and to correlate anomalous behavior to events generated by other reporting systems.
- *SDEE*—CS-MARS uses SDEE to capture security event, logs, and configuration information from Cisco IOS devices configured with Cisco IOS IPS.

The collection of NetFlow records allows CS-MARS to leverage the routing and switching infrastructure for detecting anomalous behavior such as DDoS attacks and worm propagation. NetFlow information is also leveraged for the computation of the Top N Reports (i.e., top destination ports, top sources, etc).

In order to identify traffic anomalies, CS-MARS computes a baseline of connection rates per flows. The baseline starts to be computed as soon as NetFlow collection is configured on CS-MARS. After enough flow information is collected over the course of roughly one week, CS-MARS switches into anomaly detection mode where it looks for statistically significant behavior (i.e., the current connection rate exceeds the mean by two to three times the standard deviation). CS-MARS continues to readjust the baseline as it learns new traffic. After detecting an anomaly, CS-MARS starts to dynamically store the full NetFlow records for the anomalous traffic, allowing the identification of useful contextual information including source and destination IP addresses, and destination ports.

## Verify that CS-MARS Pulls Events from a Cisco IOS Device

The first step is to ensure CS-MARS is able to communicate with the Cisco IOS device. This can be verified by forcing a device discovery. Discovery is triggered under the Cisco IOS device configuration (**Admin > System Setup > Security and Monitor Devices**).

For syslog and SNMP traps, an easy way to verify CS-MARS is receiving events from the Cisco IOS device is to generate packets or connections expected to be blocked by an existing ACLs.

A simple way to verify if the CS-MARS appliance is receiving NetFlow records, is to open an SSH session into the appliance and run a **tcpdump port 2055** command. The **tcpdump** command will show the details of NetFlow records exchanged over UDP/2055. The following is an example:

```
[pnadmin]$ tcpdump port 2055
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
07:42:08.836748 IP sfx13asa5580-1.cisco.com.260 > pnmars.2055: UDP, length 332
07:42:08.887558 IP sfx13asa5580-1.cisco.com.260 > pnmars.2055: UDP, length 176
07:42:21.946359 IP dca-core1.cisco.com.65532 > pnmars.2055: UDP, length 72
07:42:22.825689 IP sfx13asa5580-1.cisco.com.260 > pnmars.2055: UDP, length 176
07:42:22.877774 IP sfx13asa5580-1.cisco.com.260 > pnmars.2055: UDP, length 332
```

In case CS-MARS is configured to store NetFlow records, they can be viewed by running a query matching event raw messages. This is done in the web interface under **Query/Reports>Query**.

## Cisco Security Agent (CSA)

To enable CSA as a reporting system in CS-MARS, you must identify the CSA-MC as the reporting device. The CSA-MC receives alerts from the CSA agents that it monitors, and it forwards those alerts to CS-MARS as SNMP notifications.

When CS-MARS receives the SNMP notification, the source IP address in the notification is that of the CSA agent that originally triggered the event, rather than the CSA-MC that forwarded it. Therefore, CS-MARS requires host definitions for each of the CSA agents that can potentially trigger an event. These definitions are added as sub-components under the device definition of the CSA-MC.

As of CS-MARS, Release 4.1.1, the CS-MARS appliance discovers CSA agents as they generate alerts, eliminating the need for manual configuration. CS-MARS parses the alert to identify the CSA agent hostname and to discover the host operating system (OS). CS-MARS uses this information to add any undefined agents as children of the CSA-MC as a host with either the generic Windows (all Windows) or generic (Unix or Linux) OS value. It is still required to configure CSA-MC as a reporting system in CS-MARS web interface.

**Note**

The first SNMP notification from an unknown CSA agent appears to originate from the CSA-MC. CS-MARS parses this notification and defines a child agent of the CSA-MC using the discovered settings. Once the agent is defined, all subsequent messages appear to originate from the CSA agent.

Configuration of CSA-MC requires the definition of CS-MARS as SNMP-trap destination. This is done under **Events> Alerts**, add new alert configuration, set SNMP host and community. Note that currently CS-MARS supports SNMPv1. See [Figure 10-5](#).

**Figure 10-5** CSA-MC Configuration

The screenshot shows the 'Management Center for Cisco Security Agents V6.0' web interface. The breadcrumb navigation is 'Events > Alerts > MARS SNMP alert notification'. The form contains the following fields and sections:


- Name:** MARS SNMP alert notification
- Description:** (empty field)
- Send Alerts:**
  - For the following event sets: A list box containing:
    - All events [V6.0 r209]
    - All events of severity notice and lower [V6.0 r209]
    - All Monitor Events [V6.0 r209]
    - Analysis - Application Behavior [V6.0 r209]
    - Analysis - Application Deployment [V6.0 r209]
  - A 'New' button and a 'double-click event set to view' instruction are present.
- Alert Method:**
  - ☐ **Email:**
    - Recipient(s) email address(es): (empty field)
    - Sender address to use: (empty field)
    - Address of mail server: (empty field)
    - Message subject: (empty field)
    - ☐ Include event details
  - ☒ **SNMP:**
    - Community name: w2kew34kw
    - Manager IP address: 10.242.50.99

A vertical text '226709' is visible on the right side of the form.

Configuration on CS-MARS requires adding CSA-MC as a reporting device. This is done in CS-MARS web interface by clicking **Add** under **Admin> Security and Monitor Devices**, and by selecting **Add SW Security apps on a new host** as device type. Configuration also requires selecting the appropriate CSA version as the reporting application and setting the reporting and access IP addresses.

See [Figure 10-6](#) and [Figure 10-7](#).

Figure 10-6 Adding Reporting Application to CS-MARS



SUMMARYINCIDENTSQUERY / REPORTSRULESMANAGEMENTADMINHELP

System SetupSystem MaintenanceUser ManagementSystem ParametersCustom SetupMar 11, 2009 9:21:37 PM GMT

ADMIN | CS-MARS Standalone: pnmars v6.0Login: Administrator (pnadmin) :: Logout :: Activate

Note:

1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. \* denotes a required field.

Device Type: Edit host with security applications

GeneralReporting ApplicationsVulnerability Assessment Info

→ \*Device Name: sfx-csamc

→ Access IP: 1085110

→ Reporting IP: 1085110

→ Operating System: GenericLogging Info

→ NetBIOS Name:

→ Monitor Resource Usage: NO

Enter interface information:

Add InterfaceRemove Interface/IP

Name:IP Address:Network Mask:

☐ ether010851102552552550Add IP/Network Mask

DoneApplyNext

228710

**Figure 10-7 Adding Cisco CS-MC**

Note:

1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. \* denotes a required field.

Device Type: Edit host with security applications

General Reporting Applications Vulnerability Assessment Info

Enter reporting application:

→ Device Name: sfx-csamc

→ Select application:

Device Type

☐ Cisco CSA Management Center 5.x

Copyright © 2003–2008 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

226711

## Verify that CS-MARS Receives Events from CSA

The simplest way to verify if CS-MARS receives events from the CSA is to verify if clients are being dynamically added as reporting devices. This can be seen in CS-MARS web interface, under **Admin > System Setup > Security and Monitor Devices**. See [Figure 10-8](#).

**Figure 10-8 CSA Agents**

<input type="checkbox"/>	Device Name	Device Type	Provider	Agents	Access IP	Reporting IP	Monitoring Networks	Device Display
<input type="checkbox"/>	sfx-csamc	Cisco CSA Management Center 5.x	Cisco	CISCO-D7386PDF5, SFX11-PC-1.cisco.com, SFX11-PC-3.cisco.com, SFX11-PC2.cisco.com, branch-client2 ... <input type="button" value="Show All"/>	10.8.51.10	10.8.51.10		

226712

## Cisco Secure ACS

Cisco Secure ACS sever and the ACS Solutions Engine (SE) can be configured to forward CS-MARS syslog messages to notify AAA activity such as successful authentication attempts, failed authentication attempts, TACACST+ , and RADIUS accounting.

To that end, configure CS-ACS to forward the desired syslog events to CS-MARS. This is configured on CS-ACS web interface, under **System configuration> Logging**. The following are some examples:

- *PassedAuth*—Cisco ACS passed authentications.
- *FailedAuth*—Cisco ACS failed attempts.
- *RADIUSAcc*—Cisco ACS RADIUS accounting.
- *TACACSAcc*—Cisco ACS TACACS+ accounting.
- *TACACSAdmin*—Cisco ACS TACACS+ administration.

Use a maximum message length of 500 bytes, which is required for CS-MARS.

The screenshot in [Figure 10-9](#) illustrates CS-ACS configuration.

**Figure 10-9 CS-ACS Configuration**

**System Configuration**

**Syslog Failed Attempts File Configuration**

**Enable Logging** ?

☒ Log to Syslog Failed Attempts report

**If the selected log is disabled, ACS will not implement critical logging for that report.**

**Select Columns To Log** ?

**Syslog Servers** ?

	IP	Port	Max message length (Bytes)
<b>Server 1:</b>	172.26.191.99	514	500
<b>Server 2:</b>			

**Back to Help** ?

226713

On the CS-MARS, the Cisco Secure ACS server needs to be added as a reporting device. This requires adding a new device in CS-MARS web interface and selecting **Add SW Security apps on a new host** and then choosing the appropriate version of CS-ACS as a reporting applications. This is illustrated in [Figure 10-10](#) and [Figure 10-11](#).

**Figure 10-10 Adding CS-ACS**

**CISCO**

SUMMARY INCIDENTS QUERY / REPORTS RULES MANAGEMENT ADMIN HELP

System Setup System Maintenance User Management System Parameters Custom Setup Mar 11, 2009 9:21:37 PM GMT

ADMIN | CS-MARS Standalone: pnmars v6.0 Login: Administrator (pnadmin) :: Logout :: Activate

Note:  
 1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.  
 2. \* denotes a required field.

Device Type: Edit host with security applications

General Reporting Applications Vulnerability Assessment Info

→ \*Device Name: sfx-csamc

→ Access IP: 10 8 51 10

→ Reporting IP: 10 8 51 10

→ Operating System: Generic Logging Info

→ NetBIOS Name:

→ Monitor Resource Usage: NO

Enter interface information:

Add Interface Remove Interface/IP

Name:	IP Address:	Network Mask:
ether0	10 8 51 10	255 255 255 0

Add IP/Network Mask

Done Apply Next

226714

Figure 10-11 Adding CS-ACS as a Reporting Application

SUMMARYINCIDENTSQUERY / REPORTSRULESMANAGEMENTADMINHELP

System SetupSystem MaintenanceUser ManagementSystem ParametersCustom SetupMar 11, 2009 9:25:21 PM GMT

ADMIN | CS-MARS Standalone: pnmars v6.0Login: Administrator (pnadmin) :: Logout :: Activate

Note:

1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.  
2. \* denotes a required field.

Device Type: Edit host with security applications

GeneralReporting ApplicationsVulnerability Assessment Info

Enter reporting application:

→ Device Name: sfx-csamc

→ Select application: Select one Add

EditRemove

Device Type

Cisco CSA Management Center 5.x

Done

Copyright © 2003–2008 Cisco Systems, Inc. All rights reserved. Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

226715

Verify that CS-MARS Receives Events from CS-ACS

An easy way to verify if CS-MARS receives events from CS-ACS is to generate an incident by failing access attempts to a device running AAA. Failed AAA authentication events should be found at the incidents page on CS-MARS. See Figure 10-12.

Figure 10-12 Failed AAA Authentication

Incident ID: 40453200

Expand AllCollapse All

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	Tune
1		Failed AAA authentication	10.82.233.28	172.26.170.6	N/A	Total: 3				
1	S:132027790, I:40453200	Failed AAA authentication	10.82.233.28	172.26.170.6	N/A	Mar 11, 2009 4:43:31 AM GMT	ie-srv1-oob.cisco.com	attacker		False Positive Tuning
1	S:132027829, I:40453200	Failed AAA authentication	10.82.233.28	172.26.170.6	N/A	Mar 11, 2009 4:43:39 AM GMT	ie-srv1-oob.cisco.com	attacker		False Positive Tuning
1	S:132028401, I:40453200	Failed AAA authentication	10.82.233.28	172.26.170.6	N/A	Mar 11, 2009 4:45:06 AM GMT	ie-srv1-oob.cisco.com	www		False Positive Tuning

226716



# CS-MARS Design Considerations

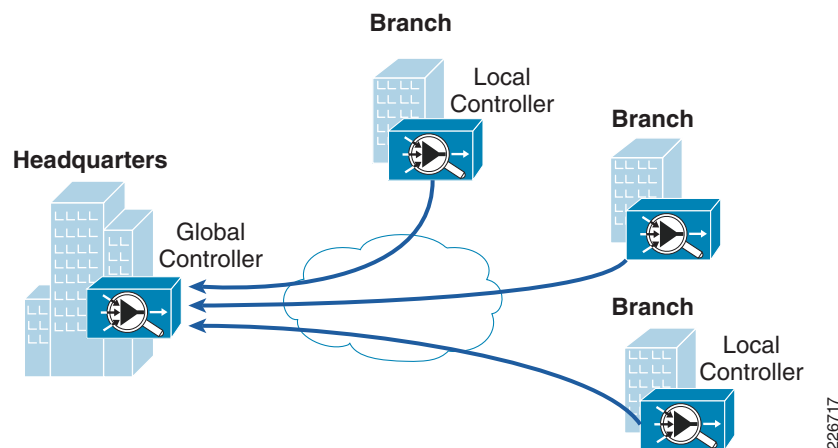
## Global/Local Architecture

While CS-MARS can be deployed as standalone appliances, environments with high levels of activity typically mandate the use of multiple appliances. There are two approaches that can be followed when implementing multiple CS-MARS appliances in the network—use them as standalone devices or, more preferably, leverage them as distributed systems managed by a global controller in a hierarchical design. Using a global controller has the following advantages:

- It provides global visibility to the entire network.
- It enables linear scalability using a multi-layer hierarchy.
- It allows for departmental/regional administration
- It preserves bandwidth on WAN links.

Figure 10-13 illustrates CS-MARS hierarchical deployment.

**Figure 10-13 CS-MARS Hierarchical Deployment**



In a hierarchical deployment, multiple local controllers are deployed at different network locations. Each local controller is responsible for receiving and pulling event data from the reporting devices at its location. The local controller is also responsible of summarizing the information about the health of the network.

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

The global controller appliance is responsible for summarizing the findings of the local controllers, and centralizing all reporting generated by the local controllers, providing a single aggregated view of the network health. In addition, the global controller provides a single user interface for managing all local controllers under its control. This includes centralized management for defining new device types, inspection rules, and queries.

Global controller capabilities include:

- Aggregation of reports across the local controller (LC) deployment
- Defining rules, reports and user accounts for local controllers



---

**Note** Configuration of LC is done *locally* on the individual LC appliance.

---

- Remote, distributed upgrade of the LCs

## CS-MARS Location

CS-MARS stores sensitive topological and configuration information, and it is one the key elements for system-wide intelligence and collaboration. For this reason, CS-MARS needs to be placed in secured environment. Cisco SAFE design places CS-MARS in the NOC/Management segment. The NOC/Management segment is protected with the use of an IDS and an ASA security appliance, and access from the network is controlled and restricted to the necessary services and systems.

Environments requiring the implementation of multiple CS-MARS appliances should follow the same approach, placing them in a secure segment and ensuring the security of their communication channels.

## CS-MARS Sizing

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

The following are the key considerations for deployment:

- *Number of sites CS-MARS supports*—The available bandwidth at hub and remote office, plus the number and type of reporting devices provide an idea of the anticipated volume and rate of event data. It also helps determine if the bandwidth available is sufficient.
- *Requirements for high availability*—Some CS-MARS models include RAID arrays and redundant power supplies.
- *Expected events per second*—CS-MARS appliance models vary in their capacity of how many events can be handled per second.
- *Online storage capacity needed*—Depending on the database size anticipated.

For more information on CS-MARS models, refer to the *CS-MARS User* documentation.

[http://www.cisco.com/en/US/products/ps6241/tsd\\_products\\_support\\_configure.html](http://www.cisco.com/en/US/products/ps6241/tsd_products_support_configure.html)

# Deployment Best Practices

## Network Foundation Protection (NTP)

When implementing network telemetry, it is important that dates and times are both accurate and synchronized across all network infrastructure devices. Without time synchronization, CS-MARS may not be able to correlate the different sources of telemetry properly. For this reason is fundamental that CS-MARS and all its reporting and mitigation devices are synchronized with NTP.

When deploying a single, centralized CS-MARS appliance the best practice is to configure all reporting and mitigation devices under the same time-zone. When using a hierarchical design, each local controller may be placed into a different time-zone. The global controller is capable of offsetting the time-zone differences.

NTP deployment best practices are covered in [Chapter 2, “Network Foundation Protection.”](#)

## Monitoring and Mitigation Device Selection

As discussed earlier, multiple access and reporting mechanisms may be available for the same device, and in some cases they may provide the same event information. At the same time, in most places in the network, the same monitoring or mitigation functions may be implemented on different platforms. Certainly, enabling all access and reporting mechanisms on all network devices is usually unnecessary, and most likely results in duplicate information, wasting and potentially exhausting precious CS-MARS resources. For this reason, CS-MARS deployment needs to be carefully planned. Part of this planning should include the identification of the best devices for monitoring and mitigation purposes. Planning should also identify the most appropriate access and monitoring mechanisms to be enabled on each one of selected devices. Factors such as the topological location, processing capacity, and supported access and mitigation methods should be considered.

The following are general recommendations of CS-MARS deployment for Cisco SAFE designs.

### Cisco IPS

CS-MARS communicates with Cisco IPS appliances and modules using SDEE. The following are the recommendations:

- Add all Cisco IPS appliances and modules to CS-MARS.
- If available, the administrative interface of the Cisco IPS sensor or module should connect to the OOB management network or over a secured segment.
- Limit the address of all hosts or network that have permission to gain administrative access to the sensor. Add the IP address of CS-MARS as a trusted host.
- Define a local administrative account to be used for CS-MARS access only. Specify the account viewer access, which is the minimum level required for the device to be discovered.

## Cisco ASA

Cisco ASA supports different access and reporting mechanisms. Which ones to use depend on several factors such as the model of Cisco ASA.

The following are the recommendations for all Cisco ASA appliances:

- For maximum visibility, all Cisco ASA devices should be added to CS-MARS.
- If available, connect the management interface of the Cisco ASA appliance to the OOB management network or over a secured segment.
- Configure SSH access to be used by CS-MARS discovery. Limit the address of all hosts or network that have permission to gain administrative access to the appliance. Make sure the IP address of CS-MARS is added to the SSH access list. Remember to use modulus size of 768 at a minimum when creating the RSA key pair.
- Define an AAA administrative account and a local account to be used for CS-MARS access only. Specify the accounts privilege access level 15. The local account is to be used as a fallback in case AAA is not available. Ensure at all times the credentials of both accounts are synchronized with the device configuration in CS-MARS.
- Configure SNMP read-only access for the monitoring of system resources. Enforce an ACL to limit access to trusted systems. Make sure to add the IP address of CS-MARS as a trusted host. Use a strong community name.
- Enable system logging (syslog) with an informational security level. A severity level of informational is sufficient to capture session setups, teardowns, packet denies, and NAT transactions. A severity level of debugging may be rarely required, for example in case HTTP and FTP logs are needed (see note below). It is also a good practice to limit the rate at which system log messages are generated in high activity environments. This is done with the **logging rate-limit** command. Cisco ASA devices monitored in-band should also be configured with secure logging (SSL/TLS-based).



### Note

When enabling trap debugging, the debug messages contain the HTTP URL address information. Therefore, in CS-MARS you can create keyword-based rules matching against the firewall message itself. For example, if the debug messages are enabled and users were logging to <http://mail.cisco.com>, you could create keyword-based rules that matched against [mail.cisco.com](mailto:mail.cisco.com).

The following are the recommendations for Cisco ASA5580 appliances running software Version 8.1(1) or later, and for all other Cisco ASA platforms running Version 8.2(1) or later:

- Enable NSEL for the reporting of session activity (setup, teardown, and deny) and NAT transactions.
- Configure the **logging flow-export-syslogs disable** command to ensure no duplicate messages are sent to CS-MARS.

The following is an example of configuration for a Cisco ASA5580 running software Version 8.1(1). Note that x.x.x.x is the IP address of the CS-MARS appliance.

```
! Enables export of NetFlow security logging
flow-export enable
! Defines the interface, IP address and UDP port to be used for reporting to CS-MARS
flow-export destination management x.x.x.x 2055
flow-export template timeout-rate 1
! Disables redundant system logging messages
logging flow-export-syslogs disable
!
! Configures syslog logging at informational level
logging trap informational
```

```

! Enables secure logging
logging host management x.x.x.x TCP/1500 secure
logging enable
no logging console
logging buffered debugging
!
! SNMP Configuration
snmp-server host management x.x.x.x poll community <strong-community>
snmp-server community <strong-community>

```

NetFlow configuration on Cisco ASA software Version 8.1(2) and later has been enhanced to support the Modular Policy Framework. The following is a sample NetFlow configuration for Cisco ASAs running software Version 8.1(2) and later. For syslog and SNMP sample configurations, see the example provided above for software Version 8.1(1):

```

! Defines the interface, IP address and UDP port to be used for NetFlow logging to CS-MARS
flow-export destination inside x.x.x.x 2055
flow-export template timeout-rate 1
! Disables redundant system logging messages
logging flow-exports-syslogs disable

class-map flow_export_class
  match any
policy-map flow_export_policy
  class flow_export_class
    flow-export event-type all destination x.x.x.x
service-policy flow_export_policy global

```



#### Note

If you previously configured flow-export actions in Version 8.1(1) using the flow-export enable command, and you upgrade to a later version, then your configuration will be automatically converted to the new Modular Policy Framework flow-export event-type command. For more information, see the 8.1(2) release notes.

The following is an example configuration for Cisco ASAs running software Version 8.0 or earlier:

```

! Configures syslog logging at informational level
logging trap informational
! Enable secure logging
logging host management x.x.x.x TCP/1500 secure
logging enable
no logging console
logging buffered debugging

! SNMP configuration
snmp-server host management x.x.x.x poll community <strong-community>
snmp-server community <strong-community>

```

## Cisco IOS Devices

Cisco IOS routers and switches support different access and reporting mechanisms. The following are recommendations for all Cisco IOS devices, independently from their location:

- If available, dedicate an interface for control and management. Connect the interface to the OOB management network or over a secured segment.
- Configure SSH access to be used by CS-MARS discovery. Limit the address of all hosts or network that have permission to gain administrative access to the appliance. Remember to use modulus size of 768, at a minimum, when creating the RSA key pair. Configure the ACL applied to the management interface to allow SSH sessions from the IP address of CS-MARS.
- Define an AAA administrative account and a local account to be used for CS-MARS access only. Specify the accounts privilege access level 15. The local account is to be used as a fallback in case AAA is not available. Ensure at all times the credentials of both accounts are synchronized with the device configuration in CS-MARS.
- Configure SNMP read-only access for the monitoring of system resources. Use a strong community name. To enable the collection of resource usage data, you must ensure that the CPU and memory usage-specific events are logged by the reporting devices. Configure the ACL applied to the management interface to allow SNMP queries from the IP address of CS-MARS.
- If the Cisco IOS router is configured with Cisco IOS IPS, configure SDEE access to allow HTTPS connections from the CS-MARS appliance.

The following configuration fragment illustrates the commands used to enable CS-MARS to retrieve events from the Cisco IOS IPS software.

```
ip http secure-server
! Sets maximum number of concurrent subscriptions
ip sdee subscriptions 2
! Sets the maximum number of SDEE events that can be stored in the event buffer
ip sdee events 500
! Send messages in SDEE format
ip ips notify sdee
! Not to send messages in syslog format
no ip ips notify log
```

The following configuration fragment illustrates the SNMP configuration. Note *x.x.x.x* corresponds to the IP address of CS-MARS.

```
access-list 55 remark ACL for SNMP access to device
access-list 55 permit x.x.x.x
access-list 55 deny any log

snmp-server community csmars RO 55
snmp-server enable traps cpu threshold
snmp-server host x.x.x.x traps <strong-community> memory cpu
```

In the context of CS-MARS, NetFlow data is exported for two main uses, to identify any statistically significant anomalous behavior and to populate the data used for top *N* reports. While NetFlow data is valuable, its collection and export may consume resources on both network devices and CS-MARS. For this reason, choose wisely where to enable NetFlow:

- Preferably, enable NetFlow collection and export on network devices that aggregate traffic, such as campus distribution switches and data center core routers.
- Use NetFlow random sampling. Random sampled NetFlow provides NetFlow data for a subset of traffic in a Cisco router by processing only one randomly selected packet out of *n* sequential packets (*n* is a user-configurable parameter). Statistical traffic sampling substantially reduces consumption

of router resources (especially CPU resources) while providing valuable NetFlow data. For the purpose of CS-MARS, random sampled NetFlow provides the same quality of data needed to identify traffic anomalies and to be used for top *N* reports.

The following configuration fragment provides an example of sampled NetFlow collection.

```
ip flow-export version 5
ip flow-export source GigabitEthernet1/3
ip flow-export destination x.x.x.x 2055

flow-sampler-map csmars-sample
  mode random one-out-of 100
interface gig4/1
  flow-sampler csmars-sample
  ip flow ingress
```

Syslog provides invaluable operational information, including system status, traffic statistics and device access information. The following are the deployment recommendations:

- Enable syslog on all routers and switches.
- Do not log to the console.
- Enable syslog rate-limiting where available. The syslog rate-limiting limits the rate of messages logged per second, helping to ensure that syslog messages do not impact the CPU of either the sending device or CS-MARS.
- Use trap-level informational for those devices configured with ACLs or any other security features controlling passing traffic. Use trap-level critical for the rest. For example, configure informational level on campus switches enforcing ACLs and configure critical level for core routers.

The following configuration template illustrates the syslog configuration.

```
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging buffered
logging trap informational
logging host x.x.x.x
logging rate-limit all 10
logging source-interface <loopback or OOB-interface>
no logging console
```

## Deployment Table

Table 10-2 summarizes the access and monitoring protocol selections used in the Cisco SAFE design blueprint.

**Table 10-2**      *Deployment Model*

Place in the Network	Device and Function	Methods
Campus	Services ASA	SSH, NetFlow, syslog (no-redundant, informational), SMNP RO
	Services IPS	SDEE
	Campus IPS	SDEE
	Distribution Switches	SSH, Sampled NetFlow, syslog (critical), SMNP RO
	Access Switches	SSH, syslog (informational), SMNP RO

**Table 10-2**      **Deployment Model (continued)**

<b>Internet Edge</b>	ASA	SSH, NetFlow, syslog (no-redundant, informational), SNMP RO
	IPS	SDEE
	Border Routers	SSH, Sampled NetFlow, syslog (informational), SNMP RO
	Inner Switches	SSH, syslog (critical), SNMP RO
<b>WAN Edge</b>	WAN/VPN Edge Routers	SSH, Sampled NetFlow, syslog (informational), SNMP RO
	Distribution Switches	SSH, syslog (critical), SNMP RO
	IPS	SDEE
<b>Branch</b>	Router	SSH, syslog (informational), SNMP RO
	ASA	SSH, syslog (informational), SNMP RO
	IPS	SDEE
	Branch Switch	SSH, syslog (informational), SNMP RO
<b>Data Center</b>	ASA	SSH, NetFlow, syslog (no-redundant, informational), SNMP RO
	IPS	SDEE
	DC Core Switches	SSH, Sampled NetFlow, syslog (critical), SNMP RO
	DC Distribution	SSH, syslog (critical), SNMP RO
	DC Access	SSH, syslog (informational), SNMP RO
<b>Core</b>	Core Switches	SSH, syslog (critical), SNMP RO

## Analysis and Correlation

In the context of threat control and containment, CS-MARS is responsible for the correlation of event alarm and log information generated throughout the network to identify and timely mitigate threats. Such functions require certain level of network intelligence on the network topology, device configurations and traffic patterns. Network topology and device configuration is learned by CS-MARS as monitoring and mitigation devices are configured, or as a result of automatic network discovery (periodic SNMP-based discovery). CS-MARS also leverages Cisco NetFlow for network traffic profiling. CS-MARS uses the network intelligence to distinguish between a legitimate threats and false-positives, and to effectively reduce the volume of event data presented to the users.

## Network Discovery

CS-MARS gathers information on the network topology and device configuration as reporting devices are added to the web interface and as a result of an automatic network discovery. The automatic network discovery uses SNMP read-only access to discover and query the devices in the network. The network discovery can be programmed to run periodically, or can be run on-demand. As not all network devices would allow a SNMP-based discovery, Telnet (not recommended) and SSH are also leveraged in the network discovery. Information gathered by CS-MARS as a result of a network discovery includes IP addresses, IP routes, Layer-2 forwarding tables, NAT rules, access control lists (ACLs), and more.

To be more efficient, CS-MARS can be configured with the list of SNMP community strings and IP networks to target during the network discovery. This is configured in CS-MARS web interface, under **Admin > System Setup > Community Strings and Networks**. See [Figure 10-14](#).



**Figure 10-14 Automatic Discovery**

**Community Strings and Networks**

172.26.191.0/255.255.255.0(\*\*\*\*\*)  
 10.0.0.0/255.0.0.0(\*\*\*\*\*)  
 198.133.219.0/255.255.255.0(\*\*\*\*\*)

Community String:

☐ Network IP:

☐ Mask:

☐ IP Range:     -

226718

To control what networks are added to the network topology, a list of valid networks can be defined in CS-MARS web interface, under **Admin > System Setup > Valid Networks** (see [Figure 10-15](#)). Optionally, a SNMP target may be indicated for each network or IP range. The SNMP discovery process starts by querying the SNMP target (if one was defined).

**Figure 10-15 Valid Networks**

**Valid Network Addresses**

10.0.0.0/255.0.0.0(172.26.191.10)  
 198.133.219.0/255.255.255.0

SNMP Target:

☐ Network IP:

☐ Mask:

☐ IP Range:     -

Copyright © 2003–2008 Cisco Systems, Inc.  
 All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

226719

Finally, network discoveries can be scheduled for a particular time and day in the week, month, etc. This can be configured in CS-MARS web interface, under **Admin > System Setup > Topology/Monitored Device Update Scheduler**. See [Figure 10-16](#).

Figure 10-16 Topology Update Schedule

SUMMARYINCIDENTSQUERY / REPORTSRULESMANAGEMENTADMINHELP

System SetupSystem MaintenanceUser ManagementSystem ParametersCustom SetupMar 12, 2009 5:53:54 AM GMT

ADMIN | CS-MARS Standalone: pnmars v6.0Login: Administrator (pnadmin) :: Logout :: Activate

Topology/Monitored Device Update Scheduler

EditBackRun NowDeleteAdd

	Group Name	Schedule	Networks
<input type="checkbox"/>	Default Discovery Group	Run on demand only	n-10.204.0.0/14, n-192.168.188.16/29, n-10.200.2.128/25, n-10.208.12.0/30, n-192.168.160.112/29, n-192.168.1.0/30, n-10.56.0.0/21, n-172.26.180.0/22, n-172.26.191.0/24, n-172.26.190.0/23, n-172.26.146.0/23, n-10.0.0.1/8, n-10.242.10.6/31, n-192.168.34.1/32, n-64.104.10.112/30, n-10.240.50.0/24, n-10.208.15.0/30, n-192.168.160.120/29, n-10.201.1.240/28, n-64.104.10.0/24, n-10.201.2.241/32, n-10.208.16.0/30, n-192.168.33.0/29, n-10.201.2.0/28, n-10.208.13.0/30, n-10.242.10.4/31, n-10.242.10.8/31, n-10.208.18.0/30, n-64.104.20.0/24, n-64.104.10.124/30, n-192.168.0.0/30, n-10.200.1.128/25, n-10.201.1.0/28, n-10.201.1.16/28, n-192.168.144.0/29, n-10.242.10.2/31, n-10.208.11.0/30, n-10.240.10.16/29, n-172.26.170.0/23, n-10.200.1.0/25, n-10.201.2.16/28, n-192.168.144.8/29, n-10.200.2.0/25, n-10.208.10.0/30, n-10.208.17.0/30
<input type="checkbox"/>	SAFE-lab	Daily: 12:00 Midnight	n-10.0.0.0/8, n-198.133.219.0/24

1 to 2 of 225 per page

EditBackRun NowDeleteAdd

Copyright © 2003–2008 Cisco Systems, Inc. All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

226720

Data Reduction

One of the primary functions of CS-MARS is to analyze and correlate the alarm information gathered from the reporting devices to distinguish real threats from false-positives and to reduce the amount of data administrators need to pay attention to. This allows for the rapid identification and response to threats.

CS-MARS uses its network intelligence to determine the context and the relevance of an incident. By leveraging the contextual information, CS-MARS can determine if the target of an attack is in fact vulnerable to the attack. CS-MARS also leverages its topological awareness to identify the path followed by an attack, and to determine whether the target was reached or the attack was blocked by an intermediate device such as a firewall or and IPS.

The snapshot in Figure 10-17 illustrates a system determined false-positive. The incident was generated in response to a WWW IIS Unicode Directory traversal attack attempt. As the icon indicates, CS-MARS determined the incident as a false-positive because the offending session has been denied by an inline Cisco IPS.

Figure 10-17 System determined false positive

Incident ID: 40453163

Expand AllCollapse All

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	Tune
3	S:131998401, I:40453163	WWW IIS Unicode Directory traversal WWW WinNT cmd.exe Exec	10.240.100.2 17277	10.245.255.250 80	TCP	Mar 11, 2009 3:29:25 AM GMT	sfx12-ips4270-1/vs0			False Positive Tuning

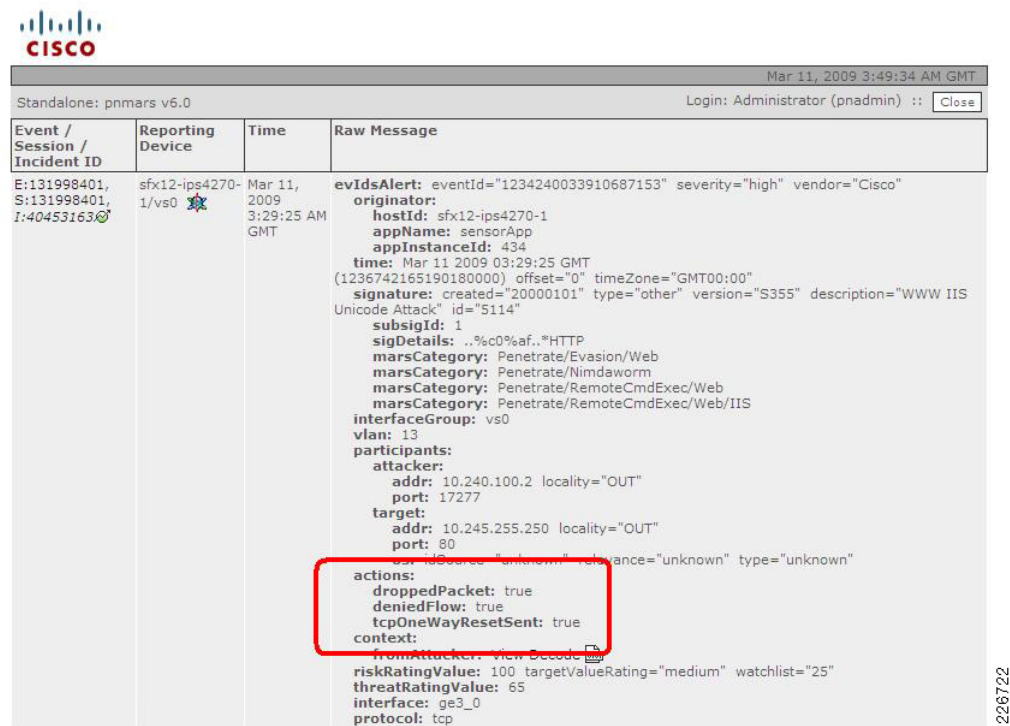
Copyright © 2003–2008 Cisco Systems, Inc. All rights reserved.

Summary :: Incidents :: Query / Reports :: Rules :: Management :: Admin :: Help

226721

This snapshot in Figure 10-18 confirms the Cisco IPS inline had successfully blocked the attack.

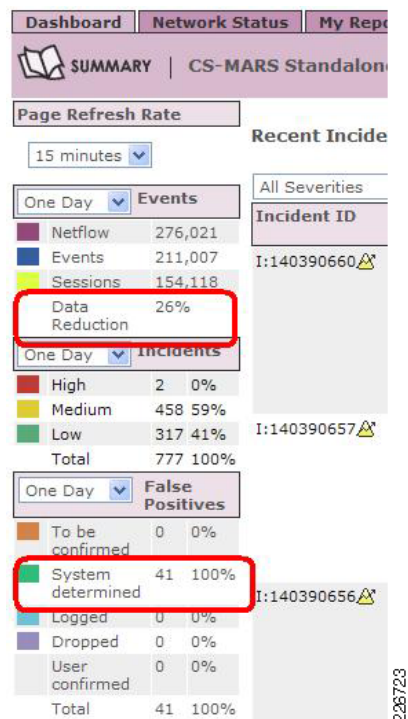
Figure 10-18 Security Incident Details



The screenshot shows the Cisco Security Incident Details page. The top bar includes the Cisco logo, the date and time (Mar 11, 2009 3:49:34 AM GMT), and the login information (Administrator (pnadmin)). Below the bar is a table with columns: Event / Session / Incident ID, Reporting Device, Time, and Raw Message. The first row shows an incident with ID E:131998401, S:131998401, I:404531636, reported from sfx12-ips4270-1/vs0 at Mar 11, 2009 3:29:25 AM GMT. The Raw Message column contains detailed event information, including eventId, severity, vendor, originator, hostId, appName, appInstance, time, signature, subSigId, sigDetails, marsCategory, interfaceGroup, vian, participants, attacker, target, actions, riskRatingValue, threatRatingValue, interface, and protocol. A red box highlights the 'actions' section, which includes 'droppedPacket: true', 'deniedFlow: true', 'tcpOneWayResetSent: true', and 'context:'. The incident ID is 226722.

Figure 10-19 shows the summary page. Highlight data reduction and determined false-positives.

Figure 10-19 Data Reduction



The screenshot shows the Cisco Security Summary page. The top bar includes the Cisco logo, the date and time (Mar 11, 2009 3:49:34 AM GMT), and the login information (Administrator (pnadmin)). Below the bar is a table with columns: Event / Session / Incident ID, Reporting Device, Time, and Raw Message. The first row shows an incident with ID E:131998401, S:131998401, I:404531636, reported from sfx12-ips4270-1/vs0 at Mar 11, 2009 3:29:25 AM GMT. The Raw Message column contains detailed event information, including eventId, severity, vendor, originator, hostId, appName, appInstance, time, signature, subSigId, sigDetails, marsCategory, interfaceGroup, vian, participants, attacker, target, actions, riskRatingValue, threatRatingValue, interface, and protocol. A red box highlights the 'actions' section, which includes 'droppedPacket: true', 'deniedFlow: true', 'tcpOneWayResetSent: true', and 'context:'. The incident ID is 226722.

## Attack Path and Topological Awareness

Thanks to its knowledge of the network topology and device configurations, CS-MARS is able to visualize the path attacks follow in the network. This allows CS-MARS to identify possible mitigation enforcement devices along the path, and to recommend the configuration command necessary to effectively mitigate the threat. Possible response actions are discussed in [Chapter 11, “Threat Control and Containment.”](#)

The screenshot in [Figure 10-20](#) illustrates CS-MARS correlation. In this case, the system was able to correlate several attacks from the same attacker system.



**Figure 10-20** Event Correlation

The screenshot displays the Cisco CS-MARS Standalone v6.0 interface. The top navigation bar includes tabs for SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, and HELP. Below this is a sub-navigation bar with tabs for Incidents, False Positives, and Cases. The main content area shows a table of recent incidents for the last one hour. The table has columns for Incident ID, Event Type, Matched Rule, Action, Time, Path, and Cases. The first incident (I:40453988) shows a sequence of events: WWW WinNT cmd.exe Exec, WWW IIS Internet Printing Overflow, TCP SYN Port Sweep, WWW IIS Unicode Directory traversal, and WWW IIS Internet Printing Overflow. The matched rule is 'System Rule: Server Attack: Web - Attempt'. The time is 'Mar 12, 2009 6:23:31 AM GMT - Mar 12, 2009 6:34:41 AM GMT'. The path is shown as a sequence of hops. The interface also includes a 'View' button and a 'Recent Incidents for Last' dropdown menu set to 'One Hour'.

Incident ID	Event Type	Matched Rule	Action	Time	Path	Cases
I:40453988	WWW WinNT cmd.exe Exec	System Rule: Server Attack: Web - Attempt		Mar 12, 2009 6:23:31 AM GMT - Mar 12, 2009 6:34:41 AM GMT		
	WWW IIS Internet Printing Overflow					
	TCP SYN Port Sweep					
	WWW IIS Unicode Directory traversal					
	WWW IIS Internet Printing Overflow					














































In the example shown in [Figure 10-21](#), anomalous activity included a reconnaissance TCP Port Sweep, and later followed by two targeted attacks, WWW IIS Unicode directory traversal attack, and WWW IIS Internet Printing Overflow.

Figure 10-21 Incident Detail

Incident ID: 40453988  

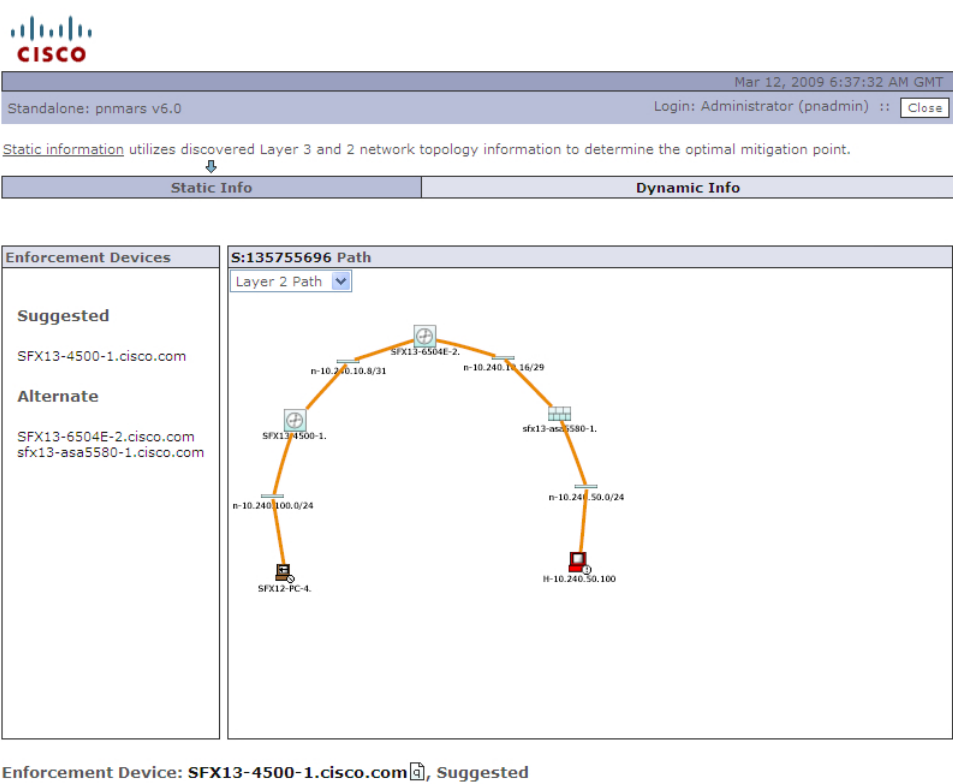
Expand All

Collapse All

Offset	Session / Incident ID	Event Type	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	Tune
1		TCP SYN Port Sweep 	10.240.100.2 	33869 	Total: 2					
1	S:135754169, I:40453988  	TCP SYN Port Sweep 	10.240.100.2 	42985 	10.240.50.100 	23 	TCP 	Mar 12, 2009 6:23:31 AM GMT	sfx12-ips4270-1/vs0 	 False Pos
1	S:135754270, I:40453988  	TCP SYN Port Sweep 	10.240.100.2 	33869 	10.240.50.100 	389 	TCP 	Mar 12, 2009 6:24:32 AM GMT	sfx12-ips4270-1/vs0 	 False Pos
2	S:135755696, I:40453988  	WWW IIS Unicode Directory traversal  	10.240.100.2 	1227 	10.240.50.100 	80 	TCP 	Mar 12, 2009 6:34:39 AM GMT	sfx12-ips4270-1/vs0 	 False Pos
2	S:135755697, I:40453988  	WWW IIS Internet Printing Overflow  	10.240.100.2 	1228 	10.240.50.100 	80 	TCP 	Mar 12, 2009 6:34:41 AM GMT	sfx12-ips4270-1/vs0 	 False Pos

Finally, CS-MARS network intelligence allowed it to reconstruct the attack path and identify possible mitigation points. See Figure 10-22.

Figure 10-22 Attack Path



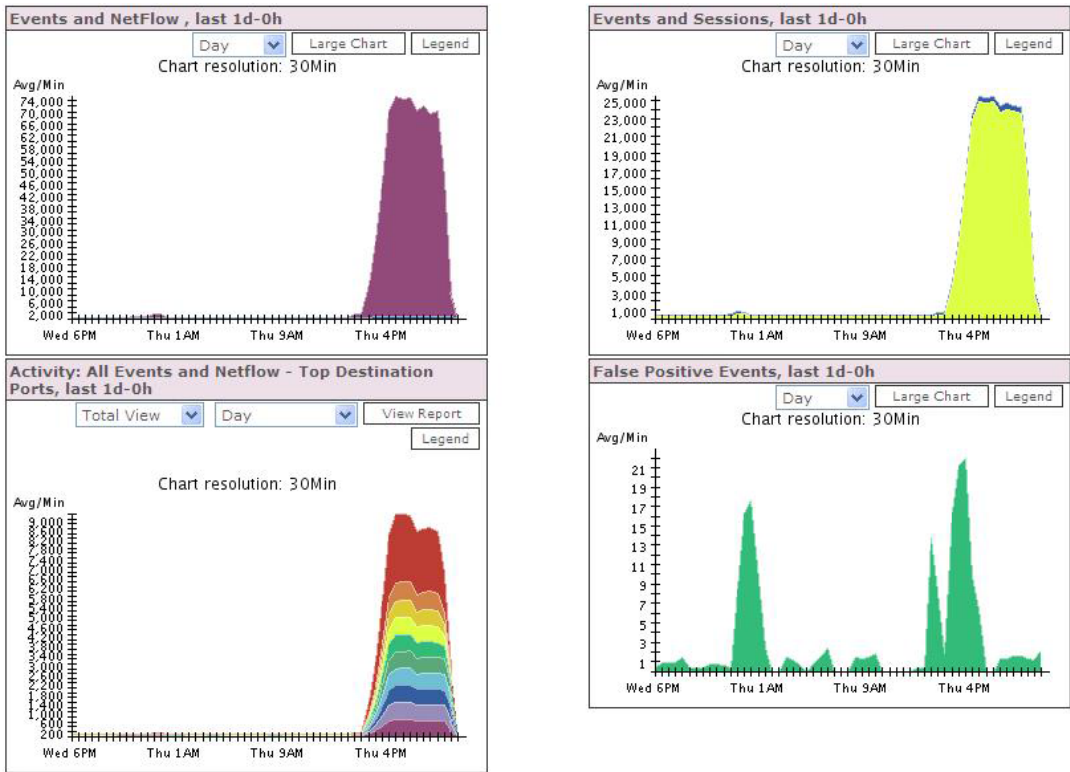
226726

NetFlow

As described earlier in chapter, CS-MARS is capable of leveraging NetFlow Versions 1, 5, 7 and 9 data to profile the network usage, detect statistically significant anomalous behavior, and to correlate anomalous behavior. This allows CS-MARS to leverage the network infrastructure to effectively identify anomalous behavior such as DDoS attacks and worm propagation.



Figure 10-23 shows a DDoS attack initiated in the lab testing Internet edge topology. The graphs indicate a sudden traffic surge.

Figure 10-23 Activity Graphs




The screenshot in Figure 10-24 provides more detailed information on the incident, including the attacker's IP address (198.133.219.128). It can be deduced that the attack consisted in a connection flood to multiple destinations on port 80 (HTTP).

Figure 10-24 Incident Details

Incident ID: 40437877  

Expand All Collapse All

Offset	Session / Incident ID	Event Type	Source IP / Port	Destination IP / Port	Protocol	Time	Reporting Device	Reported User	Path / Mitigate	Tune
3	5:45810168, 1:40437877, 1:40437876	Sudden increase of traffic to a port	198.133.219.128 0	N/A 80	IP	Feb 16, 2009 4:19:15 PM GMT	pmars			False Positive Tuning