National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme

Validation Report

Cisco Security Monitoring, Analysis and Response System (CSMARS) v5.2

(Cisco Security MARS 110 and 110R, Cisco Security MARS 210, Cisco Security MARS GC2, Software Version 5.2 (5.2.4.2487))

Report Number: **CCEVS-VR-VID10181-2008**
Dated: **August 7, 2008**
Version: **1.2**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, Maryland 20899

National Security Agency
Information Assurance Directorate
9600 Savage Road Suite 6757
Fort George G. Meade, MD 20755-6757

Acknowledgements:

The TOE evaluation was sponsored by:

Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95124-1706
USA

Evaluation Personnel:
Arca Common Criteria Testing Laboratory
Abdul Qayyum
Rick West

.

Validation Personnel:
Robin Medlock, The MITRE Corporation
Jandria Alexander, The Aerospace Corporation

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco CSMARS Version 5.2. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of the Cisco CSMARS Version 5.2 was performed by the Arca Common Criteria Testing Laboratory (CCTL) in the United States and was completed during July 2008. The information in this report is largely derived from the Security Target (ST), written by Cisco Systems, Inc. and the Evaluation Technical Report (ETR) and associated Evaluation Team Test Report, both written by Arca CCTL. The evaluation team determined the product to be CC version 2.3 Part 2 extended and Part 3 conformant, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 2 have been met.

The TOE consists of hardware and software used to provide an intrusion detection analyzer solution, hereafter referred to as the TOE. This ST is modeled after the Intrusion Detection System Analyzer, Protection Profile, April 27, 2005, Version 1.2 and describes Cisco product features that satisfy several key security functional and assurance requirements identified in the Protection Profile. The CS MARS purpose is to identify, isolate and recommend precise removal of offending elements. Please note, however, that the ST does not claim Protection Profile compliance.

The TOE hardware consists of Local and Global Controllers running version 5.2 of the CS MARS (Monitoring, Analysis, and Response System) software. Please refer to the installation guide for appropriate certified image as csmars-5.2.4.2487.iso; henceforth referred to as version 5.2. The TOE is configured to operate in one of two evaluated configurations: a local or a global configuration.

Figures 1 and 2 show the evaluated TOE network configurations. These configurations are further described in Section 2 of this Security Target. The administrator must determine which configuration will apply prior to deploying the TOE.

NOTE: *The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.*

The TOE can perform notification actions in the case of incident identification, including emails and pages to immediately notify a human user of an existing problem which requires attention. These notifications are outbound communications only and once sent are out of the boundary and control of the TOE. All notification communication should be over the management network connection.

Caution: It should be noted that some of the sensor devices supported by the TOE use non-secure protocols (HTTP, Syslog, SNMPv1, OPSEC-LEA, OPSEC-CPMI, POP, MS-RPC, SQLNet) for raw data transfer to the TOE.

The authorized administrator must ensure that appropriate measures are taken in the IT Environment to protect this data in transit (OE.INTEGR).

When non-secure protocols are used to collect events from a sensor, it is the IT Environment that must provide protected networks to protect the transmitted data. The sensor and alert notification data can be protected while in transit to and from the TOE by use of physical isolation or cryptographic means. Wherever network segments cannot be secured physically, network

segments between remote devices and the MARS sensor interface can be secured by use of encrypted tunnels, where both end-points of such tunnels would be entirely implemented by the IT Environment, and not by MARS. For additional security both could be used.

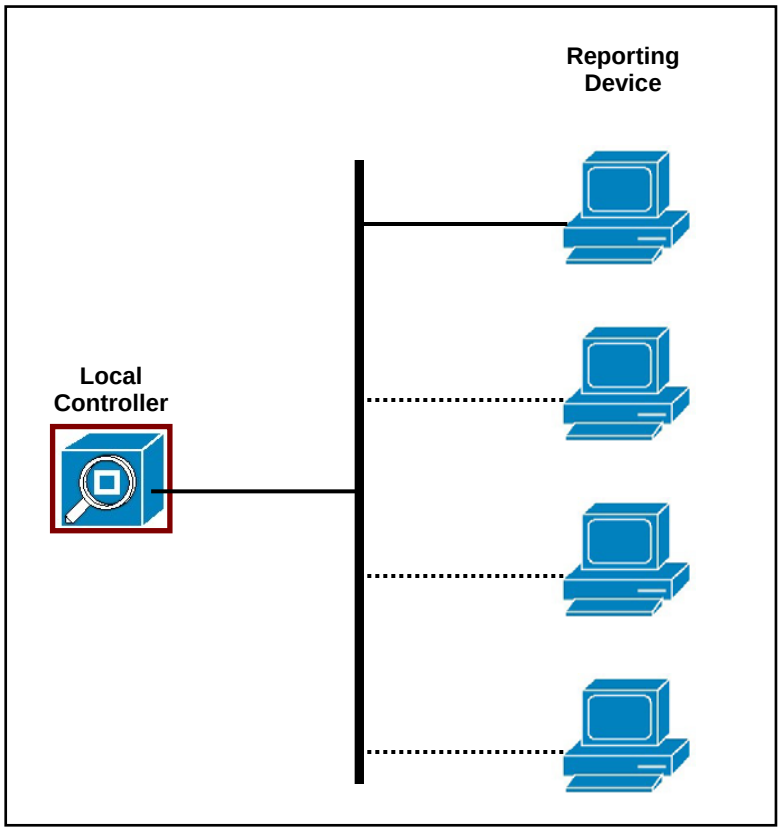

Figure 1: Typical TOE Configuration with a single Local Controller

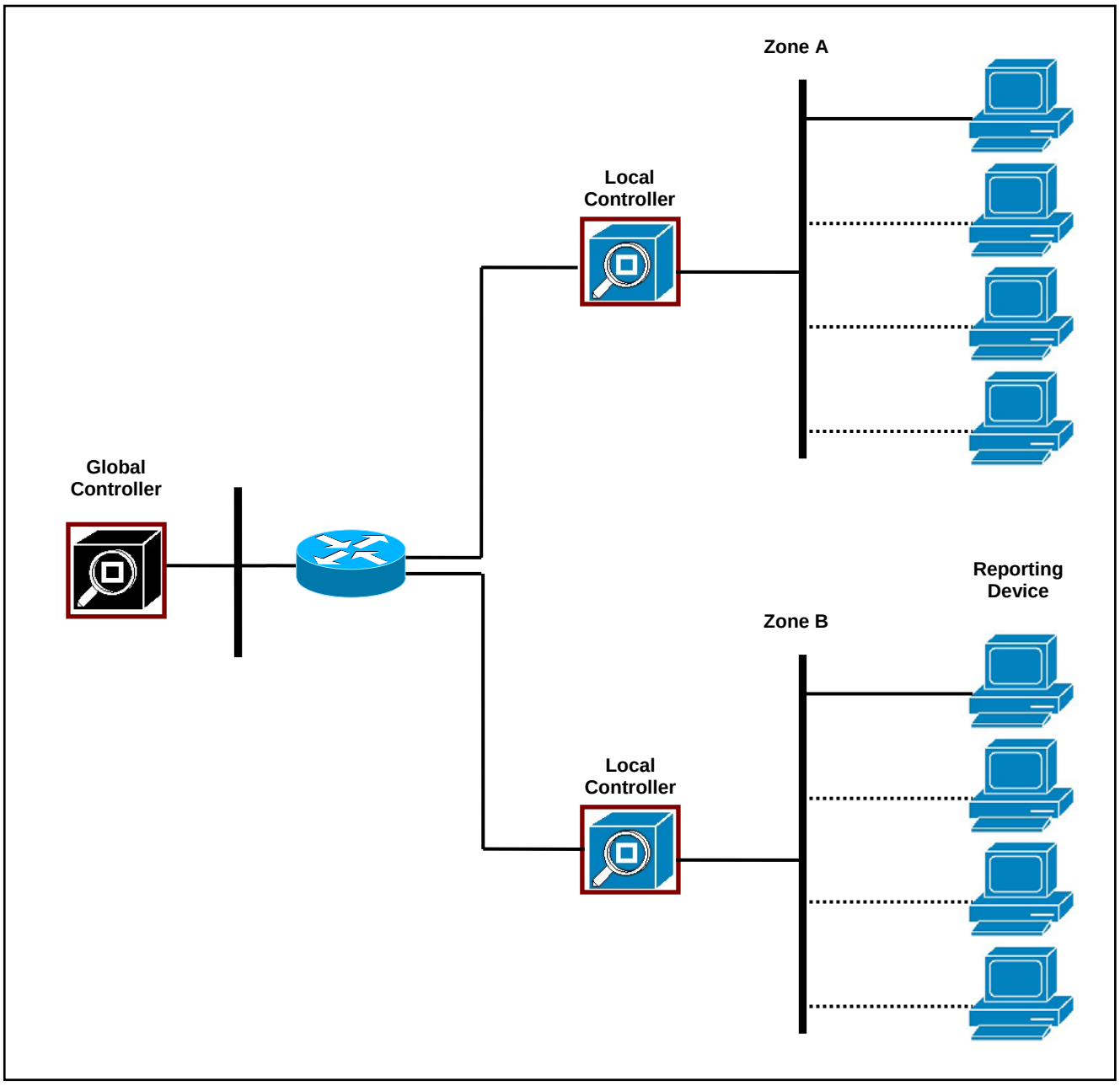

Figure 2: Typical TOE Configuration with one Global-Controller and multiple Local-Controllers

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the Common Evaluation Methodology (CEM) work unit verdicts), and reviewed successive versions of the ETR and test report.

The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 2 evaluation.

Therefore the validation team concludes that the Arca CCTL findings are accurate and the conclusions justified.

2 Identification

The CCEVS is a National Security Agency (NSA) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) or candidate CCTLs using the CEM for EAL 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns validators to monitor the CCTLs and candidate CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's NIAP Validated Products Listing.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Cisco CSMARS Version 5.2 (Cisco Security MARS 110 and 110R, Cisco Security MARS 210, Cisco Security MARS GC2, Software Version 5.2 (5.2.4.2487))
Security Target	Cisco CSMARS Version 5.2, Security Target, version 7.0, dated July 9, 2008

Item	Identifier
Evaluation Technical Report	• ASE (Security Target Evaluation): ASE Evaluation Technical Report for Cisco CSMARS Version 5.2, document version 7.0, released July 10, 2008. • ACM_CAP.2 Evaluation Technical Report for Cisco CSMARS Version 5.2, document version 6.0, released April 30, 2008. • ADO_DEL.1; ADO_IGS.1 Evaluation Technical Report for Cisco CSMARS Version 5.2, document version 6.1, released July 10, 2008. • ADV_FSP.1; ADV_HLD.1; ADV_RCR.1 Evaluation Technical Report for Cisco CSMARS Version 5.2, document version 6.0, released April 30, 2008. • AGD_ADM.1; AGD_USR.1 Evaluation Technical Report for Cisco CSMARS Version 5.2, document version 6.1, released July 10, 2008. • ATE_COV.1; ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for Cisco CSMARS Version 5.2, document version 6.0, released April 30, 2008. • AVA_VLA.1; AVA_SOF.1 Evaluation Technical Report for Cisco CSMARS Version 5.2, document version 6.0, released April 30, 2008.
Protection Profile	None
Conformance Result	CC Part 2 extended and CC Part 3 conformant, EAL 2
Applicable interpretations and precedents	▪ PD-106: Situations Where AGD_USR May Be Vacuously Satisfied
Sponsor	Cisco Systems Inc. 170 West Tasman Drive San Jose, CA 95124-1706
Common Criteria Testing Lab (CCTL)	SAVVIS Communications Arca Common Criteria Testing Laboratory NVLAP Lab Code 200429 45901 Nokes Boulevard Sterling, VA 20166
CCEVS Validator(s)	Robin Medlock The MITRE Corporation 7515 Colshire Drive McLean, VA 22102 Jandria Alexander The Aerospace Corporation 6940 Columbia Gateway Drive, Suite 400 Columbia, Maryland 21046-2877

3 Security Policy

3.1 Identification and Authentication Security Function

All user interfaces to the TOE require identification and authentication. Identification and authentication is carried out by entering a user identifier and a password. The identification and authentication of users establishes the authorizations and the role (Admin, Security Analyst, or Operator) a user has on the TOE. Users that are set up as being part of the Notification role are not allowed to authenticate to the TOE, so they can not gain access into the TOE. The Notification Role is considered a non-user role.

The user interfaces to the TOE are a web based interface and a command line interface (CLI). The web based interface requires the user to be authenticated before allowing any other actions on behalf of that user. Only after users have successfully identified and authenticated themselves through the web interface will the TOE present the features and capabilities that may be used through this interface.

The CLI is accessible through a serial console interface along with being reachable thru SSHv1 or SSHv2. The CLI is used for initial configuration and setup of the TOE. The CLI requires users to supply a user identifier and a password before they are allowed to carry out any other actions with the TOE. Only users that log in as the Admin role may use the CLI. Further, the CLI is only accessible to the user “pnadmin”, which operates in the Admin role. The user “pnadmin” is a default defined account for carrying out administration of the TOE through the web or CLI interfaces.

The Strength of Function for the password authentication is SOF-basic.

3.2 External Device Communication Security Function

For the TOE to carry out its analysis activities and to detect intrusions on specified networks, it needs to collect data from sensors that are on the networks to be monitored and analyzed for intrusions. These network devices are referred to as sensors. Sensors are the networking devices through which data passes, is collected, and processed, for those networks that are to be monitored and analyzed for intrusions. Sensors are routers, switches, security devices, and network applications (such as firewalls, intrusion detection systems, vulnerability scanners, and antivirus applications), hosts (such as Windows, Solaris, and Linux syslogs), and other applications (such as databases, Web servers, and authentication servers).

In the CS MARS web interface, the administrator configures the sensors so that the TOE can discover their settings and collect data. The administrator needs to define the device. The TOE is then able to match the true reporting IP address to that of a known reporting device type. By knowing the sensor type, the TOE can correctly collect and parse the raw event data. Refer to Table 2-2 of Local Controller User Guide for sample data available from network device types.

Communication with the external devices involves health query messages (using the SNMPv1 protocol) to ensure the devices are still operational as well as raw data collection from the sensors. This is the data that becomes analyzed TOE data. The data is collected using several different communication mechanisms; the communication mechanism used depends on the type of sensor involved. Sensor events collected by the TOE are parsed by the Cisco written CS-MARS parser and the data obtained is stored in a small number of fields in the database. These fields have defined data types and cannot store arbitrary or binary data. These fields are generally very small with a maximum size of less than 100 characters. Information that is malformed or does not satisfy the parsers strict proprietary format is dropped.

Configuration retrieval protocols are used by the TOE to pull configuration data from the sensor. Sensors do not push configuration information to the TOE. Raw data is pushed to the TOE via syslog and SNMP traps with a few exceptions where the TOE pulls raw data from the sensors. Data collected by the TOE is identified within the TOE by its originating host, the date and time of collection, the device type, and the event type.

3.3 Administration Security Function

Administration functions for the TOE are accomplished through the use of a web interface management GUI and a management CLI. Communications through these mechanisms use established communication protocols for request transfer to command the TOE for configuration and maintenance. Administrative requests generated via the web interface management GUI are transmitted via HTTPS as a secure communication channel that protects the confidentiality and integrity (detection of modification) of the administrative commands. If the integrity of any of the HTTPS communications is compromised, the TOE will drop the networking packets that are corrupt, based on the fact that the MAC is incorrect, and request a resend of the dropped packet. The TOE will not accept any packet where the MAC is incorrect. The CLI is used to carry out initial administrative configuration of the TOE. The web interface management GUI is used for operational administration of the TOE once in the evaluated configuration.

Data from the TOE is made available to those connecting to the TOE through the web interface as long as the user is using Internet Explorer and the workstation from which the user is connecting to the TOE has a routable connection to the TOE.

Administrative access permissions are defined by the role associated with the user. The user roles defined for the TOE are Admin, Security Analyst, and Operator. The Notification Role is considered a non-user role. The Admin role performs all tasks associated with the Administration Security Function as stated in the FMT requirements. The Security Analyst is able to perform a subset of those tasks, as indicated in FMT_MTD.1(2) and FMT_MTD.1(3). Notification roles have no interactive access to the TOE.

- **Administrator (Admin Role):** users operating in the Admin role may carry out all administrative operations.
- **Security Analyst (User Role)**: users operating in the Security Analyst role may only carry out the administrative operations of defining user accounts of users that operate in the Notification role and defining alerts for rules.
- **Operator** role (**User Role)**: users operating in the Operator role may only view configurations of the TOE and do not have any other administrative capabilities except to modify their own identification information maintained by the TOE.
- **Notification** role (**Non-User Role**): users operating in the Notification role may not authenticate to or access the TOE or carry out any administrative capabilities. Those with the Notification role may only receive alerts.

The roles are organized such that the Security Analyst has all capabilities of the Operator, plus what is described above. The Admin has capabilities of the Operator and the Security Analyst plus the Admin may carry out all administrative operations.

3.3.1 User Account Administration

The TOE has the ability to accept user configuration requests via a web interface. A user is any person who has interactive access to the TOE. Users have associated qualifying attributes that uniquely define them; these attributes are a combination of name, authentication identifier, password, email, role, organization, and group. The Notification role is a non-user role and has no access to TOE resources. People in the Notification role may receive notification alerts only.

The administrative actions for users include adding, deleting, and modifying users, and any of their associated attributes. Included in these actions is the ability to define the authentication identifier, password, role, and group of each user. The Admin role is granted the ability to add and delete users of any role type, as well as modify an existing user's critical attribute information, such as authentication identification, role, and group. Both the Admin role and a user without regard to its role are able to modify non security relevant identifying information such as organization, email, and phone number of that specific user once the user has been created.

3.3.2 System Time Administration

The management CLI interface allows the Admin role to initialize and modify the system time. Only the Admin role has access to CLI functionality. Further, the CLI is only accessible by using the pre-defined "pnadmin" user account that operates in the Admin role.

3.3.3 Sensor Administration

The analyses function of the TOE relies on the network devices and sensors chosen to be monitored. These sensors can be added only by a user operating in the Admin role. The sensors from which data are collected can be configured through the GUI interface, or by using a seed file that contains the required parameters for each element, or by automatic topology discovery to locate all the sensing devices in a defined network segment.

The parameters required to establish a device or a sensor are the device name or IP address, the device type, its access and reporting IP addresses, and communication access type with any required authentication information. Sensors can be added, edited, and deleted by a user operating in the Admin role. All configured monitored element information is readable by all roles with web interface access.

3.3.4 Analyses Rule Administration

Data collected from the sensors is analyzed according to a set of analysis rules that define and identify suspect traffic flow behavior, potential security incidents, and intrusions. Rules can be added, edited, and duplicated, as well as having the status of individual rules toggled between active and inactive using the web management GUI. Parameters of rules include the source and destination IP address, the sensor, the event, the severity, and any actions to be taken such as emails or pages when the rule is violated. The Admin role is granted access to rule addition, modification, and deletion. All user roles granted access to the TOE may view any of the rules.

3.3.5 Audit Administration

The auditing capabilities of the TOE are administered through users operating in the Admin, Security Analyst, or Operator role through the web interface to the TOE. Users operating with the Admin, Security Analyst, or Operator role are allowed to read the audit trail of the TOE.

Audit records contain the date and time of record generation, the source of the record, and a corresponding text message. All records are displayed according to date and time, from most recent to least recent, inclusive of the requested time frame.

3.4 Reporting Security Function

The TOE supports the ability to query analysis results through the web interface. Users operating in the Admin, Security Analysts and Operator roles all have read access to the reports. Analysis results are queried using time, a source and destination IP, a communication service (TCP, UDP, IP, etc), an event type, a device, a user, a keyword, an operation, a rule, and an action. These values can be edited with specific values to fine tune an event search, or may be left as generic, all-encompassing values.

Queries are displayed through the web interface to the TOE according to a predefined report format. The result contents displayed are contingent on the report format chosen. The content of the displayed results includes record parameters such as the date and time of the record, a corresponding incident id, the event type, the resulting action, and any policy rule that triggered the event. User with query access can also define new report formats with customized data result columns. Queries can be saved as report generators with user-defined timed execution and a list of report recipients.

3.5 Analysis Security Function

The TOE performs internal analysis on data that it collects from sensors to identify unusual or suspect activity (security incidents, intrusions, and events) within a network. Analysis of data by the TOE combines security event monitoring with network intelligence, context correlation, vector analysis, and anomaly detection.

The TOE protects all event data and ensures the availability of the event data. The TOE protects the event data through the use of its roles and requiring all users to successfully identify and authenticate themselves before carrying out any other operation dealing with modification or configuration of any functions that may affect the event data or the availability of that data. Further, the TOE will ensure that all event data that has been saved to the hard drive of the TOE is made available and is protected, regardless of if the hardware resources storing the event data become exhausted or are attacked. When the hardware resources storing the event data become exhausted, the TOE will overwrite the oldest stored event data and send an e-mail alarm to a configured e-mail address indicating that the storage capacity has been reached.

3.5.1 Data Analysis

The TOE relies on information generated and gathered from selected sensors such as routers, switches, VPN concentrators, firewall applications, and endpoint devices. The configurations of these components, as well as their security policies, are used to model the traffic flow in the network. The TOE collects or receives the data from their sources through uploading of logs, alerts, and Netflow communications from the routers to perform analysis in search of abnormal system traffic.

The TOE processes incoming data containing security relevant information and combines them into a lesser number of categorized events. Through the processes of context correlation and vector analysis, these events are then grouped together to identify incidents using system and user defined rules for analysis. Data matched against a rule definition indicates a recognizable event and is categorized according to severity and possible recovery action.

3.5.2 Incident Viewing and Selection

Incidents are viewed through the web interface to the TOE. Incidents are retrieved according to search criteria submitted through the web interface. Each recorded event contains a unique incident identifier, the date and time of discovery, a severity indicator of green, red, or yellow, the system or user rule that the data matched to identify the event, an action, and the detected path the data traveled. Incidents can be selectively viewed by their severity level, or rule name, or both.

Graphs of activity are supplied to visually summarize event activity over an elapsed period of time. The viewable summary data on these graphs can be selected by time period, ranging from an hour to a year in incremental time. Some of the visual representation presented indicates the events collected through Netflow, and the number of false positive indicators.

3.6 Reaction Security Function

When the TOE detects an actionable event through analysis of the sensors' data as applied to the active rules, an incident record is created. Rules may have associated actions that alert

human users of the incident, such as sending an email or page to certain users or groups of users indicating the alarm. Administrators and Security Analysts may configure alerts for defined rules.

3.7 Audit Security Function

The TOE's Audit Security Functionality provides event auditing and audit viewing for system functions and management functions.

3.7.1 Management of Auditing

The management auditing of the TOE records, in the audit trail, the completion of system management events submitted through the web interface. These events include system login attempts and results, changes in users (including addition, modification, and removal), and modifications to saved queries, rules, or actions as indicated by a database modification event. Each event contains a date and time of occurrence, the name of the system user, and a text message describing the management action.

Management of audit data when the database, which includes the audit trail, becomes exhausted (the database, audit trail, is within 2.5% of filling up) is done by purging the oldest stored audit records to make room for the current audit records being generated. When the utilized audit trail reaches 2.5% of filling up, an alarm is sent in the form of an e-mail to a configured e-mail address.

3.7.2 Audit Data Viewing and Selection

Audit data, resulting from interactions with the TOE, is viewed through the audit trail via the web interface to the TOE. The data displayed contains the date and time of the event, the user id that generated the event, and a text message containing the location of the event (Web or CLI), and details describing the originating action.

The data is retrieved according to the elapsed time in days, hours, and minutes, or the year, month, day, hours, and minutes selected through the web interface. Selection is also made based on the user level to be queried. User levels are defined as all, group names, individual users, and a category titled "inactive". The user roles of Admin, Security Analyst, and Operator all have access to audit data for review. The audit events are displayed by date and time, from the earliest event to the most recent.

3.8 Self Protection Security Function

The protection mechanisms employed by the TOE ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. The CSMARS does not allow any TSF-mediated actions to occur unless the user has been successfully identified and authenticated. The TOE mediates all actions occurring over its management interfaces. Communication at the web interface is protected using SSLv2 or SSLv3, and at the CLI using SSHv1 or SSHv2.

The self-protection function is responsible for providing an execution domain that is protected from interference and tampering by unauthorized users. The TOE is a hardware device that executes all of its processes internally. It is accessible only via the defined interfaces, and only authorized users are able to modify the functionality of the TOE. The external communication interface (the interface that collects data from routers, switches, firewalls, and Windows systems and other sensors) enforces domain separation in that any data collected by this interface for use by the TOE is logically separated from all other TOE data while being collected and analyzed for intrusions. The data collected through the external communication interface is only used for analysis and has the analysis rules applied to the collected data; this data is never executed. Data collected by the TOE is subject to the policies as defined by the authorized users. At all physical interfaces, the TOE intercedes to ensure domain separation. Traffic can only come into

the TOE via three physical interfaces: the Serial Port (which is used only during initial setup and configuration of the TOE), the ETH1 interface (which is solely used for administrative purposes), or ETH0 (which is the interface where data is collected for analysis by the TOE and which can also allow for secure administrative and authorized user communications). The collected data and/or unauthorized users cannot bypass the identification and authentication mechanisms, preventing interference and tampering by untrusted subjects, thereby maintaining a domain for its own execution.

Global and local controllers communicate using SSLv2 or SSLv3. Global controllers control, configure, and collect data from local controllers.

4 Assumptions

The specific conditions listed in Table 2 are assumed to exist in the TOE's IT environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE. They are classified as to whether they apply to personnel security, physical security, or to the IT environment.

Table 2: TOE Assumptions

Name	Assumption	Area
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions	IT Environment
A.INTEGR	An authorized administrator will ensure that administrative guidance is properly implemented in the IT environment to protect event and notification data in transit.	IT Environment
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.	Physical
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	Physical
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.	Personnel

Name	Assumption	Area
A.NOEVIL	The authorized administrators are not careless, wilfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.	Personnel
A.NOTRST	The TOE can only be accessed by authorized users.	IT Environment

5 Architectural Information

The CS-MARS 5.2 TOE is a hardware and software solution which is comprised of the following hardware and software components:

- Hardware: Cisco Security MARS 110 *or* 110R *or* 210, and optionally Cisco Security MARS GC2 (with two or more 110, 110R or 210 components)
- Software: MARS Operating System version 5.2 (5.2.4.2487)

6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor):

Table 3: Evaluation Evidence

Assurance Requirement	Title(s)
ACM_CAP.2	Cisco CSMARS Version 5.2, Configuration Management Documentation, version 10.0, July 9, 2008
ADO_DEL.1	Cisco CSMARS Version 5.2, Delivery Documentation, version 6.0, July 9, 2008
ADO_IGS.1	Cisco CSMARS Version 5.2, Installation, Generation, and Start-up documentation, version 7.0, dated July 9, 2008
ADV_FSP.1	Cisco CSMARS Version 5.2, Functional Specification, version 7.0, July 9, 2008
ADV_HLD.1	Cisco CSMARS Version 5.2, High Level Design, version 6.0, July 9, 2008
ADV_RCR.1	Cisco CSMARS Version 5.2, Representation Correspondence, version 6.0, July 9, 2008
AGD_ADM.1	Cisco CSMARS Version 5.2, Administrative Guide, version 7.0, July 9, 2008
AGD_ADM.1	User Guide for Cisco Security MARS Local Controller, Release 5.2.x May 2007
AGD_ADM.1	User Guide for Cisco Security MARS Global Controller, Release 5.2.x May 2007
AGD_ADM.1	Cisco CSMARS Version 5.2, User Guide (for Operator and Security Analyst admin roles)
AGD_USR.1	As all users of the TOE are Administrative in nature. No user guidance is provided for this product as there are no non-administrative users (PD-0106). This work unit is vacuously satisfied.
ATE_COV.1	Cisco CSMARS Version 5.2, Test Coverage, version 5.0, July 9, 2008
ATE_FUN.1	Cisco CSMARS Version 5.2, Test Coverage, version 5.0, July 9, 2008
ATE_IND.1	*Cisco_CSMARS_v5.2_EAL2_CCTL_Team_Test_Plan_v5.0_102907.doc*

Assurance Requirement	Title(s)
AVA_SOF.1	Cisco CSMARS Version 5.2, Strength of Function Documentation, version 3.0, October 9, 2007
AVA_VLA.1	Cisco CSMARS Version 5.2, Vulnerability Analysis Documentation, version 6.0, July 9, 2008
ASE	Cisco CSMARS Version 5.2, Security Target, version 7.0, July 9, 2008

The following is the list of other non-proprietary evaluation evidence provided by the sponsor:

- Cisco CSMARS Version 5.2, Installation, Generation, and Start-Up Documentation, version 7.0, July 9, 2008
- Install and Setup Guide for Cisco Security MARS , Release 5.x, September 2007
- Cisco CSMARS Version 5.2, Administrative Guide, version 7.0, dated July 9, 2008
- Cisco CSMARS Version 5.2, Security Target, version 7.0, dated July 9, 2008
- Cisco CSMARS Version 5.2, User Guide (for Operator and Security Analyst admin roles)
- User Guide for Cisco Security MARS Global Controller, Release 5.2.x May 2007
- User Guide for Cisco Security MARS Local Controller, Release 5.2.x May 2007

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team.

7.1 Developer Testing

The developer performed a testing and coverage analysis, which examined a subset of SFRs and developed one or more Cisco test cases that verified the function or command requirement. These tests were documented in the EAL2 Detailed Test Plan. The scope of the developer tests included all TOE Security Functions. The developer also tested all of the models that are part of the evaluation.

The developer testing addresses the following security functionality claimed by the TOE: audit generation and recording; identification and authentication mechanism; ability of the administrators to carry out management functions; functionality of the sensor to collect, analyze, and react to network traffic systems data; set time; and create users.

There are 14 different test sets performed by the developers. These test-sets tested different TSFIs and SFRs (or a subset of SFR). Some of these test sets have multiple tests in them, and some are representing a single test. The test sets are run using either CLI commands or GUI by executing certain functions as defined in the SFRs being tested, and then verifying that the function actually was executed by checking the audit log and by checking the actual result of the test (depending on the SFR function being tested). For example, if wrong user credentials were provided to log in to the TOE, in addition to an audit log being generated and logged, the actual result was TOE denied access.

The evaluation team determined that the developer's test methodology met the coverage requirements and that the actual test results matched the expected results.

Table 4: Vendor Test Mapping of TSF to External Interfaces to SFR

TOE Security Function	External Interface	TOE SFR
• Audit	• Command Line Interface	• FPT_STM.1
• Administration • Identification and Authentication • Reporting	• Administrative Web Interface	• FAU_GEN.1 • FAU_SAR.1 • FIA_UID.2 • FIA_UAU.2 • FMT_MOF.1 • FMT_MTD.1(1) • FMT_SMF.1 • FMT_SMR.1 • IDS_RDR.1
• Administration	• Administrative Web Interface • Inbound NetFlow Interface	• FMT_SMF.1
• External Device Communication (syslog only) • Reporting (admin web only) • Analysis • Self Protection	• Administrative Web Interface • Inbound Syslog Interface	• IDS_SDC.1 • IDS_STG.1 • IDS_ANL.1 • IDS_RDR.1 • FPT_SEP.1
• Reaction	• Administrative Web Interface • Outbound Alarm/Notification Interface	• IDS_RCT.1

7.2 Evaluation Team Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addresses the security functions as described in the functional specification. This was done through completing an analysis to verify correctness of test sets mapped to TSFI & SFRs and by re-running a subset of the vendor testing confirming that results generated match with the actual results provided by developer. In addition to this, the evaluation team performed its own independent testing to verify some functions tested by the developer, and to test some functions either not tested or not directly tested by the vendor test sets.

The evaluation team performed a sample of the developer's test suite, and devised an independent set of team tests and penetration tests. The evaluation team reran a subset of the developer's test suite that tested 5 of the 7 TSFs, and 14 of the 31 SFRs. The functions tested through rerun include

- audit generation and recording,
- identification and authentication mechanism,
- ability of the administrators to carry out management functions,
- functionality of the sensor to collect,

- analysis of network traffic systems data (raw data),
- time set, and
- protection of communication channel for administrative sessions

The evaluation team also performed a penetration flaw hypothesis analysis of the product to prepare for a penetration testing effort. The analysis examined each SFR to determine whether it was possible that the evaluated configuration could be susceptible to vulnerability. The specific penetration tests executed include the following:

- Used a port scanner to check for open ports and run vulnerability testing against those ports on the TOE (LC-110 and GC2)
- Checked that TOE does not allow any non-encrypted communication (HTTP and Telnet) to the TOE Management interfaces (GUI and CLI)
- Checked that the TOE hides/masks all use of password by any means (GUI, CLI, Console) and that the actual password cannot be seen though eavesdropping
- Checked that the TOE does not allow access to any of its Management Interfaces (GUI, CLI, Console) without proper I&A performed and successfully completed first

The evaluation team constructed and ran each of the identified tests. The results of the penetration test execution verified that none of the hypothesized flaws was exploitable.

8 Evaluated Configuration

The evaluated configuration of the TOE includes two types of deployments (see Figures 1 and 2 in this document). The TOE can consist of only one Local Controller, or it can be a Global Controller with multiple Local Controllers. All the models run the same software image and version. These models only differ in hardware configuration and throughput, and do not affect how the security functions specified in the ST are met.

Table 5: TOE Hardware Models and Part Numbers

Model Name	Part Number
Cisco Security MARS 110	CS-MARS-110-K9
Cisco Security MARS 110R	CS-MARS-110R-K9
Cisco Security MARS 210	CS-MARS-210-K9
Cisco Security MARS GC2	CS-MARS-GC2-K9

The evaluated configuration was tested in the configuration identified in Figure 3, below. The evaluation results are valid for all configurations of CSMARS v5.2 appliance identified in Table 5.
Note: The evaluated configuration used physical protection of the environment to address OE.INTEGR, “Those responsible for the TOE must ensure that appropriate measures have been taken in the environment to protect from modification the sensor and alert data while in transit to and from the TOE by use of physical isolation of cryptographic means”.

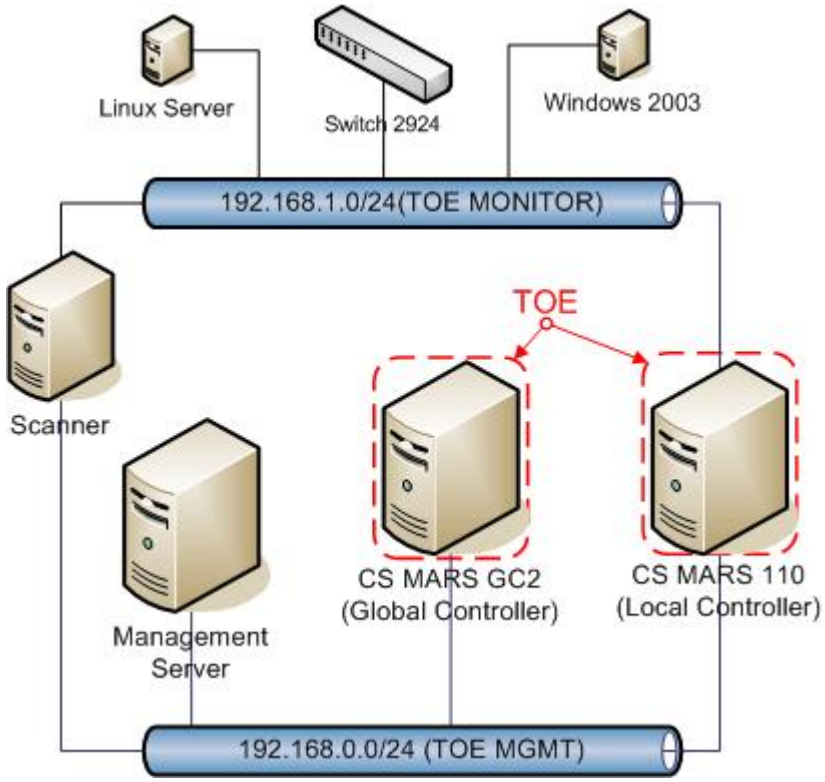

Figure 3: Cisco CSMARS v5.2 testing environment

Table 6 - Hardware and Software Components Tested by the CCTL

Component	Description
TOE: Local Controller CSMARS 110	Cisco Security MARS 110 running software version 5.2 (5.2.4.2487)
TOE: Global Controller CSMARS GC2	Cisco Security MARS GC2 running software version 5.2 (5.2.4.2487)

9 Validator Comments

The validator has reviewed the evaluation technical report and agrees with the conclusion of this evaluation. The customer is reminded that the following were not included within the scope of the evaluation.

- There are no Protection Profile compliance claims.
- The cryptography used in this product has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.
- Some of the sensor devices supported by the TOE use non-secure protocols (HTTP, Syslog, SNMPv1, OPSEC-LEA, OPSEC-CPML, POP, MS-RPC, SQLNet) for raw data

transfer to the TOE. The authorized administrator must ensure that appropriate measures are taken in the IT environment to protect this data in transit (OE.INTEGR).

10 Security Target

Cisco CS MARS (Security Monitoring, Analysis and Response System) Version 5.2, Security Target, version 7.0, dated July 9, 2008

11 List of Acronyms

Tables 7 and 8 below presents the acronyms, abbreviations and terms are used in this Security Target:

Table 7: Acronyms and Abbreviations

Acronyms / Abbreviations	Definition
CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
IT	Information Technology
OS	Operating System
PP	Protection Profile
SNMPv1	Simple Network Management Protocol version 1
SSHv1 or SSHv2	Secure Shell
SSLv2 or SSLv3	Secure Socket Layer
ST	Security Target
TCP	Transport Control Protocol
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy

Table 8: Terms

Term	Definition
JDBC	Java Database Connectivity- A Java standard defined by Sun Microsystems that specifies how Java applications access database data.
NetFlow	NetFlow is a Cisco technology that supports monitoring network traffic and is supported on all basic IOS images. NetFlow uses an UDP-based protocol to periodically report on flows seen by the Cisco IOS device.
OPSEC-CPMI	Open Platform for Security Check Point Management Interface; Communications protocol used for configuration discovery.
OPSEC-LEA	Open Platform for Security Log Export API; Communications protocol used for retrieving audit and firewall logs
POP	Post Office Protocol- A protocol that defines how e-mail clients get mail from mail servers.
RDEP	Remote Data Exchange Protocol is a protocol designed by Cisco Systems in order to exchange IDS/IPS events, configuration, log, and control messages.
SDEE	Security Device Event Exchange- SDEE is a Network Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) alert format based on XML.
Sessionize	Sessionize refers to correlating the reported 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.
SNMPv1	A protocol that defines network management and the monitoring of network devices and the functions of those devices.
SQL Net	Oracle's client/server middleware product that offers transparent connection from client tools to the database, or from one database to another. Implemented in the firewall at the edge to enforce certain security policy to control traffic in and out of the internal networks.
SSHv1 or SSHv2	A protocol permitting secure access over a network from one IT system to IT system.
SSLv2 or SSLv3	Protocol used for encrypting and security messages transmitted over the Internet
TCP	A transport layer protocol that moves packet data between applications

12 Bibliography

The following documents referenced during preparation of the validation report.

[1] Common Methodology for Information Technology Security Evaluation. ISO/IEC18045. August 2005 version 2.3 CCMB-2005-08-004.

[2] Common Criteria for Information Technology Security Evaluation, Parts 1-3, August 2005 version 2.3.

[3] CCIMB Interpretations.

[4] CCIMB CC and CEM Interpretations Database.

[5] Common Criteria Evaluation and Validation Scheme (CCEVS) for IT Security, Scheme Publications 1-6, v 2.0.

[6] CCEVS Precedents Database.

[7] CCEVS CC and CEM Public Interpretations Database.

[8] ISO/IEC 17025 General Requirements for the competence of testing and calibration laboratories, First Edition (1999, 12-15.)

[9] National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) Handbook 2001 Edition 150 Procedures and General Requirements.

[10] National Institute for Standards and Technology (NIST) Handbook 150: Requirements Analysis. 1994 Edition and 2001 Edition.

[11] NIST NVLAP Handbook 150 IT Security Testing Handbook.

[12] Cisco CSMARS Version 5.2, Security Target.

[13] *Cisco_CSMARS_v5.2_EAL2_CCTL_Team_Test_Plan_v5.0.doc.*

13 Interpretations

13.1 International Interpretations

Official start date of the evaluation was August 9, 2006. The evaluation team performed an analysis of the international interpretations and applied those that were applicable and had impact to the TOE evaluation as the CEM work units were applied.

The following international interpretations were applied for this evaluation:

None, as all Common Criteria International Interpretations were incorporated in Version 2.3.

13.2 NIAP Interpretations

The Evaluation Team determined that the following NIAP interpretation was applicable to this evaluation:

Table 9: Applicable Precedents

Precedent	Date
PD-0106: Situations Where AGD_USR May Be Vacuously Satisfied	2004-04-20

13.3 Interpretations Validation

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.