# Cisco CS MARS Version 5.2

# Security Target

**Version 7.0**

**July 9, 2008**

# Table of Contents

**1 SECURITY TARGET INTRODUCTION ........................................ 2**

1.1 ST AND TOE IDENTIFICATION ........................................ 2
1.2 SECURITY TARGET OVERVIEW ........................................ 3
1.3 REFERENCES ........................................ 4
1.4 ACRONYMS, ABBREVIATIONS, AND TERMS ........................................ 5

**2 TOE DESCRIPTION ........................................ 8**

2.1 TOE PRODUCT TYPE ........................................ 8
2.2 TOE OVERVIEW ........................................ 8
2.3 TOE PHYSICAL BOUNDARY ........................................ 9
*2.3.1 Data included in the TOE Physical Boundary ........................................ 11*
2.4 TOE LOGICAL BOUNDARY ........................................ 12
2.5 IT ENVIRONMENT DEPENDENCIES ........................................ 13
*2.5.1 Sensors ........................................ 14*
2.6 TOE SECURITY ARCHITECTURE ........................................ 18
2.7 SECURITY FUNCTIONS CLAIMED BY THE TOE ........................................ 18
2.8 TOE EVALUATED CONFIGURATION ........................................ 19
2.9 TOE ENVIRONMENT ........................................ 19

**3 SECURITY ENVIRONMENT ........................................ 21**

3.1 ASSUMPTIONS ........................................ 21
3.2 THREATS ........................................ 22
3.3 ORGANIZATIONAL SECURITY POLICIES ........................................ 22

**4 SECURITY OBJECTIVES ........................................ 24**

4.1 SECURITY OBJECTIVES FOR THE TOE ........................................ 24
4.2 SECURITY OBJECTIVES FOR THE ENVIRONMENT ........................................ 24

**5 SECURITY REQUIREMENTS ........................................ 25**

5.1 TOE SECURITY FUNCTIONAL REQUIREMENTS ........................................ 26
*5.1.1 FAU_GEN.1 Audit data generation ........................................ 27*
*5.1.2 FAU_SAR.1 Audit review ........................................ 28*
*5.1.3 FAU_SAR.2 Restricted audit review ........................................ 28*
*5.1.4 FAU_STG.2 Guarantees of audit data availability ........................................ 29*
*5.1.5 FAU_STG.4 Prevention of audit data loss ........................................ 29*
*5.1.6 FCS_CKM.1(1) Crytpographic Key Generation (SSH) ........................................ 29*
*5.1.7 FCS_CKM.1(2) Cryptographic key generation (HTTPS/SSL) ........................................ 29*
*5.1.8 FCS_CKM.2 Cryptographic Key Distribution ........................................ 29*
*5.1.9 FCS_CKM.4 Cryptographic Key Destruction ........................................ 30*
*5.1.10 FCS_COP.1(1) Cryptographic Operation (SSH Confidentiality) ........................................ 30*
*5.1.11 FCS_COP.1(2) Cryptographic Operation (SSH Integrity) ........................................ 30*
*5.1.12 FCS_ COP.1(3): Cryptographic Operation (HTTPS/SSL) ........................................ 30*
*5.1.13 FIA_UAU.2 Timing of authentication ........................................ 30*
*5.1.14 FIA ATD.1 User attribute definition ........................................ 31*
*5.1.15 FIA_UID.2 Timing of identification ........................................ 31*
*5.1.16 FMT_MOF.1 Management of security functions behaviour ........................................ 31*
*5.1.17 FMT_MTD.1(1) Management of TSF data ........................................ 31*
*5.1.18 FMT_MTD.1(2) Management of TSF data (User Accounts) ........................................ 31*
*5.1.19 FMT_MTD.1(3) Management of TSF data (TOE Configuration) ........................................ 31*

*5.1.20 FMT_SMF.1 Specification of Management Functions ............31*
*5.1.21 FMT_SMR.1 Security roles ............32*
*5.1.22 FPT_ITC.1 Inter-TSF confidentiality during transmission ............32*
*5.1.23 FPT_ITI.1 Inter-TSF detection of modification ............32*
*5.1.24 FPT_RVM.1 Non-bypassability of the TSP ............32*
*5.1.25 FPT_SEP.1 TSF domain separation ............33*
*5.1.26 FPT_STM.1 Reliable time stamps ............33*
*5.1.27 IDS_SDC.1 Sensor data collection [Explicit Stated SFR for the TOE] ............33*
*5.1.28 IDS_ANL.1 Analyser analysis [Explicit Stated SFR for the TOE] ............33*
*5.1.29 IDS_RCT.1 Analyzer react [Explicit Stated SFR for the TOE] ............33*
*5.1.30 IDS_RDR.1 Restricted Data Review [Explicit Stated SFR for the TOE] ............34*
*5.1.31 IDS_STG.1 Guarantee of Analyzer Data Availability [Explicit Stated SFR for the TOE] ......34*
5.2 TOE SECURITY ASSURANCE REQUIREMENTS ............35

**6 TOE SUMMARY SPECIFICATION ............36**

6.1 TOE SECURITY FUNCTIONS ............36
*6.1.1 Identification and Authentication Security Function ............36*
*6.1.2 External Device Communication Security Function ............36*
*6.1.3 Administration Security Function ............37*
*6.1.4 Reporting Security Function ............39*
*6.1.5 Analysis Security Function ............40*
*6.1.6 Reaction Security Function ............41*
*6.1.7 Audit Security Function ............41*
*6.1.8 Self Protection Security Function ............42*
6.2 ASSURANCE MEASURES ............42

**7 PROTECTION PROFILE CLAIMS ............44**

7.1 PROTECTION PROFILE REFERENCE ............44
7.2 PROTECTION PROFILE REFINEMENTS ............44
7.3 PROTECTION PROFILE ADDITIONS ............44

**8 RATIONALE ............45**

8.1 SECURITY OBJECTIVES RATIONALE ............45
8.2 RATIONALE FOR SECURITY FUNCTIONAL REQUIREMENTS ............52
*8.2.1 Rationale for Security Functional Requirements of the TOE Objectives ............52*
8.3 TOE SECURITY FUNCTIONS ............57
8.4 TOE SECURITY FUNCTIONAL COMPONENT HIERARCHIES AND DEPENDENCIES ............63
8.5 RATIONALE FOR EXPLICITLY STATED SFR FOR THE TOE ............66
8.6 RATIONALE FOR STRENGTH OF FUNCTION CLAIM ............66
8.7 ASSURANCE MEASURES RATIONALE FOR TOE ASSURANCE REQUIREMENTS ............67

# List of Tables

Table 1 Acronyms ........ 6
Table 2 Terms ........ 6
Table 3 Physical Boundary Elements of the TOE ........ 10
Table 4 TSF Data Types ........ 11
Table 5 Supported Devices ........ 14
Table 6 TOE Assumptions ........ 21
Table 7 Threats ........ 22
Table 8 Organizational Security Policies ........ 23
Table 9 Security Objectives for the TOE ........ 24
Table 10 Security Objectives for the Environment ........ 25
Table 11 TOE Security Functional Requirements ........ 26
Table 12 Auditable Events ........ 28
Table 13 TOE Assurance Requirements ........ 35
Table 14: Assurance Measures ........ 43
Table 15: Threats, Assumptions, and Policies to Security Objectives Mapping ........ 45
Table 16: Threats, Assumptions, and Policies to Security Objectives Rationale ........ 47
Table 17: TOE Security Functional Requirement to TOE Security Objectives Mapping ...... 53
Table 18: TOE Security Functional Requirement to TOE Security Objectives Rationale ..... 54
Table 19: TOE Security Functional Requirement to TOE Security Functions Mapping ....... 58
Table 20 Rationale of how the SF(s) meet the SFR(s) ........ 59
Table 21: TOE Security Functional Requirements Dependency Rationale ........ 64
Table 22: EAL2 SAR Dependencies ........ 67

## DOCUMENT INTRODUCTION

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Cisco Security MARS 110 and 110R, Cisco Security MARS 210, Cisco Security MARS GC2 Target of Evaluation. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats and/or network security events that the product intends to identify, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements.

# 1 SECURITY TARGET INTRODUCTION

This Chapter presents security target (ST) identification information and an overview of the ST. An ST contains the information technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. An ST principally defines:

a) A security problem [security event or security incident] expressed as a set of assumptions about the security aspects of the environment, a list of threats that the product is intended to counter, and any known rules with which the product must comply (Chapter 3, Security Environment).

b) A set of security objectives and a set of security requirements to address the security problem (Chapters 4 and 5, Security Objectives and Security Requirements, respectively).

c) The IT security functions provided by the TOE that meet the set of requirements (Chapter 6, TOE Summary Specification).

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3, Chapter 4.

## 1.1 ST and TOE Identification

This section provides information needed to identify and control this ST and its TOE. This ST targets Evaluation Assurance Level EAL2.

| **ST TITLE** | Cisco CS MARS Version 5.2 Security Target |
|---|---|
| ST Version | Version 7.0 |
| Publication Date | July 9, 2008 |
| Vendor | Cisco Systems |
| ST Authors | Cisco Systems |
| TOE Identification | Cisco Security MARS 110 and 110R, Cisco Security MARS 210, Cisco Security MARS GC2 Target of Evaluation (TOE) |
| TOE Software Version | Cisco CS MARS Version 5.2.4.2487 |
| CC Identification | Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005 |
| Common Criteria Conformance Claim | The ST is compliant with the Common Criteria (CC) Version 2.3.<br>The ST is EAL2 Part 3 conformant.<br>The ST is CC Part 2 extended |
| Protection Profile Conformance | The TOE does not claim conformance to any Protection Profile. |
| Security Target Evaluation Status | Complete |
| Keywords | IDS, Analyzer, Network Security |

## 1.2 Security Target Overview

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 PP. The CS MARS purpose is to identify, isolate and recommend precise removal of offending elements.

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 2 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 ST. The administrator must determine which configuration will apply prior to deploying the TOE.

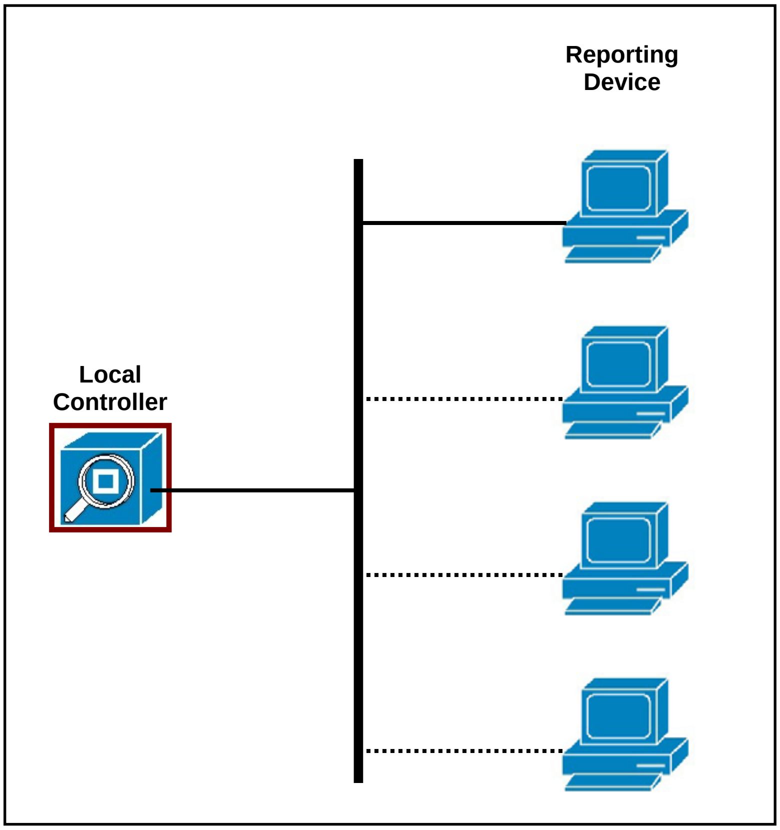

**Figure 1. Single Local Controller Configuration**

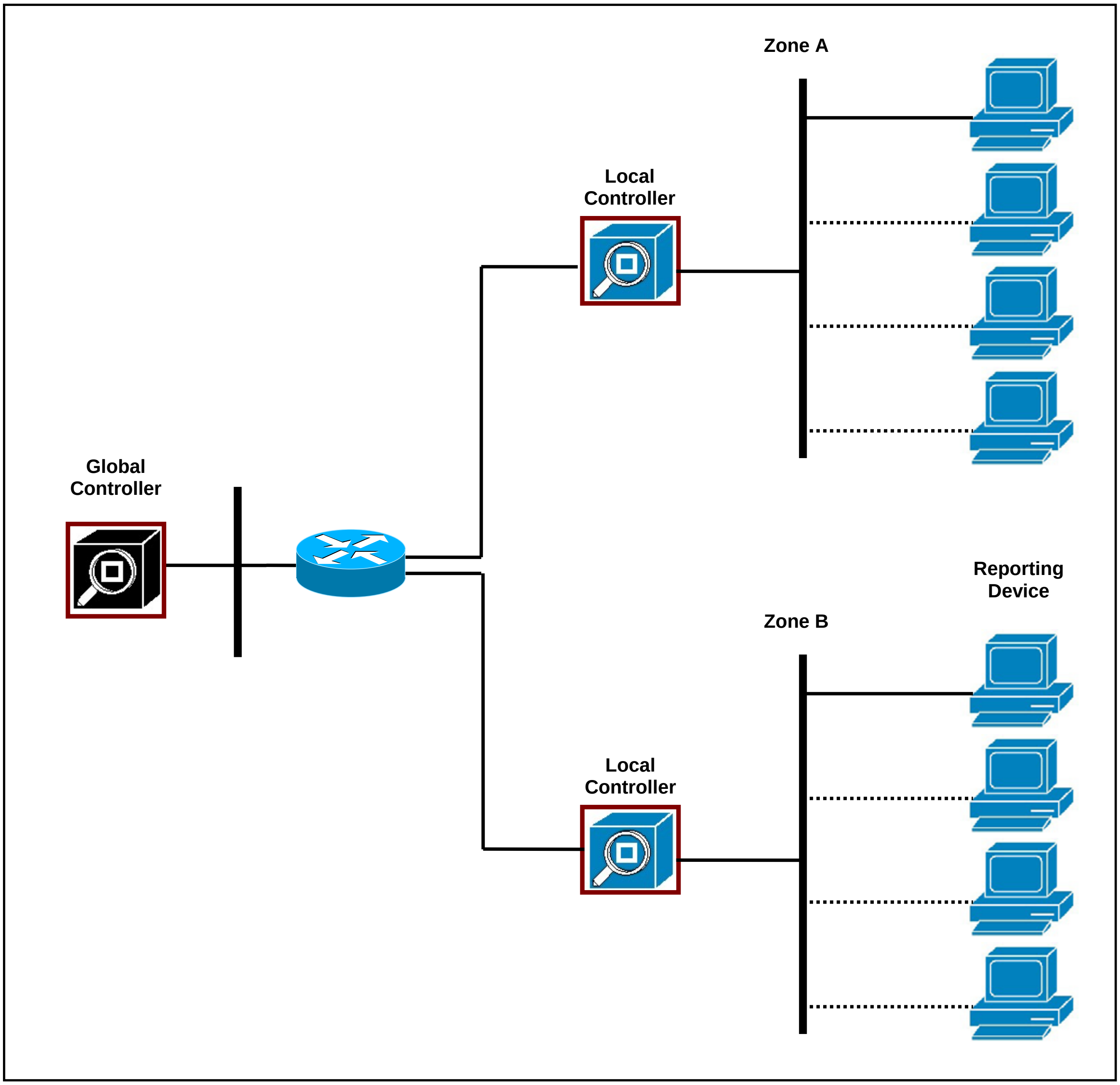

**Figure 2. Global Controller Configuration**

## 1.3 References

The following documentation was used to prepare this ST:

| | |
|---|---|
| [CC_PART1] | Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 2005, version 2.3, CCMB-2005-08-001 |

[CC_PART2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, version 2.3, CCMB--2005-08-002

[CC_PART3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, version 2.3, CCMB-2005-08-003

[CEM] Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated August 2005, version 2.3 CCMB-2005-08-004

## 1.4 Acronyms, Abbreviations, and Terms

The following acronyms and abbreviations are used in this Security Target:

**Table 1 Acronyms**

| 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 2 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. |

| Term | Definition |
|---|---|
| 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 |

# 2 TOE DESCRIPTION

This section provides an overview of the CS MARS Version 5.2 Target of Evaluation (TOE) to assist potential users in determining whether it meets their needs for identification, isolation and management to counter security threats. The TOE for this ST consists of the following Cisco Security Monitoring, Analysis and Response System components: Cisco Security MARS 110 and 110R, Cisco Security MARS 210, Cisco Security MARS GC which support version 5.2. This section also defines the physical and logical boundaries of the TOE and describes the evaluated configuration of the TOE.

## 2.1 TOE Product Type

The CS-MARS TOE is an appliance-based monitoring, analysis and response system analyzer designed to work with existing network devices and security applications to identify, manage and recommend actions to counter security intrusions within its connected network.

Data collected by the TOE is used to subvert valid security incidents [i.e. centralize, detect, mitigate, and report on priority threats]. The TOE centrally aggregates logs and events from a wide range of network devices (such as routers and switches), security devices and applications (such as firewalls, intrusion detection systems [IDSs], vulnerability scanners, and antivirus applications), hosts (such as Windows, Solaris, and Linux syslogs), applications (such as databases, Web servers, and authentication servers), and network traffic (such as Cisco NetFlow).

## 2.2 TOE Overview

CS-MARS Version 5.2 TOE is an intrusion detection system analyzer that collects data from reporting devices (hereafter referred to as reporting devices or sensors) within the network which it then analyzes for intrusions. The information being collected by the TOE or received by the TOE from reporting devices is hereafter referred to as data or raw data. The TOE collects events from routers, switches, firewalls, vulnerability scanners, VPN devices, antivirus applications, host IDS applications, Windows, Solaris, RedHat Linux, web servers, web proxies, Oracle database server, Cisco ACS, syslog servers, SNMPv1 devices, and network IDS devices. All of these devices act as sensors to the TOE.

The TOE receives or pulls (see Section 6.1.2) raw data in the form of device logs, alerts, events[1] and NetFlow communications generated by the sensors and further compares it to system and rules created to identify possible attacks, security incidents or other intrusions across the network segments that are being monitored by the reporting devices. A rule is a real-time filter that detects patterns of network activity. Rules trigger based on what the TOE collects from sensors. If a match occurs, the TOE creates an incident which is then used for viewing and analysis and recommends possible commands to help mitigate a security incident. The TOE comes with a set of

[1] In the context of raw data, ‘event’ or ‘event data’ should be understood to mean an occurrence on the network which was detected by the reporting device. This ‘event’ should not be confused with events that are generated by the TOE.

rules representing a variety of attack types, while rules may also be defined by users of the TOE with permission to do so.

Throughout the ST, the term “user” is meant to mean any of the user roles defined by FMT_SMR.1 that have access to TOE resources. The Notification role is considered a non- user role for the TOE because it has no access to TOE resources and only receives alerts. The term “administrator” refers to only the defined Administrator role. Roles and the management functions associated with them are defined in the FMT requirements and described in the TSS.

The TOE gathers configuration information from the sensing networking devices to create a network topology from these devices to help in the analysis and notification functions carried out by the TOE. The TOE has an automatic discovery mechanism to collect information, which the TOE uses in turn to create a topology map containing the configuration and security policies of its elements. This topology map enables modeling of packet flow throughout the entire network. As raw data is received it is normalized against the network topology and device type into events which are then correlated and matched to the rules mentioned above to identify security incidents.

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.

Audit and analysis records are created according to events identified within the network as well as actions recommended by the TOE. A web based interface is presented to users of the TOE to view these records as well as assist in analysis and possible commands that a user may send to a sensor to help mitigate an identified incident. The web interface visually presents summarized and detailed accounts of each identified security incident. A topology map is used to indicate hotspots, incidents, the full attack paths, and rule matches with alerting to the event. The TOE has the capability of identifying devices along an attack path which are being compromised and automatically providing the device or application commands that can be entered by the user to configure the device to help mitigate the threat; depending on the device in question.

The TOE stores all raw data collected from sensors. The TOE allows real time and ad hoc query on the raw data and analysis records, allowing additional analysis and replay of attacks through stored information. Reports generated from the TOE can be generated using TOE defined reports or the reports can be stored and modified to suit a user’s needs.

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.

## 2.3 TOE Physical Boundary

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

The CSMARS 5.2 Operating system includes Oracle database 10.2.0.3 and JBoss application server 3.2.7.

The TOE is configured in one of two ways. It is either a local controller acting alone or a global controller with two or more local controllers. Either configuration provides all security functionality defined in this ST.

Local controllers receive and pull (see Section 6.1.2) data from sensors, such as firewalls, routers, intrusion detection/prevention systems, and vulnerability assessment systems. A local controller summarizes information about the health of your network based on data it receives from the sensors that it monitors

A global controller must manage two or more local controllers in order to function in the evaluated TOE configuration. When multiple (two or more) local controllers are deployed, a global controller is deployed to manage and summarize the findings of two or more local controllers that receive and pull (see Section 6.1.2) data as described above. In this configuration, the global controller enables the TOE to scale the network monitoring without increasing the management burden. The global controller provides a single user interface for defining new device types, inspection rules, and queries, and it enables the administrator to manage local controllers under its control. This management includes defining administrative accounts and performing remote, distributed upgrades of the local controllers.

The following table identifies the physical boundary of the different versions of the TOE. An 'X' in a cell indicates the version of the TOE has that physical boundary element.

**Table 3 Physical Boundary Elements of the TOE**

| Element | MARS 110 and 110R | MARS 210 | MARS GC2 |
|---|---|---|---|
| Drives 1-3 | X | X | X |
| Drives 4-6 | X | X | X |
| Drive status lights | X | X | X |
| DVD Drive | X | X | X |
| DVD eject button | X | X | X |
| Power switch | X | X | X |
| Power indicator light | X | X | X |
| Face plate release screws | X | X | X |
| PS/2 Keyboard port | X | X | X |
| PS/2 Mouse Port | X | X | X |
| Parallel port (not supported) | X | X | X |
| eth0, Ethernet 0 port | X | X | X |
| eth1, Ethernet 1 port | X | X | X |
| eth2, Ethernet 2 Port | X | X | X |
| RJ-11 Line-in port | X | X | X |
| Telephone port (line out) | X | X | X |
| Power socket | X | X | X |

| Element | MARS 110 and 110R | MARS 210 | MARS GC2 |
|---|---|---|---|
| Serial Port | X | X | X |
| VGA port | X | X | X |
| USB 0 port (not supported) | X | X | X |
| USB 1 port (not supported) | X | X | X |
| Power source release screw | | | |
| Power source release lever | X | X | X |
| Power source handle | X | X | X |
| Power source light | X | X | X |
| Power source switch | X | X | X |

### 2.3.1 Data included in the TOE Physical Boundary

The following sections identify the data included in the TOE's physical boundary.

#### 2.3.1.1 TSF Data

TSF data in the TOE includes rule definitions used during raw data analysis to identify possible intrusions and security incidents for the network being monitoring. Rule definitions identifying intrusion scenarios are supplied with the TOE. Administrators may add and modify rules according to the desired scenarios to extend and alter intrusion analysis and security incident detection. Rules created or modified by a administrator of the TOE are considered TSF data. Incidents generated by a rule are considered TSF data. TSF data includes audit records generated by the system during the course of execution.

**Table 4 TSF Data Types**

| Type of TSF Data | Description |
|---|---|
| Events | Normalized data that has been processed by the TOE classified in events types and event groups. This is also referred to as Analyzer event data. |
| Rules | Identifications of intrusion or violation scenarios |
| Audit data | Audit records generated by the TOE during the course of execution AND audit records created in accordance with events occurring on the network |
| Incidents | Events that are grouped together through context correlation and vector analysis |
| TOE configuration data | Data used for operational administration of the TOE evaluated configuration |

#### 2.3.1.2 User Data

The raw data generated by and collected from sensors that is analyzed by the TOE is considered user data. Raw data is composed of security relevant information from each sensor. This includes configuration data from the remote sensors. Reports that a user creates or modifies for their use is considered user data.

#### 2.3.1.3 Security Attributes

The security attributes of the TOE are roles (the authorizations a user has), user password (authentication data), user identifier, and the group the user belongs to.

## 2.4 TOE Logical Boundary

The TOE is comprised of a monitoring service, analysis service, response service, access control routings and security management capabilities. The TOE interfaces with human users through a web interface and a command line interface (CLI). The web interface provides the monitoring service, analysis service and response service to the human users. The CLI is an administrator only interface that is reachable only through SSHv1 or SSHv2 or a physical serial console connection on the TOE. The TOE interfaces with sensors, which supply the raw data to the TOE that is processed and correlated and grouped into sessions real-time (sessionised) by the TOE for intrusions and security incidents.

The web interface for human users presents the user with a tab-based, hyperlinked user interface that provides command options that provide the users with access to the monitoring, analysis, and response services of the TOE. Users may click the command options and other web screens are displayed to them so that they can further configure, modify, analyze, or review the capabilities and data that is protected, processed, and stored on the TOE for users use. The Summary, Incidents, Query/Reports, Rules, Management, and Admin tab command options presented to users through the web interface provides interfaces to the security management, reviewing, analysis, querying, and reporting capabilities of the TOE. The Summary command option in the web interface provides a summary of the most recent incidents that have been analyzed by the TOE and summarizes other security incidents and data that has been collected by the TOE. The Incident command option of the web interface provides the capabilities for users to review and analyze the incidents that have been found and recorded by the TOE through the collection of data from reporting devices. The Query/Reports command option of the web interface provides the capabilities to users to query the data the TOE has for incidents (intrusions and security incidents) and report that information in a standard report form or a user defined report form. The reports that are defined and can be defined are saved queries that can be run once or on a periodic time frame to gather the information that was defined in the saved report. The system rule and custom rule command option of the web interface provides the capability to configure and modify the analysis capabilities of the TOE. The Management and Admin command options of the web interface provides the security management capabilities that allow for the viewing of the audit trail, configuring user accounts, configuring reporting devices, configuring alarms (e-mail, SNMPv1, pager, and SMS), and configuring the settings of the TOE.

The TOE communicates with reporting devices to collect or receive raw data. Once the raw data is within the TOE boundary, it is considered "collected data" whether it was pushed to the TOE or pulled from the sensor by the TOE (see Section 6.1.2). The raw data is collected, correlated and grouped in to sessions analyzed by the TOE to determine intrusions and security incidents. The TOE communicates with external reporting devices through the use of protocols such as SSHv1 or SSHv2, or SNMPv1. The TOE only communicates with those reporting devices that the TOE has been configured to communicate with. The TOE initiates the communications to remote devices using SSHv1 or SSHv2, or SNMPv1.

The TOE provides access control capabilities through the web interface and the CLI interface. The TOE ensures that the access control capabilities are invoked whenever any user attempts access through one of these interfaces. Part of the access control capabilities of the TOE is the use of roles. Each role has different privileges, authorizations. The TOE supports Admin, Security Analyst, Operation, and Notification roles. These roles are set when the user account is setup and may be changed any time after the user account has been setup.

The TOE includes either a local controller acting alone or a global controller with two or more local controllers. The local controllers are Cisco Security MARS 110 and 110R, and the Cisco Security MARS 210. The global controller is Cisco Security MARS GC2. A local controller has no management capabilities outside of it own operation. A global controller manages two or more local controller's rules, configured sensors, queries, and user information. A global controller collects incidents from the local controllers that it is configured to manage. The purpose of the global controller is to summarize the findings of two or more local controllers. The only reporting devices configured for a global controller are the local controllers it manages. Global and local controllers are configured for secure communication using SSLv2 or SSLv3.

## 2.5 IT Environment Dependencies

The TOE collects raw data from the reporting devices. The TOE depends and interoperates with IT Environment sensors broken down into the categories in the following sections: router and switch devices; firewall devices; VPN devices; network IDS devices; host IDS devices; anti-virus devices; vulnerability assessment devices; web server devices; web proxy devices; database server devices; AAA server devices; and syslog servers and SNMPv1 devices. The column in the tables labeled 'Protocol: Configuration Retrieval' helps support the analysis security function of the TOE. The TOE retrieves configuration information from sensors to help better determine if security incidents are occurring on the network(s) that it is analyzing. The column in the tables labeled 'Protocol: Data Retrieval' helps support the analysis security function of the TOE. The TOE retrieves events generated by sensors to help in its determination if security incidents are occurring on the network(s) that it is analyzing. For the column in the tables labeled 'Protocol: Configuration Retrieval' this function is initiated outbound along with all the protocols identified in the column outbound from the TOE. For the column in the tables 'Protocol: Event Retrieval' this function is initiated outbound along with all the protocols identified in the column. For a brief definition of the protocols refer to Table 2 above.

The following table lists the sensors and versions that the TOE interoperates with. The TOE can interoperate with any type of IT Environment supplied sensor listed in the tables at its current version of the sensor and any future version of the sensors detailed in the following tables.

Note that in the table below, cells that contain N/A should be understood to mean that the particular retrieval type is not applicable to that particular product.

In addition to the sensors identified in the table below, the TOE has the following IT Environment dependencies:

- The TOE requires Internet Explorer Web browser (Microsoft Internet Explorer 6.0 or higher) to be used by users and administrators of the TOE to communicate with the TOE's web interface.
- The IT Environment must include an SSHv1 or SSHv2 client
- The IT Environment must include an SSLv2 or SSLv3 client
- The IT Environment must supply an email server

### 2.5.1 Sensors

The following table lists the devices from which the TOE receives or collects raw data for analysis. The table lists the device type and the vendor, the supported version of software loaded on the given device, the protocol(s) used. **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).

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 mostly pushed to the TOE via syslog and SNMP traps. Any exceptions are indicated in the rightmost column of the table below.

Note that when the global TOE configuration is used, local controllers push their reports to global controllers using SSLv2 or SSLv3.

**Table 5 Supported Devices**

| **Type** | **Vendor** | **Versions** | **Configuration retrieval protocol** | **Raw Data retrieval protocol** | **Pushed to TOE or Pulled from Sensor** |
|---|---|---|---|---|---|
| Router / Switch | Cisco IOS | 11.x, 12.x | SSHv1 or SSHv2, SNMPv1 | Syslog (from device), | Pushed |
| | | | | NetFlow v1,v3,v5,v7 | Pushed |

| **Type** | **Vendor** | **Versions** | **Configuration retrieval protocol** | **Raw Data retrieval protocol** | **Pushed to TOE or Pulled from Sensor** |
|---|---|---|---|---|---|
| | Cisco CatOS | 6.x | SSHv1 or SSHv2, SNMPv1 | Syslog (from device) | Pushed |
| | Extreme Extremeware | 6.x | SNMPv1 | Syslog (from device) | Pushed |
| Firewall | Cisco PIX | 6.0, 6.1, 6.2, 6.3, 7.0 | SSHv1 or SSHv2, SNMPv1 | Syslog (from device) | Pushed |
| | Cisco ASA | 7 | SSHv1 or SSHv2, SNMPv1 | Syslog (from device) | Pushed |
| | Cisco FWSM | 1.1, 2.1, 2.2, 2.3 | SSHv1 or SSHv2, SNMPv1 | Syslog (from device) | Pushed |
| | Cisco IOS FW Feature | 12.2(T) and later | SSHv1 or SSHv2, SNMPv1 | Syslog (from device) | Pushed |
| | Netscreen | 3.0, 4.0, 5.0 | SSHv1 or SSHv2, SNMPv1 | Syslog (from device) | Pushed |
| | Checkpoint FW1 | FP3, FP4, AI | CPMI | LEA (from Log Server or Management Server) | Pushed |
| | Nokia Firewall (running Checkpoint) | FP3, FP4, AI | CPMI | LEA (from Log Server or Management Server) | Pulled |
| VPN | Cisco VPN 3000 | 4.0, 4.7 | N/A | Syslog (from device) | Pushed |
| Network IDS | Cisco NIDS, IDSM | 3.x | N/A | POP (from device) | Pulled |
| | Cisco NIDS, IDSM | 4.x | N/A | RDEP (from device) | Pulled |

| **Type** | **Vendor** | **Versions** | **Configuration retrieval protocol** | **Raw Data retrieval protocol** | **Pushed to TOE or Pulled from Sensor** |
|---|---|---|---|---|---|
| | Cisco IPS, ASA module | 5.0, 5.1 | N/A | SDEE (from device) | Pulled |
| | Cisco IOS IPS | 12.2 | N/A | SDEE (from device) | Pulled |
| | McAfee Intrushield | 1.5, 1.8 | N/A | SNMP (from Management Server) | Pushed |
| | Netscreen IDP | 2.x | N/A | SNMP (from Management Server) | Pushed |
| | Symantec Manhunt | 4.0 | N/A | SNMP (from Device) | Pushed |
| | ISS RealSecure | 6.5, 7.0 | N/A | SNMP (from Device) | Pushed |
| | Snort | 1.x, 2.x | N/A | Syslog (from Device) | Pushed |
| | Enterasys Dragon | 6.x | N/A | Syslog (from Manager) | Pushed |
| Host IDS | Cisco CSA | 4.0, 4.5 | | SNMP (from CSA MC) | Pushed |
| | McAfee Entercept | 2.5, 4.x | N/A | SNMP (from Management Server) | Pushed |
| | ISA RealSecure Host Sensor | 6.5, 7.0 | N/A | SNMP (from Device) | Pushed |
| Anti-virus | Symantec AV | 9.x | N/A | SNMP (from Management Server) | Pushed |
| | CICC, Trend Micro OPS | 11.x-Prg 7.5 –Engine | N/A | Syslog (from CICC Server) | Pushed |

| Type | Vendor | Versions | Configuration retrieval protocol | Raw Data retrieval protocol | Pushed to TOE or Pulled from Sensor |
|---|---|---|---|---|---|
| | Network Associates | 8.x | N/A | SNMP (from Management Server) | Pushed |
| Vulnerability Assessment | E-eye REM | 1.x | N/A | JDBC (MS SQL) (from REM server) | Pulled |
| | Qualys | 3.4 | N/A | HTTPS | Pulled |
| | Foundstone Foundscan | 4.x | N/A | JDBC (MS SQL) (from Management Sever) | Pulled |
| Host OS | Windows | NT, 2000, 2003 | N/A | Syslog (from SNARE agent) or MS-RPC event pull | Pulled ( in case of MS_RPC) |
| | Solaris | 8.x, 9.x, 10.x | N/A | Syslog (from Device) | Pushed |
| | Redhat Linux | 7.x, 8.x | N/A | Syslog (from Device) | Pushed |
| Web Server | Microsoft IIS | ANY | N/A | Syslog (from SNARE agent) | Pushed |
| | Sun iPlanet | ANY | N/A | HTTP (from Protego Agent) | Pushed |
| | Apache | ANY | N/A | HTTP (from Protego Agent) | Pushed |
| Web proxy | NetApp Netcache | | N/A | HTTP | Pushed |
| Database | Oracle | 9i, 10g | N/A | SQLNet (from Host) | Pulled |
| AAA | Cisco ACS | 3.x | N/A | Syslog (from Protego Agent) | Pushed |

## 2.6 TOE Security Architecture

The following section provides details about how the security architecture of the TOE for this ST cannot be bypassed, corrupted, or otherwise compromised. An explanation is provided for how each TOE type supports the secure operation of the TSF.

The TOE is a self contained hardware and software appliance. The TOE provides IDS Analysis services. It is a dedicated device, with no general purpose operating system or programming interface. The TOE mediates the interfaces and communications and makes sure that the security enforcement functions are invoked and succeed before allowing any other mediated security function to be used. By doing this the TOE ensures that it and its security functions are non-bypassable.

The TOE maintains a security domain for its own use. The security domain is all the hardware and software that makes up the TOE. The TOE provides for isolation at the physical boundary of the component. For this reason the whole TOE is an isolated security domain. The TOE helps in keeping the domain separate and protected by controlling interfaces into it so that only trusted and authorized communications occur that are directly related to satisfying the TOE's capability to provide IDS Analysis services. The administrative and user interface is protected by authentication and by physical controls, and by means of encryption when used remotely. No untrusted processes are permitted on the TOE. Because the whole TOE is a separate physical domain and a dedicated platform solely supporting its own processes and the fact that it controls and mediates access to its interfaces, it provides a security domain for the TSF that is protected from interference and tampering.

## 2.7 Security Functions Claimed by the TOE

The TOE's security function (TSF) Functions summary is:

- Identification and Authentication Security Function:

  The TOE's Identification and Authentication Security Function provides security when users log into the TOE using account information and role application.

- External Device Communication Security Function:

  The TOE provides communication with the devices in the network to collect or receive the raw data as well as to recommend mitigation commands for the sensors.

- Administration Security Function:

  The TOE provides the administrator the ability to configure system parameters related to user accounts and the system, as well as define within the TOE what network elements the TOE will monitoring and collect data from. Note that throughout the ST, "user" may refer to any of the roles defined in FMT_SMR.1 except the Notification role which has no access to TOE resources and is a non-user role. "Administrator" refers only to the authorized administrator.

- Audit Security Function:

  The TOE provides a mechanism to view and query the audit records generated by the system.

- Reporting Security Function:

  The TOE provides the ability to create report formats, as well as view and modify existing report formats.

- Analysis Security Function:

  The TOE performs data analysis and creates records and GUI views to display the results.

- Reaction Security Function:

  The TOE provides reaction actions in the form of alerts, pages and emails as well as proposes possible mitigation commands to the user for specific sensors. SSHv1 or SSHv2 is the configured protocol that must be used when commands are entered by the user to a sensor for mitigation by the sensor.

- Self Protection Security Function:

  The TOE provides self protection by requiring all users to be identified and authenticated and by monitoring all interfaces, actions, and resources of the TOE and only allowing those actions of user to be performed if they have the appropriate authorizations.

## 2.8 TOE Evaluated Configuration

The TOE's evaluated configuration requires one or more instances of:

- 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

And one or more of the reporting devices specified in the IT Environment dependency section above.

## 2.9 TOE Environment

In the evaluated configuration the TOE is configured to receive events from assorted sensor devices in the IT environment, identified in Table 5. If the events satisfy the criteria of a TOE system rule, the rule is triggered and a security incident is created and logged. An authorized TOE administrator can configure the TOE to provide recommended actions/commands that the administrator can execute on network assets to mitigate the security incident.

The TOE can be configured to notify selected administrative users, of an incident, by E-mail, SMS, and pager alerts. The TOE sends the incident ID, matched rule name, severity, and incident time in email, SMS and pager formats respectively. The administrator must login to the MARS to view all the incident details including the recommended mitigation.

These recommended actions/commands are executed out of band (externally) of the TOE. The administrator must execute the actions/commands directly on the network device associated with security incident.

The TOE can also be configured to notify a specified administrator that the TOE database is near exhaustion.  When the TOE is configured, an e-mail message is sent to an administrator when the database, which includes the audit trail, is within 2.5% of filling. This percentage is not a settable parameter. Only the sending of an e-mail is a settable parameter.

# 3 SECURITY ENVIRONMENT

This chapter identifies the following:

A) Significant assumptions about the TOE's operational environment.

B) IT related threats to the organisation identified by the TOE.

C) Environmental threats requiring controls to provide sufficient protection.

D) Organisational security policies for the TOE as appropriate.

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name. Policies are identified as P.policy with "policy" specifying a unique name.

## 3.1 Assumptions

The specific conditions listed in the following subsections 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.

**Table 6 TOE Assumptions**

| Name | Assumption |
|---|---|
| A.ACCESS | The TOE has access to all the IT System resources necessary to perform its functions. |
| 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. |
| A.PROTCT | The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. |
| A.LOCATE | The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. |
| A.MANAGE | There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. |
| A.NOEVIL | The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. |
| A.NOTRST | The TOE can only be physically accessible by authorized users. |

## 3.2 Threats

Table 7 lists the threats addressed by the TOE and the IT Environment. For the threats below, attackers are assumed to be of low attack potential.

**Table 7 Threats**

| Threat Name | Threat Definition |
|---|---|
| T.COMINT | An unauthorized person may attempt to compromise the integrity of the data analyzed and produced by the TOE by bypassing a security mechanism. |
| T.COMDIS | An unauthorized person may attempt to disclose the data analyzed and produced by the TOE by bypassing a security mechanism. |
| T.LOSSOF | An unauthorized person may attempt to remove or destroy data analyzed and produced by the TOE. |
| T.NOHALT | An unauthorized person may attempt to compromise the continuity f the TOEs analysis functionality by halting execution of the TOE. |
| T.PRIVIL | An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. |
| T.IMPCON | The TOE may be susceptible to improper configuration by an authorized or unauthorized person causing potential intrusions to go undetected. |
| T.INFLUX | An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle. |
| T.INTEGR | An unauthorized user may attempt to modify sensor data in transit from sensor devices or alert notification from the TOE transmitted over non-secured protocols. |
| T. FALACT | The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity. |
| T.FALREC | The TOE may fail to recognize vulnerabilities or inappropriate activity based on data received from each data source. |
| T.FALASC | The TOE may fail to identify vulnerabilities or inappropriate activity based on association of data received from all data sources. |

## 3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs.

Table 8: Organizational Security Policies identifies the organizational security policies.

**Table 8 Organizational Security Policies**

| Policy Name | Policy Definition |
|---|---|
| P.ANALYZ | Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to raw data and appropriate response actions taken. |
| P.DETECT | The TOE shall apply analytical processes to data collected from sensors. |
| P.MANAGE | The TOE shall only be managed by authorized users. |
| P.ACCESS | All data analyzed and generated by the TOE shall only be used for authorized purposes. |
| P.ACCACT | Users of the TOE shall be accountable for their actions within the TOE. |
| P.INTGTY | Data analyzed and generated by the TOE shall be protected from modification. |
| P. PROTCT | The TOE shall be protected from unauthorized accesses and disruptions of analysis and response activities. |

# 4 SECURITY OBJECTIVES

This Chapter identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

- This document identifies objectives of the TOE as O.*objective* with *objective* specifying a unique name. Objectives that apply to the IT environment are designated as OE.*objective* with *objective* specifying a unique name.

## 4.1 Security Objectives for the TOE

Table 9: Security Objectives for the TOE identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

**Table 9 Security Objectives for the TOE**

| Name | TOE Security Objective |
|---|---|
| O. PROTCT | The TOE must protect itself from unauthorized modifications and access to its functions and data. |
| O.IDACTS | The TOE must accept data from reporting devices and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future). |
| O.RESPON | The TOE must respond appropriately to analytical conclusions. |
| O.EADMIN | The TOE must include a set of functions that allow effective management of its functions and data. |
| O.ACCESS | The TOE must allow authorized users to access only appropriate TOE functions and data. |
| O.IDAUTH | The TOE must be able to identify and authenticate authorized users prior to allowing access to TOE functions and data. |
| O.OFLOWS | The TOE must appropriately handle potential audit and event data storage overflows. |
| O.AUDITS | The TOE must record audit records for data accesses and use of the Analyzer functions. |
| O.INTEGR | The TOE must ensure the integrity of all audit and event data. For data collected from sensor devices, Toe involvement will begin once the data enters the TOE boundary. |
| O. EXPORT | When the TOE makes its event data available to other components, the TOE will ensure the confidentiality of the Analyzer event data. |

## 4.2 Security Objectives for the Environment

The assumptions identified in Section 3.1.1 are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. Table 10: Security Objectives for the Environment identifies the security objectives for the environment.

**Table 10 Security Objectives for the Environment**

| Name | IT Environment Security Objective |
|---|---|
| OE.INSTAL | Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security. |
| OE. PHYCAL | Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack. |
| OE.CREDEN | Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security. |
| OE.PERSON | Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the Analyzer. |
| OE.INTROP | The TOE is interoperable with the IT System it monitors. |
| 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 or cryptographic means. |

# 5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE and for the IT Environment. The Security Functional Requirements included in this section are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.3* and all National Information Assurance Partnership (NIAP) and international interpretations with the exception of the items listed below.

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC.

Assignments: indicated by showing the value in square brackets [Assignment_value].

Selections: indicated by italicized text.

Assignments within selections: indicated in italics and underlined text.

Refinements: indicated in **bold text** with the addition of details and ~~**bold text**~~ when details are deleted.

Multiple Security Functional Requirement instances (iterations) are identified by the Security Functional Requirement component identification followed by the instance number in parenthesis (e.g. FAU_SAR.1(1)) and the Security Functional Requirement element name followed by the instance number in parenthesis (e.g. FAU_SAR.1.1(1)).

Explicitly stated SFRs are identified by having a label ‘Explicit Stated SFR for the TOE’ after the requirement name for TOE SFRs.

## 5.1 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in Table 11 are described in more detail in the following subsections.

**Table 11 TOE Security Functional Requirements**

| Functional Component | | Dependencies |
|---|---|---|
| FAU_GEN.1 | Audit data generation | FPT_STM.1 |
| FAU_SAR.1 | Audit review | FAU_GEN.1 |
| FAU_SAR.2 | Restricted audit review | FAU_SAR.1 |
| FAU_STG.2 | Guarantees of audit data availability | FAU_GEN.1 |
| FAU_STG.4 | Prevention of audit data loss | FAU_STG.1 |
| FCS_CKM.1(1) | Cryptographic key generation (SSH) | FCS_CKM.2,<br>FCS_CKM.4,<br>FCS_COP.1(1),<br>FMT_MSA.2 |
| FCS_CKM.1(2) | Cryptographic key generation (SSL) | FCS_CKM.2,<br>FCS_CKM.4,<br>FCS_COP.1(3),<br>FMT_MSA.2 |
| FCS_CKM.2 | Cryptographic key distribution | FDP_ITC.1,or<br>FDP_ITC.2 or<br>FCS_CKM.1,<br>FCS_CKM.4,<br>FMT_MSA.2 |
| FCS_CKM.4 | Cryptographic key destruction | FDP_ITC.1,or<br>FDP_ITC.2 or<br>FCS_CKM.1,<br>FMT_MSA.2 |
| FCS_COP.1(1) | Cryptographic operation (SSH confidentiality) | FMT_MSA.2,<br>FDP_ITC.1,or<br>FDP_ITC.2 or<br>FCS_CKM.1(1),<br>FCS_CKM.4 |

| Functional Component | | Dependencies |
|---|---|---|
| FCS_COP.1(2) | Cryptographic operation (SSH integrity) | FMT_MSA.2, FDP_ITC.1,or FDP_ITC.2 or FCS_CKM.1(1), FCS_CKM.4 |
| FCS_COP.1(3) | Cryptographic operation (SSL) | FMT_MSA.2, FDP_ITC.1,or FDP_ITC.2 or FCS_CKM.1(2), FCS_CKM.4 |
| FIA_UAU.2 | Timing of authentication | FIA_UID.2 |
| FIA_ATD.1 | User attribute definition | No Dependencies |
| FIA_UID.2 | Timing of identification | No Dependencies |
| FMT_MOF.1 | Management of security functions behavior | FMT_SMR.1<br>FMT_SMF.1 |
| FMT_MTD.1(1) | Management of TSF data | FMT_SMR.1<br>FMT_SMF.1 |
| FMT_MTD.1(2) | Management of TSF data (User Accounts) | FMT_SMR.1<br>FMT_SMF.1 |
| FMT_MTD.1(3) | Management of TSF data (TOE Configuration) | FMT_SMR.1<br>FMT_SMF.1 |
| FMT_SMF.1 | Specification of Management Functions | No Dependencies |
| FMT_SMR.1 | Security roles | FIA_UID.2 |
| FPT_ITC.1 | Inter-TSF confidentiality during transmission | No Dependencies |
| FPT_ITI.1 | Inter-TSF detection of modification | No Dependencies |
| FPT_RVM.1 | Non-bypassability of the TSP | No Dependencies |
| FPT_SEP.1 | TSF domain separation | No Dependencies |
| FPT_STM.1 | Reliable time stamps | No Dependencies |
| IDS_ANL.1 | Analyzer analysis | No Dependencies |
| IDS_RCT.1 | Analyzer react | No Dependencies |
| IDS_RDR.1 | Restricted data review | No Dependencies |
| IDS_SDC.1 | Sensor Data Collection | No Dependencies |
| IDS_STG.1 | Guarantee of analyzer data availability | No Dependencies |

### 5.1.1 FAU_GEN.1 Audit data generation

**FAU_GEN.1.1** The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *not specified* level of audit; and

c) [Access to the TOE and access to event data].

**Table 12** Auditable Events

| Component | Event | Details |
|---|---|---|
| FAU_GEN.1 | Start- up and shutdown of audit functions | |
| FAU_GEN.1 | Access to TOE | |
| FAU_GEN.1 | Access to the TOE event data | **Object ID, Requested access** |
| FAU_SAR.2 | Unsuccessful attempts to read information from the audit records | |
| FIA_UAU.2 | All use of the web authentication mechanism | **User identity** |
| FIA_UID.2 | All use of the web identification mechanism | **User identity** |
| FMT_MOF.1 | All modifications in the behaviour of the functions of the TSF | |
| FMT_MTD.1(1),(2),(3) | All modifications to the values of TSF data | |
| FMT_SMR.1 | Modifications to the group of users that are part of a role | **User identity** |

**FAU_GEN.1.2** The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [the additional information specified in the Details column of Table 23 Auditable Events]**.**

### 5.1.2 FAU_SAR.1 Audit review

**FAU_SAR.1.1** The TSF shall provide [Admin, Security Analyst, Operator] with the capability to read [all information] from the audit records.

**FAU_SAR.1.2** The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

### 5.1.3 FAU_SAR.2 Restricted audit review

**FAU_SAR.2.1** The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

### 5.1.4 FAU_STG.2 Guarantees of audit data availability

**FAU _STG.2.1** The TSF shall protect the stored audit records from unauthorized deletion.

**FAU_STG.2.2** The TSF shall be able to *detect* unauthorized modifications to the stored audit records in the audit trail.

**FAU_STG.2.3** The TSF shall ensure that [97.5% of all hard drive stored] audit records will be maintained when the following conditions occur: *audit storage exhaustion*.

*Application Note: The percentage of hard drive storage for audit storage exhaustion is set at 97.5% and is not changeable. The TOE must be configured to send an e-mail message to an administrator when the database, which includes the audit trail, is within 2.5% of filling. This percentage is not a settable parameter. Only the sending of an e-mail is a settable parameter.*

### 5.1.5 FAU_STG.4 Prevention of audit data loss

**FAU_STG.4.1** The TSF shall *overwrite the oldest stored audit records* and [send an alarm] if the audit trail is full.

### 5.1.6 FCS_CKM.1(1)Crytpographic Key Generation (SSH)

**FCS_CKM.1.1(1)** The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [2048 bits] that meet the following: [ANSI X9.31 and ANSI X9.80]

### 5.1.7 FCS_CKM.1(2) Cryptographic key generation (HTTPS/SSL)

**FCS_CKM.1.1(2)**The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [RSA] and specified cryptographic key sizes [1024 bits] that meet the following: [ANSI X9.31 and ANSI X9.80].

### 5.1.8 FCS_CKM.2 Cryptographic Key Distribution

**FCS_CKM.2.1** The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [diffie-hellman-group1-sha1] that meets the following: [RFC 4251, RFC 4252, RFC 4253, RFC 4254: SSHv1 or SSHv2 ]

### 5.1.9 FCS_CKM.4 Cryptographic Key Destruction

**FCS_CKM.4.1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [overwrite method] that meets the following: [no standard].

*Application Note: No formal key destruction method is followed for SSHv1 or SSHv2 and SSLv2 or SSLv3. Keys are overwritten as new keys are loaded.*

### 5.1.10 FCS_COP.1(1) Cryptographic Operation (SSH Confidentiality)

**FCS_COP.1.1(1)** The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [AES, TDES, and blowfish] and cryptographic key sizes [168 bits (TDES), 128 bits (Blowfish), 128 bits, 192 bits, 256 bits (AES)] that meet the following: [FIPS 46-3 (TDES), FIPS 197(AES), RFC 2451 (Blowfish)].

### 5.1.11 FCS_COP.1(2) Cryptographic Operation (SSH Integrity)

**FCS_COP.1.1(2)** The TSF shall perform [secure hash (message digest) computation] in accordance with a specified cryptographic algorithm [HMAC-SHA1 and HMAC-MD5] and cryptographic key sizes [160 bits (HMAC-SHA1), and 128 bits (HMAC-MD5)] that meet the following: [FIPS 198 and RFC 2104 HMAC-SHA1, RFC 1321 (HMAC-MD5)].

### 5.1.12 FCS_ COP.1(3): Cryptographic Operation (HTTPS/SSL)

**FCS_COP.1.1(3)** The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [128 bits] that meet the following: [FIPS 197].

### 5.1.13 FIA_UAU.2 Timing of authentication

**FIA_UAU.2.1** The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

### 5.1.14 FIA ATD.1 User attribute definition

**FIA_ATD.1.1** The TSF shall maintain the following list of security attributes belonging to individual users:

a) [User identity;
b) Authentication data;
c) Authorisations;] and
d) [Group].

### 5.1.15 FIA_UID.2 Timing of identification

**FIA_UID.2.1** The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

### 5.1.16 FMT_MOF.1 Management of security functions behaviour

**FMT_MOF.1.1** The TSF shall restrict the ability to *modify the behaviour of* the functions [of analysis and reaction] to [Admin role and Security Analyst role].

*Application Note: For FMT_MOF.1, a Security Analyst may only configure alerts for rules they have defined. The Administrator has the ability to modify all aspects of the analysis and reaction functions.*

### 5.1.17 FMT_MTD.1(1) Management of TSF data

**FMT_MTD.1.1(1)** The TSF shall restrict the ability to *query* [and add event and audit data, and shall restrict the ability to query,and modify all other TOE data] to [Admin].

*Application Note: For FMT_MTD.1(1), "…and modify all other TOE data" includes adding and deleting sensors and modifying user accounts. Modifying should be understood to include adding and deleting.*

### 5.1.18 FMT_MTD.1(2) Management of TSF data (User Accounts)

**FMT_MTD.1.1(2)** The TSF shall restrict the ability to *add, modify [and delete]* the [Attributes defined in the IDS_RCT.1 (Notification attributes)] to [Administrator and Security Analyst].

### 5.1.19 FMT_MTD.1(3) Management of TSF data (TOE Configuration)

**FMT_MTD.1.1(3)** The TSF shall restrict the ability to *query* [TOE configuration information] to [the Administrator, Security Analyst and Operator].

### 5.1.20 FMT_SMF.1 Specification of Management Functions

**FMT_SMF.1.1** The TSF shall be capable of performing the following security management functions: [

a) the ability to add and delete Sensor devices;
b) the ability to modify behavior of System data collection, analysis and reaction;
c) the ability to query and add event and audit data;
d) the ability to add, modify and delete user accounts and
e) the ability to query and modify all other TOE data.].

### 5.1.21 FMT_SMR.1 Security roles

**FMT_SMR.1.1** The TSF shall maintain the **following** roles [Admin, Security Analyst and Operator]]**.**

**FMT_SMR.1.2** The TSF shall be able to associate users with roles.

*Application Note: The Notification Role has no access to TOE resources and is only used for receiving alerts.*

### 5.1.22 FPT_ITC.1 Inter-TSF confidentiality during transmission

**FPT_ITC.1.1** The TSF shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

*Application Note: This requirement applies to the administrative access via SSH to the TOE CLI or SSLv2 or SSLv3 for the administrator GUI only.*

### 5.1.23 FPT_ITI.1 Inter-TSF detection of modification

**FPT_ITI.1.1** The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [all incorrect Message Authentication Code (MAC)].

**FPT_ITI.1.2** The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [drop network packet and request resend for those packets with incorrect MACs] if modifications are detected.

*Application Note: The integrity provided by FPT_ITC.1 and FPT_ITI.1 is not meant to apply to email, SNMPv1, pager and SMS messages. Only administrative sessions are protected. This requirement applies to the administrative access via SSH to the TOE CLI or SSLv2 or SSLv3 for the administrator GUI only.*

### 5.1.24 FPT_RVM.1 Non-bypassability of the TSP

**FPT_RVM.1.1** The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

### 5.1.25 FPT_SEP.1 TSF domain separation

**FPT_SEP.1.1** The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

**FPT_SEP.1.2** The TSF shall enforce separation between the security domains of subjects in the TSC.

### 5.1.26 FPT_STM.1 Reliable time stamps

**FPT_STM.1.1** The TSF shall be able to provide reliable time stamps for its own use.

### 5.1.27 IDS_SDC.1 Sensor data collection [Explicit Stated SFR for the TOE]

**IDS_SDC.1.1** The TSF shall be able to collect or receive raw data in the form of device logs and/or alerts and/ or NetFlow communications from its configured sensors.

**IDS_SDC.1.2** The TSF shall, at a minimum, collect or receive the following information from configured sensors:

a) Originating host
b) Date and time of collection by the sensor
c) Device type
d) Event type

*Application Note: 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.*

### 5.1.28 IDS_ANL.1 Analyser analysis [Explicit Stated SFR for the TOE]

**IDS_ANL.1.1** The TSF shall perform the following analysis function(s) on all raw data collected or received:

a) *statistical, signature;* and
b) [vector analysis].

**IDS_ANL.1.2** The TSF shall record within each analytical result at least the following information:

a) Date and time of the result, type of result, identification of data source; and
b) [No other security relevant information about the result].

### 5.1.29 IDS_RCT.1 Analyzer react [Explicit Stated SFR for the TOE]

**IDS_RCT.1.1** The TSF shall send an alarm to [the specified e-mails address(s), pager number(s), SMTP trap address(s), or to the SMS message address(s)] and take [the action of generating an Incident and recommending mitigation commands for sensors] when an intrusion is detected.

### 5.1.30 IDS_RDR.1 Restricted Data Review [Explicit Stated SFR for the TOE]

**IDS_RDR.1.1** The TSF shall provide [Admin, Security Analyst, Operator] with the capability to read [all information] from the event data.

**IDS_RDR.1.2** The TSF shall provide the event data in a manner suitable for the user to interpret the information.

**IDS_RDR.1.3** The TSF shall prohibit all users read access to the event data, except those users that have been granted explicit read-access.

### 5.1.31 IDS_STG.1 Guarantee of Analyzer Data Availability [Explicit Stated SFR for the TOE]

**IDS_STG.1.1** The TSF shall protect the stored event data from unauthorized deletion.

**IDS_ STG.1.2** The TSF shall protect the stored event data from modification.

## 5.2 TOE Security Assurance Requirements

The TOE security assurance requirements summarized in Table 13: TOE Assurance Requirements identify the management and evaluative activities required to address the threats and policies identified in section 3 of this ST. This ST complies with assurance level EAL2.

**Table 13 TOE Assurance Requirements**

| Assurance Class | Assurance Components |
|---|---|
| Configuration Management | Configuration items (ACM_CAP.2) |
| Delivery and Operations | Delivery procedures (ADO_DEL. 1)<br>Installation, generation, and start-up procedures (ADO_IGS.1) |
| Development | Informal functional specification (ADV_FSP.1)<br>Security enforcing high-level design (ADV_HLD.1)<br>Informal correspondence demonstration (ADV_RCR. 1) |
| Guidance documents | Administrator guidance (AGD_ADM. 1)<br>User guidance (AGD_USR. 1) |
| Tests | Analysis of coverage (ATE_COV. 1)<br>Functional testing (ATE_FUN. 1)<br>Independent testing - sample (ATE_IND.2) |
| Vulnerability Assessment | Strength of TOE security function evaluation (AVA_SOF. 1)<br>Developer vulnerability analysis (AVA_VLA. 1) |

# 6 TOE SUMMARY SPECIFICATION

This chapter identifies and describes the security functions implemented by the TOE and the assurance measures applied to ensure their correct implementation.

## 6.1 TOE Security Functions

### 6.1.1 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 setup 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 a user has 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 a user to supply a user identifier and a password before they are allowed to carry out any other actions with the TOE. Only users that login 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 thru the web or CLI interfaces.

The SOF for the password authentication is SOF-basic as stated and explained in section 8.6.

### 6.1.2 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 that are desired to be monitored and analyzed for intrusions. These network devices are referred to as sensors. Sensors are the networking devices that data passes through, is collected, or processed for those networks that one wants to monitor and analyze for intrusions. Sensors are routers, switches, security devices and applications (such as firewalls, intrusion detection systems [IDSs], vulnerability scanners, and antivirus applications), hosts (such as Windows, Solaris, and Linux syslogs), 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, as indicated in Table 5. 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 can not 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 are dropped. **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.

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 (see Table 5). 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.

### 6.1.3 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 were 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 that the workstation that the user is using to connect to the TOE from has a routable connection to the TOE.

Administrative access permissions are defined by the role associated with the user accessing the system. The user roles defined for the TOE are Admin, Security Analyst, and Operator. The Notification Role is considered a non-user role,. The Administrator role performs all tasks associated with the Administration Security Function as stated in the FMT requirements. The Security Analyst 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 that they define.
- **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 Administrator has capabilities of the Operator and the Security Analyst plus the Administrator may carry out all administrative operations.

### 6.1.3.1 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 which 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 user 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.

### 6.1.3.2 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 which operates in the Admin role.

#### 6.1.3.3 Sensor Administration

The analyses function of the TOE relies on the network devices, sensors, chosen to be monitored. These sensors can be added only by a user operating in the Admin role. The sensors that data are collected from can be configured through the GUI interface, or by using a seed file which 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, 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.

#### 6.1.3.4 Analyses Rule Administration

Data collected from the sensors is analyzed according to a set of analysis rules which 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.

#### 6.1.3.5 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.

### 6.1.4 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 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 predefined report format. The result contents displayed are contingent on the report format chosen. The content of the displayed results include 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.

### 6.1.5 Analysis Security Function

The TOE performs internal analysis on data it collects from sensors to identify unusual or suspect activity (security incidents, intrusions, and events) with 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 if the hardware resources storing the event data becomes exhausted or is attacked. When the hardware resources storing the event data becomes 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.

#### 6.1.5.1 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 incoming data containing security relevant information is processed by the TOE 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.

#### 6.1.5.2 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 to the TOE. 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.

### 6.1.6 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.

### 6.1.7 Audit Security Function

The TOE's Audit Security Functionality provides event auditing (based on the events listed in Table 12) and audit viewing for system functions and management functions.

#### 6.1.7.1 Management Auditing

The management auditing of the TOE records the completion of system management events submitted through the web interface in the audit trail.  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, exhaustion, an alarm is sent. The alarm is an e-mail to a configured e-mail address.

#### 6.1.7.2 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.

### 6.1.8 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 and 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.

## 6.2 Assurance Measures

The TOE satisfies CC EAL2 assurance requirements. This section identifies the Configuration Management, Delivery and Operation, Development, Flaw Remediation, Guidance Documents, Testing, and Vulnerability Assessment Assurance Measures applied by CISCO to satisfy the CC EAL2 assurance requirements. Table 14 lists the details.

**Table 14: Assurance Measures**

| Assurance Component | How requirement will be met |
|---|---|
| ACM_CAP.2<br>Configuration items | Cisco performs configuration management on configuration items of the TOE. Configuration management is performed on the TOE and the implementation representation of the TOE. The configuration items are uniquely identified and each release of the TOE has a unique reference. |
| ADO_DEL.1<br>Delivery procedures | Cisco documents the delivery procedure for the TOE to include the procedure on how to download certain components of the TOE from the Cisco website and how certain components of the TOE are physically delivered to the user. The delivery procedure detail how the end-user may determine if they have the TOE and if the integrity of the TOE has been maintained. Further, the delivery documentation describes how to acquire the proper license keys to use the TOE components. |
| ADO_IGS.1<br>Installation, generation and startup procedures | Cisco documents the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration. |
| ADV_FSP.1<br>Informal functional specification | The externally visible interfaces of the TOE used by the users of the TOE along with the description of the security functions and a correspondence between the interfaces and the security functions from the ST are documented by Cisco in their development evidence. |
| ADV_HLD.1<br>Descriptive high-level design | The subsystems and the communication between the subsystems of the TOE are documented in Cisco's development evidence. |
| ADV_RCR.1<br>Informal correspondence demonstration | The correspondence is contained in the documents used for ADV_FSP.1 and ADV_HLD.1. |
| AGD_ADM.1<br>Administrator Guidance | The administrative guidance is detailed to provide descriptions of how administrative users of the TOE can securely administer the TOE using those functions and interfaces detailed in the guidance. |
| AGD_USR.1<br>User guidance | User guidance is provided for those roles defined in the TOE that do not have all the authorizations as the administrative role. |
| ATE_COV.1<br>Evidence of coverage | Cisco demonstrates the interfaces tested during functional testing using a coverage analysis. |
| ATE_FUN.1<br>Functional testing | Cisco functional testing documentation contains a test plan, a description of the tests, along with the expected and actual results of the test conducted against the functions specified in the ST. |
| ATE_IND.2<br>Independent testing - sample | Cisco will help meet the independent testing by providing the TOE to the evaluation facility. |
| AVA_SOF.1<br>Strength of TOE security function evaluation | Cisco documented the strength of functions in the vulnerability analysis documentation. |
| AVA_VLA.1<br>Developer vulnerability analysis | Cisco carried out a vulnerability analysis search for obvious flaws and weaknesses in the TOE. |

# 7 PROTECTION PROFILE CLAIMS

## 7.1 Protection Profile Reference

This ST does not claim conformance to any registered PP.

## 7.2 Protection Profile Refinements

This ST does not claim conformance to any registered PP.

## 7.3 Protection Profile Additions

This ST does not claim conformance to any registered PP.

# 8 RATIONALE

## 8.1 Security Objectives Rationale

This section demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective.  Table 15 and Table 16 provide the mapping and rationale for the security objectives identified in Chapter 4 and the assumptions, threats and policies identified in Chapter 3.

**Table 15: Threats, Assumptions, and Policies to Security Objectives Mapping**

| | O. PROTCT | O.IDACTS | O.RESPON | O.EADMIN | O.ACCESS | O.IDAUTH | O.OFLOWS | O.AUDITS | O.INTEGR | O. EXPORT | OE.INSTAL | OE. PHYCAL | OE.CREDEN | OE.PERSON | OE.INTROP | OE.INTEGR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A.ACCESS | | | | | | | | | | | | | | | X | |
| A.INTEGR | | | | | | | | | | | | | | | | X |
| A.PROTCT | | | | | | | | | | | | X | | | | |
| A.LOCATE | | | | | | | | | | | | X | | | | |
| A.MANAGE | | | | | | | | | | | | | | X | | |
| A.NOEVIL | | | | | | | | | | | X | X | X | | | |
| A.NOTRUST | | | | | | | | | | | | X | X | | | |
| T.COMINT | X | | | | X | X | | | X | | | | | | | |
| T.COMDIS | X | | | | X | X | | | | X | | | | | | |
| T.LOSSOF | X | | | | X | X | | | X | | | | | | | |
| T.NOHALT | | X | | | X | X | | | | | | | | | | |
| T.PRIVIL | X | | | | X | X | | | | | | | | | | |
| T.IMPCON | | | | X | X | X | | | | | X | | | | | |
| T.INFLUX | | | | | | | X | | | | | | | | | |
| T.INTEGR | | | | | | | | | | | | | | | | X |
| T.FALACT | | | X | | | | | | | | | | | | | |
| T.FALREC | | X | | | | | | | | | | | | | | |
| T.FALASC | | X | | | | | | | | | | | | | | |
| P.ANALYZ | | | X | | | | | | | | | | | | | |
| P.DETECT | | X | | | | | | X | | | | | | | | |
| P.MANAGE | X | | | X | X | X | | | | | X | | X | X | | |
| P.ACCESS | X | | | | X | X | | | | | | | | | | |
| P.ACCACT | | | | | | X | | X | | | | | | | | |
| P.INTEGR | | | | | | | | | X | | | | | | | |
| P.PROTCT | | | | X | | | | | | | | X | | | | |

**Table 16: Threats, Assumptions, and Policies to Security Objectives Rationale**

| Threat/Assumption /Policy | Security Objectives Rationale |
|---|---|
| A.ACCESS | The OE.INTROP objective ensures the TOE has the needed access. |
| A.INTEGR | The OE.INTEGR objective ensures 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 or cryptographic means. |
| A.PROTCT | The OE.PHYCAL provides for the physical protection of the TOE hardware and software. |
| A.LOCATE | The OE.PHYCAL provides for the physical protection of the TOE. |
| A.MANAGE | The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE. |
| A.NOEVIL | The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data. |
| A.NOTRUST | The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data. |
| T.COMINT | The O.IDAUTH (FAU_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_ATD.1, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), FMT_SMF.1, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_RDR.1, IDS_STG.1) objective provides for authentication of users prior to any TOE data access.<br>The O.ACCESS (FUA_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), IDS_RDR.1, IDS_STG.1) objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data.<br>The O.INTEGR (FAU_STG.2, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),, FPT_ITC.1, FPT_ITI.1, FPT_RVM.1, FPT_SEP.1, IDS_STG.1) objective ensures no TOE data will be modified.<br>The O.PROTCT (FAU_STG.2, FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), |

| Threat/Assumption /Policy | Security Objectives Rationale |
|---|---|
| | FMT_MTD.1(3),, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_STG.1) objective addresses this threat by providing TOE self-protection. |
| T.COMDIS | The O.IDAUTH (FAU_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_ATD.1, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),, FMT_SMF.1, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_RDR.1, IDS_STG.1) objective provides for authentication of users prior to any TOE data access.<br>The O.ACCESS (FUA_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), IDS_RDR.1, IDS_STG.1) objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data.<br>The O.EXPORT (FPT_ITC.1, FPT_ITI.1) objective ensures that confidentiality of TOE data will be maintained.<br>The O.PROTCT (FAU_STG.2, FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_STG.1) objective addresses this threat by providing TOE self-protection. |
| T.LOSSOF | The O.IDAUTH (FAU_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_ATD.1, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),, FMT_SMF.1, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_RDR.1, IDS_STG.1) objective provides for authentication of users prior to any TOE data access.<br>The O.ACCESS (FUA_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), IDS_RDR.1, IDS_STG.1) objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data.<br>The O.INTEGR (FAU_STG.2, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),, FPT_ITC.1, FPT_ITI.1, FPT_RVM.1, FPT_SEP.1, IDS_STG.1) objective ensures no TOE data will be deleted.<br>The O.PROTCT (FAU_STG.2, FMT_MOF.1, FMT_MTD.1(1), |

| Threat/Assumption /Policy | Security Objectives Rationale |
|---|---|
| | FMT_MTD.1(2), FMT_MTD.1(3),, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_STG.1) objective addresses this threat by providing TOE self-protection. |
| T.NOHALT | The O.IDAUTH (FAU_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_ATD.1, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),, FMT_SMF.1, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_RDR.1, IDS_STG.1) objective provides for authentication of users prior to any TOE function accesses.<br>The O.ACCESS (FUA_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),IDS_RDR.1, IDS_STG.1) objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.<br>The O.IDACTS (FMT_SMR.1, IDS_ANL.1) objective addresses this threat by requiring the TOE to collect all events, including those attempts to halt the TOE. |
| T.PRIVIL | The O.IDAUTH (FAU_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_ATD.1, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),, FMT_SMF.1, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_RDR.1, IDS_STG.1) objective provides for authentication of users prior to any TOE function accesses.<br>The O.ACCESS (FUA_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), IDS_RDR.1, IDS_STG.1) objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.<br>The O.PROTCT (FAU_STG.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_STG.1) objective addresses this threat by providing TOE self-protection. |
| T.IMPCON | The O.INSTAL objective states the authorized administrators will configure the TOE properly.<br>The O.EADMIN (FAU_SAR.1, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_RDR.1) objective ensures the TOE has all the necessary administrator functions to manage the product. |

| Threat/Assumption /Policy | Security Objectives Rationale |
|---|---|
| | The O.IDAUTH (FAU_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_ATD.1, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),, FMT_SMF.1, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_RDR.1, IDS_STG.1) objective provides for authentication of users prior to any TOE function accesses.<br>The O.ACCESS (FUA_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), IDS_RDR.1, IDS_STG.1) objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. |
| T.INFLUX | The O.OFLOWS (FAU_STG.2, FAU_STG.4, FMT_SMR.1, IDS_STG.1) objective counters this threat by requiring the TOE handle data storage overflows. |
| T.INTEGR | The OE.INTEGR environment objective counters this threat by requiring an authorized administrator to 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. |
| T.FALACT | The O.RESPON (FMT_SMR.1, IDS_RCT.1) objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity. |
| T.FALREC | The O.IDACTS (FMT_SMF.1, IDS_ANL.1) objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source. |
| T.FALASC | The O.IDACTS (FMT_SMF.1, IDS_ANL.1) objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources. |
| P.ANALYZ | The O.RESPON (FMT_SMR.1, IDS_RCT.1) objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity. |
| P.DETECT | The O.IDACTS (FMT_SMF.1, IDS_ANL.1) objective requires analytical processes be applied to data collected from Sensors and Scanners. |
| P.MANAGE | The O.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN (FAU_SAR.1, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_RDR.1) objective ensures there is a set of functions for administrators to use. The O.INSTAL objective supports the O.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. |

| Threat/Assumption /Policy | Security Objectives Rationale |
|---|---|
| | The O.IDAUTH (FAU_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_ATD.1, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),, FMT_SMF.1, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_RDR.1, IDS_STG.1) objective provides for authentication of users prior to any TOE function accesses.<br>The O.ACCESS (FUA_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), IDS_RDR.1, IDS_STG.1) objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.<br>The O.CREDEN objective requires administrators to protect all authentication data.<br>The O. PROTCT (FAU_STG.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_STG.1) objective provides for TOE self-protection. |
| P.ACCESS | The O.IDAUTH (FAU_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_ATD.1, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),, FMT_SMF.1, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_RDR.1, IDS_STG.1) objective provides for authentication of users prior to any TOE function accesses.<br>The O.ACCESS (FUA_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3), IDS_RDR.1, IDS_STG.1)objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.<br>The O.PROTCT (FAU_STG.2, FMT_MOF.1, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_STG.1) objective provides for TOE self-protection. |
| P.ACCACT | The O.AUDITS (FAU_GEN.1, FAU_STG.4, FPT_RVM, FPT_SEP.1, FPT_STM.1) objective implements this policy by requiring auditing of all data accesses and use of TOE functions.<br>The O.IDAUTH (FAU_SAR.2, FAU_STG.2, FIA_UAU.2, FIA_ATD.1, FIA_UID.2, FMT_MOF.1, FMT_MTD.1(1), |

| Threat/Assumption /Policy | Security Objectives Rationale |
|---|---|
|  | FMT_MTD.1(2), FMT_MTD.1(3),, FMT_SMF.1, FMT_SMR.1, FPT_RVM.1, FPT_SEP.1, IDS_RDR.1, IDS_STG.1) objective supports this objective by ensuring each user is uniquely identified and authenticated. |
| P.INTEGR | The O.INTEGR (FAU_STG.2, FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),, FPT_ITC.1, FPT_ITI.1, FPT_RVM.1, FPT_SEP.1, IDS_STG.1) objective ensures the protection of data from modification. |
| P.PROTCT | The O.OFLOWS (FAU_STG.2, FAU_STG.4, FMT_SMR.1, IDS_STG.1) objective requires the TOE handle disruptions.<br>The O.PHYCAL objective protects the TOE from unauthorized physical modifications. |

## 8.2 Rationale for Security Functional Requirements

### 8.2.1 Rationale for Security Functional Requirements of the TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the Security Functional Requirements are suitable to address the security objectives. Table 17 identifies each Security Functional Requirement identified in Section 5.1, the TOE security objective(s) identified in Section 4.1 that addresses it. Table 17 and Table 18 provide the mapping and rationale for inclusion of each SFR in this ST.

**Table 17: TOE Security Functional Requirement to TOE Security Objectives Mapping**

| | O. PROTCT | O.IDACTS | O.RESPON | O.EADMIN | O.ACCESS | O.IDAUTH | O.OFLOWS | O.AUDITS | O.INTEGR | O. EXPORT |
|---|---|---|---|---|---|---|---|---|---|---|
| FAU_GEN.1 | | | | | | | | X | | |
| FAU SAR.1 | | | | X | | | | | | |
| FAU_SAR.2 | | | | | X | X | | | | |
| FAU_STG.2 | X | | | | X | X | X | | X | |
| FAU_STG.4 | | | | | | | X | X | | |
| FCS_CKM.1(1) | X | | | | | | | | | |
| FCS_CKM.1(2) | X | | | | | | | | | |
| FCS_CKM.2 | X | | | | | | | | | |
| FCS_CKM.4 | X | | | | | | | | | |
| FCS_COP.1(1) | X | | | | | | | | | |
| FCS_COP.1(2) | X | | | | | | | | | |
| FCS_COP.1(3) | X | | | | | | | | | |
| FIA_UAU.2 | | | | | X | X | | | | |
| FIA_ATD.1 | | | | | | X | | | | |
| FIA_UID.2 | | | | | X | X | | | | |
| FMT_MOF.1 | X | | | | X | X | | | | |
| FMT_MTD.1(1) | X | | | | X | X | | | X | |
| FMT_MTD.1(2) | X | | | | X | X | | | X | |
| FMT_MTD.1(3)_ | X | | | | X | X | | | X | |
| FMT_SMF.1 | X | X | X | X | | X | X | | | |
| FMT_SMR.1 | | | | | | X | | | | |
| FPT_ITC.1 | | | | | | | | | X | X |
| FPT_ITI.1 | | | | | | | | | X | X |
| FPT_RVM.1 | X | | | X | | X | | X | X | |
| FPT_SEP.1 | X | | | X | | X | | X | X | |
| FPT_STM.1 | | | | | | | | X | | |
| IDS_ANL.1 | | X | | | | | | | | |
| IDS_RCT.1 | | | X | | | | | | | |
| IDS_RDR.1 | | | | X | X | X | | | | |
| IDS_SDC.1 | | X | | | | | | | | |
| IDS_STG.1 | X | | | | X | X | X | | X | |

**Table 18: TOE Security Functional Requirement to TOE Security Objectives Rationale**

| Security Objective (TOE) | Security Functional Requirement Rationale |
|---|---|
| O. PROTCT | The TOE protects the audit data from deletion as well as guarantees the availability of the audit data in the event of storage exhaustion or attack [FAU_STG.2]. The TOE protects the analyzed data and analysis results from any modification and unauthorized deletion, as well as guarantees the availability of the data in the event of storage exhaustion or attack [IDS_STG.1]. The TOE provides the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the TOE may query the analysis data, the analyzed results, and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),]. The TOE provides the management security functions to manage the security attributes for users [FMT_SMF.1]. The TOE ensures that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF protects itself form interference that would prevent it from performing its functions [FPT_SEP.1]. The TOE provides protection of its management interfaces.[ FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3)] |
| O.IDACTS | The TOE collects or receives raw data from sensors it is configured to collect or receive from. This data includes logs and/or alerts, and/or events and/or NetFlow communications. [IDS_SDC.1].<br>The TOE performs analysis and generates conclusions [IDS_ANL.1]. The TOE provides the management security functions to manage the rules and the sources for data to be analyzed that it applies its analytic processes that are used to derive its analysis conclusions [FMT_SMF.1]. |
| O.RESPON | The TOE responds accordingly in the event of a detected intrusion based on how it has been configured [IDS_RCT.1]. The TOE provides the management security functions that allows for the management of the TOE’s response to intrusions [FMT_SMF.1]. |

| Security Objective (TOE) | Security Functional Requirement Rationale |
|---|---|
| O.EADMIN | The TOE provides the ability to review and manage the audit trail of the TOE [FAU_SAR.1]. The TOE provides the ability for authorized administrators to view the TOE data [IDS_RDR.1].<br>The TOE provides the management security functions for the security functions of the TOE [FMT_SMF.1]. The TOE ensures that all functions are invoked and succeed before each function may proceed [FPT_RVM.1].<br>The TSF protects itself from interference that would prevent it from performing its functions [FPT_SEP.1]. |
| O.ACCESS | The TOE restricts the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The TOE restricts the review of TOE data to those granted with explicit read-access [IDS_RDR.1]. The TOE protects the audit data from deletion as well as guarantees the availability of the audit data in the event of storage exhaustion or attack [FAU_STG.2]. The TOE protects the TOE data from any modification and unauthorized deletion [IDS_STG.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.2, FIA_UAU.2]. The TOE provides the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the TOE may query and add analysis and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),]. |

| Security Objective (TOE) | Security Functional Requirement Rationale |
|---|---|
| O.IDAUTH | The TOE restricts the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The TOE restricts the review of collected data and analysis results to those granted with explicit read-access [IDS_RDR.1]. The TOE protects the stored audit records from unauthorized deletion [FAU_STG.2]. The TOE protects the collected data and analysis conclusions from unauthorized deletion as well as guarantee the availability of the data in the event of storage exhaustion or attack [IDS_STG.1].<br>Security attributes of subjects used to enforce the authentication policy of the TOE are defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.2, FIA_UAU.2]. The TOE provides the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the TOE may query and add collected data, analysis conclusions and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),]. The TOE provides the security management functions for the security attributes for defining an authorized user of the TOE [FMT_SMF.1]. The TOE recognizes distinct administrative, analyst and user roles [FMT_SMR.1].<br>The TOE ensures that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF protects itself form interference that would prevent it from performing its functions [FPT_SEP.1] |
| O.OFLOWS | The TOE protects the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion or attack [FAU_STG.2]. The TOE prevents the loss of audit data in the event its audit trail is full [FAU_STG.4]. The TOE provides the security management functions that manage the use of storing of data on the TOE [FMT_SMF.1]. The TOE protects the collected data and analysis conclusions from any modification and unauthorized deletion, as well as guarantees the availability of the data in the event of storage exhaustion [IDS_STG.1]. |

| Security Objective (TOE) | Security Functional Requirement Rationale |
|---|---|
| O.AUDITS | Security-relevant events are defined and auditable in the TOE [FAU_GEN.1]. The TOE prevents the loss of collected data in the event its audit trail is full [FAU_STG.4]. The TOE provides the capability to select which security-relevant events to audit [FAU.SEL.1]. The TOE ensures that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF protects itself form interference that would prevent it from performing its functions [FPT_SEP.1]. Time stamps associated with an audit record are reliably generated by the TOE [FPT_STM.1]. |
| O.INTEGR | The TOE protects the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion or attack [FAU_STG.2]. The TOE protects the collected data and analysis conclusions from any modification and unauthorized deletion [IDS_STG.1]. For data collected from sensor devices, Toe involvement will begin once the data enters the TOE boundary. Only authorized administrators of the TOE may query or add audit and collected data [FMT_MTD.1(1), FMT_MTD.1(2), FMT_MTD.1(3),]. The TOE protects the collected data from modification and ensures its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1]. The TOE ensures that all functions to protect the data are not bypassed [FPT_RVM.1]. The TSF protects itself from interference that would prevent it from performing its functions [FPT_SEP.1]. |
| O. EXPORT | The TOE protects the event data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1]. |

## 8.3 TOE Security Functions

This section demonstrates the suitability of the security functions defined in section 6.1 of meeting the TOE’s Security Functional Requirements identified in Section 5.1 and that the security functional requirements are completely and accurately met by the TOE’s Security Functions identified in Sections 6.1.

Table 19 demonstrates the correspondence between the Security Functions and the TOE Security Functional Requirements. With the demonstration of correspondence given in Table 20 and the descriptions of the security functions given in Section 6.1 on how the security functions are providing the functionality to meet the security functional requirements this provides the evidence of suitability of the security functions in meeting the security functional requirements stated in Section 5.1.

**Table 19: TOE Security Functional Requirement to TOE Security Functions Mapping**

| TOE Security Functional Requirement | Identification and Authentication Security Function | External Device Communication Security Function | Administration Security Function | Reporting Security Function | Analysis Security Function | Reaction Security Function | Audit Security Function | Self Protection Security Function |
|---|---|---|---|---|---|---|---|---|
| FAU_GEN.1 | | | | | | | X | |
| FAU_SAR.1 | | | | | | | X | |
| FAU_SAR.2 | | | | | | | X | |
| FAU_STG.2 | | | | | | | X | |
| FAU_STG.4 | | | | | | | X | |
| FCS_CKM.1(1) | | | | | | | | X |
| FCS_CKM.1(2) | | | | | | | | X |
| FCS_CKM.2 | | | | | | | | X |
| FCS_CKM.4 | | | | | | | | X |
| FCS_COP.1(1) | | | | | | | | X |
| FCS_COP.1(2) | | | | | | | | X |
| FCS_COP.1(3) | | | | | | | | X |
| FIA_UAU.2 | X | | | | | | | |
| FIA_ATD.1 | X | | | | | | | |
| FIA_UID.2 | X | | | | | | | |
| FMT_MOF.1 | | | X | | | | | |
| FMT_MTD.1(1) | | | X | | | | | |
| FMT_MTD.1(2) | | | X | | | | | |
| FMT_MTD.1(3) | | | X | | | | | |
| FMT_SMF.1 | | | X | | | | | |
| FMT_SMR.1 | | | X | | | | | |
| FPT_ITC.1 | | | X | | | | | |
| FPT_ITI.1 | | | X | | | | | |

| TOE Security Functional Requirement | Identification and Authentication Security Function | External Device Communication Security Function | Administration Security Function | Reporting Security Function | Analysis Security Function | Reaction Security Function | Audit Security Function | Self Protection Security Function |
|---|---|---|---|---|---|---|---|---|
| FPT_RVM.1 | | | | | | | | X |
| FPT_SEP.1 | | | | | | | | X |
| FPT_STM.1 | | | | | | | X | |
| IDS_ANL.1 | | X | | | X | | | |
| IDS_RCT.1 | | | | | | X | | |
| IDS_RDR.1 | | | | X | | | | |
| IDS_SDC.1 | | X | | | X | | | |
| IDS_STG.1 | | | | | X | | | |

**Table 20 Rationale of how the SF(s) meet the SFR(s)**

| SFR | SF and Rationale |
|---|---|
| FAU_GEN.1 | Is implemented by the Audit Security Function. The Audit security function generates audit records for access to the TOE which shows access to the TOE and analysis data stored and processed by the TOE. All users that operate in the Admin, Security Analyst, and Operator role are allowed to access and review all audit records and the audit trail. The TOE generates audit records when roles are changed; rules are created, modified, or deleted; when sensors, are added or deleted; and when alerts are created or modified. |
| FAU_SAR.1 | Is implemented by the Audit Security Function. The TOE provides a web interface to users operating in the Admin, Security Analyst, and Operator roles to review the audit records of the TOE. The web interface provides the audit records in HTML format that is suitable for human users to review. |
| FAU_SAR.2 | Is implemented by the Audit Security Function. The TOE only allows users operating in the Admin, Security Analyst, and Operator roles to review the |

| SFR | SF and Rationale |
|---|---|
| | audit records. The users operating in any one of these three roles must successfully identify and authenticate themselves to the TOE before they are allowed to access the TOE and therefore be able to review the audit records. Identification and authentication to the TOE is the explicit request of a user in one of the roles that must be successfully made to be able to review the audit records and the user must be granted the explicit read access by having a user account setup for the user with one of these roles and their identification and authentication information. |
| FAU_STG.2 | Is implemented by the Audit Security Function. The TOE requires users to successfully identify and authenticate themselves to the TOE before they are allowed to carry out any other actions with the TOE. All users that have permission to log into the TOE (those users operating in the Admin, Security Analyst and Operator roles) are allowed to view the audit records only the Admin role users are allowed to purge (back up) the audit records from the TOE. The purge event is audited when a user operating in the Admin role carries this activity out. The generation of the audit record is a detection capability that can be used to determine if an unauthorized modification to the stored audit records have occurred with the audit trail. |
| FAU_STG.4 | Is implemented by the Audit Security Function. The TOE will overwrite the oldest stored audit records, by purging the oldest data, when the audit trail becomes full and send an e-mail (an alarm) to an administrator of the TOE indicating that the audit trail is within 2.5% of filling up. |
| FCS_CKM.1(1) | Is implemented by the Self-protection Function by contributing to the SSHv1 or SSHv2 functionality to protect the management interface by RSA key generation. |
| FCS_CKM.1(2) | Is implemented by the Self-protection Function by contributing to the SSLv2 or SSLv3 functionality to protect the management interface by RSA key generation. |
| FCS_CKM.2 | Is implemented by the Self Protection Security Function by contributing to the SSHv1 or SSHv2 functionality to protect the management interface by diffie hellman distribution method. |
| FCS_CKM.4 | Is implemented by the Self Protection Security Function by contributing to the SSHv1 or SSHv2 functionality to protect the management interfaces by using overwrite method for key destruction |
| FCS_COP.1(1) | Is implemented by the Self Protection Security Function by contributing to the SSHv1 or SSHv2 functionality to protect the management interface (encryption and decryption). |
| FCS_COP.1(2) | Is implemented by the Self Protection Security Function by contributing to the SSHv1 or SSHv2 functionality to protect the management interface (secure hash computation). |
| FCS_COP.1(3) | Is implemented by the Self Protection Security Function by contributing to the SSLv2 or SSLv3 functionality to protect the management interface (encryption and decryption). |
| FIA_UAU.2 | Is implemented by the Identification and Authentication Security Function. The TSF ensures that a user is authenticated before any other actions are allowed within the TSF. |
| FIA_ATD.1 | Is implemented by the Identification and Authentication Security Function. |

| SFR | SF and Rationale |
|---|---|
| | The Identification and Authentication security function maintains the user security attributes of identifier, password information (authentication data), the user authorizations (the users role), and the group the user belongs. |
| FIA_UID.2 | Is implemented by the Identification and Authentication Security Function. The TSF ensures that a user is authenticated before any other actions are allowed within the TSF. |
| FMT_MOF.1 | Is implemented by the Administration Security Function. The TSF restricts the ability to modify the behavior of the analysis and reaction capabilities of the TOE to the authorized Analyzer administrators, those users that operate at the Admin role level of privilege. The TSF restricts the ability to modify the behavior of the analysis and reactions capabilities of the TOE by requiring all users to successfully identify and authenticate themselves to the TOE before being allowed to carry out any types of administrative functions and by maintaining a user profile that contain a role security attribute. The role security attribute defines the types of actions that the user can carry out on the TOE and the TOE requires users to have the Admin role to modify the analysis and reaction capabilities of the TOE. |
| FMT_MTD.1(1) | Is implemented by the Administration Security Function. The TSF restricts the ability to query and add analyzed data and audit data and to query and modify all other TOE data- including modification of user accounts and adding and deleting sensors- to those users operating in the Admin role. |
| FMT_MTD.1(2) | Is implemented by the Administration Security Function. The TSF restricts the ability to add, modify and delete user accounts for the Notification Role to the Security Analyst and the Administrator. |
| FMT_MTD.1(3) | Is implemented by the Administration Security Function. The TSF restricts the ability to query TOE configuration information to users in the Administrator, Security Analyst and Operator roles. |
| FMT_SMF.1 | Is implemented by the Administration Security Function. The TOE provides a capability to allow for users to communicate with the TSF through a web interface. The web interface provides access to those authorized to those management functions that are necessary to management the security attributes and security functions defined in the security functional requirement defined in section 5 of this ST. |
| FMT_SMR.1 | Is implemented by the Administration Security Function. The TOE implements the user roles of Admin, Security Analyst, and Operator. The Notification Role is a non-user role. Each role has specific capabilities that it can or can not use and the roles are hierarchical as listed with Admin being the most privilege role, role that can use all capabilities of the TOE. |
| FPT_ITC.1 | Is implemented by the Administration Security Function. The TOE uses SSLv2 or SSLv3 as the security capability to protect the confidentiality of communications that happen between it and the web browser interface that the TOE provides to authorized users of the TOE. The SSLv2 or SSLv3 communication protects the confidentiality of passwords, user IDs, roles, rule definitions, and reaction and mitigation settings that may be set, modified or configured through the web browser interface to the TOE.<br>The TOE uses SSLv2 or SSLv3 for communications that may take place between local and global controllers. SSLv2 or SSLv3 is used to protect the rules, analysis settings, and other configuration data that may pass between |

| SFR | SF and Rationale |
|---|---|
| | the TOEs communicating with each other. |
| FPT_ITI.1 | Is implemented by the Administration Security Function. The TOE uses the features of SSLv2 or SSLv3 to detect modification of TSF data when the TSF data is being transmitted between the TOE and a web browser and between TOE components.<br>Specifically the message authentication code (MAC) is used of SSLv2 or SSLv3 to detect modification of TSF data. If any of the transmissions are modified in transit the MAC will indicate this with an error and the packet(s) will be dropped. The TOE will request a resend of dropped packets and will only accept those packets that have the proper MAC. The TSF data that is protected by detection of modification with this SSLv2 or SSLv3 capability are rules, user IDs, passwords, audit data, analyzed data, reaction/mitigation settings, and the settings dealing with the collection of data to be analyzed. |
| FPT_RVM.1 | Is implemented by the Self Protection Security Function. The TOE has well defined user and analysis interfaces. All the action through these interfaces are mediated and only can carry out a well defined set of actions based on the type of interface. The TOE makes sure that security enforcing functions are invoked and succeed before allowing any other mediated action to occur. |
| FPT_SEP.1 | Is implemented by the Self Protection Security Function. The Self-Protection Function provides a protected execution domain and separation of the processing of information flows that deal with administration of the TOE and those that deal with collecting and analysis of collected data. The TOE is a dedicated device, with no general purpose operating system capabilities or programming interfaces provided. No untrusted processes are permitted on the TOE. |
| FPT_STM.1 | Is implemented by the Audit Security Function. The TOE has an internal system clock which is used to generate timestamps for audit records. |
| IDS_ANL.1 | Is implemented by the External Device Communication Security Function and the Analysis Security Function. The TOE performs statistical, signature, and vector analysis on the data that it collects or receives from external network devices and appliances that it has been configured to collect or receive from. This analysis is performed based on a preset number of rules and the rules that are configured into the TOE by an authorized user with the proper privileges. |
| IDS_RCT.1 | Is implemented by the Reaction Security Function. Upon detection of an incident the TOE will send an e-mail to the specified e-mail address(s) that have been configured to receive an alarm, send a page to the configured pager number(s), send an SMS message to the configured SMS message address(s) that are to receive and alarm or send an SNMPv1 trap to the configured SNMPv1 trap IP addresses identifying as an alert that an incident is occurring. Further, the TOE is able to recommend mitigation commands for particular sensors that a user may send or manually type into the sensor via SNMP. For those sensors that have mitigation commands configured for them the TOE displays the mitigation command to an authorized user when the user is investigating incidents. It is up to the user |

| SFR | SF and Rationale |
|---|---|
| | to carry out the mitigation command recommended by the TOE. |
| IDS_RDR.1 | Is implemented by the Reporting Security Function. The Reporting security function only allows those explicitly authorized and authenticated users operating in the Admin, Security Analyst, and Operator roles to review the incidents, auditing data, and reports generated by the TOE. The TOE presents this data to users through the web interface to the TOE which allows human users to understand the data the TOE is presenting them. |
| IDS_SDC.1 | Is implemented by the Analysis Security Function and the External Device Communication Security Function. The TOE must be able to collect or receive raw data from sensors it is configured to collect or receive from. This raw data consists of device logs and/ or alerts, and/or events and/ or NetFlow communications. At a minimum, the information must include originating host, time and date collected, sensor type and event type. |
| IDS_STG.1 | Is implemented by the Analysis Security Function. The TOE requires users to successfully identify and authenticate themselves to the TOE before they are allowed to carry out any other actions with the TOE. All users that have permission to log into the TOE (those users operating in the Admin, Security Analyst and Operator roles) are allowed to view the audit records only the Admin role users are allowed to purge (back up) the analysis data from the TOE. The purge event is audited when a user operating in the Admin role carries this activity out. The generation of the audit record is a detection capability that can be used to determine if an unauthorized modification to the stored analyzer data have occurred with the stored analysis data. The TOE will ensure that all analyzer data stored on the hard drives of the TOE are maintained when the physical hard drive resources are exhausted or attacked. |

## 8.4 TOE Security Functional Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified TOE and IT Security Functional Requirements include the appropriate hierarchical SFRs and dependent SFRs. Table 21 lists the TOE Security Functional Components and the Security Functional Components each are hierarchical to and dependent upon and any necessary rationale.

N/A in the Rationale column means the Security Functional Requirement has no dependencies and therefore, no dependency rationale is required. Satisfied in the Rationale column means the Security Functional Requirements dependency was included in the ST.

**Table 21: TOE Security Functional Requirements Dependency Rationale**

| Security Functional Requirement (TOE) | Hierarchical To | Dependency | Rationale |
|---|---|---|---|
| FAU_GEN.1 | No other components | FPT_STM.1 | Satisfied |
| FAU_SAR.1 | No other components | FAU_GEN.1 | Satisfied |
| FAU_SAR.2 | No other components | FAU_SAR.1 | Satisfied |
| FAU_STG.2 | FAU_STG.1 | FAU_GEN.1 | Satisfied |
| FAU_STG.4 | FAU_STG.3 | FAU_STG.1 | Satisfied by FAU_STG.2 because of hierarchy |
| FCS_CKM.1(1) | No other components | FCS_CKM.2,<br>FCS_CKM.4,<br>FCS_COP.1,<br>FMT_MSA.2 | Satisfied<br>FMT_MSA.2 is not applicable for this TOE because the TOE does not provide an interface for the administrator to enter secure values relating to the cryptographic aspects of SSH. |
| FCS_CKM.1(2) | No other components | FCS_CKM.2,<br>FCS_CKM.4,<br>FCS_COP.1,<br>FMT_MSA.2 | Satisfied<br>FMT_MSA.2 is not applicable for this TOE because the TOE does not provide an interface for the administrator to enter secure values relating to the cryptographic aspects of SSL. |
| FCS_CKM.2 | No other components | FDP_ITC.1,or<br>FDP_ITC.2 or<br>FCS_CKM.1,<br>FCS_CKM.4,<br>FMT_MSA.2 | Satisfied<br>FMT_MSA.2 is not applicable for this TOE because the TOE does not provide an interface for the administrator to enter secure values relating to the cryptographic aspects of SSH. |
| FCS_CKM.4 | No other components | FDP_ITC.1,or<br>FDP_ITC.2 or<br>FCS_CKM.1,<br>FMT_MSA.2 | Satisfied<br>FMT_MSA.2 is not applicable for this TOE because the TOE does not provide an interface for the administrator to enter secure values relating to the cryptographic aspects of SSH. |
| FCS_COP.1(1) | No other components | FMT_MSA.2,<br>FDP_ITC.1,or<br>FDP_ITC.2 or<br>FCS_CKM.1(1),<br>FCS_CKM.4 | Satisfied<br>FMT_MSA.2 is not applicable for this TOE because the TOE does not provide an interface for the administrator to enter secure values relating to the cryptographic aspects of SSH. |

| Security Functional Requirement (TOE) | Hierarchical To | Dependency | Rationale |
|---|---|---|---|
| FCS_COP.1(2) | No other components | FMT_MSA.2,<br>FDP_ITC.1,or<br>FDP_ITC.2 or<br>FCS_CKM.1(1),<br>FCS_CKM.4 | Satisfied<br>FMT_MSA.2 is not applicable for this TOE because the TOE does not provide an interface for the administrator to enter secure values relating to the cryptographic aspects of SSH. |
| FCS_COP.1(3) | No other components | FMT_MSA.2,<br>FDP_ITC.1,or<br>FDP_ITC.2 or<br>FCS_CKM.1(2),<br>FCS_CKM.4 | Satisfied<br>FMT_MSA.2 is not applicable for this TOE because the TOE does not provide an interface for the administrator to enter secure values relating to the cryptographic aspects of SSL. |
| FIA_UAU.2 | No other components | FIA_UID.2 | Satisfied |
| FIA_ATD.1 | No other components | No dependencies | N/A |
| FIA_UID.2 | No other components | No dependencies | N/A |
| FMT_MOF.1 | No other components | FMT_SMR.1<br>FMT_SMF.1 | Satisfied |
| FMT_MTD.1(1) | No other components | FMT_SRM.1<br>FMT_SMF.1 | Satisfied |
| FMT_MTD.1(2) | No other components | FMT_SRM.1<br>FMT_SMF.1 | Satisfied |
| FMT_MTD.1(3) | No other components | FMT_SRM.1<br>FMT_SMF.1 | Satisfied |
| FMT_SMR.1 | No other components | FIA_UID.2 | Satisfied |
| FPT_ITC.1 | No other components | No dependencies | N/A |
| FPT_ITI.1 | No other components | No dependencies | N/A |
| FPT_RVM.1 | No other components | No dependencies | N/A |
| FPT_SEP.1 | No other components | No dependencies | N/A |
| FPT_STM.1 | No other components | No dependencies | N/A |
| IDS_ANL.1 | No other components | No dependencies | N/A |
| IDS_RCT.1 | No other components | No dependencies | N/A |
| IDS_RDR.1 | No other components | No dependencies | N/A |

| Security Functional Requirement (TOE) | Hierarchical To | Dependency | Rationale |
|---|---|---|---|
| IDS_SDC.1 | No other components | No dependencies | N/A |
| IDS_STG.1 | No other components | No dependencies | N/A |

## 8.5 Rationale for Explicitly Stated SFR for the TOE

A family of IDS requirements was included in this ST drawn from the Intrusion Detection System Analyzer Protection Profile, Version 1.2, dated April 27, 2005. The PP stated rational for the explicitly stated requirements is:

> "A family of IDS requirements was created to specifically address the data collected and analysed by an IDS. The audit family of the CC (FAU) was used as a model for creating these requirements. The purpose of this family of requirements is to address the unique nature of IDS data and provide for requirements about collecting, reviewing and managing the data. These requirements have no dependencies since the stated requirements embody all the necessary security functions."

This ST uses this rational for including the IDS explicitly stated SFR for the TOE.

## 8.6 Rationale for Strength of Function Claim

Part 1 of the CC defines "strength of function" in terms of the minimum efforts assumed necessary to defeat the expected security behavior of a TOE security function. There are three strength of function levels defined in Part 1: SOF-basic, SOF-medium and SOF-high. SOF-basic is the strength of function level chosen for this ST.

SOF-basic states, "a level of the TOE strength of function where analysis shows that the function provides adequate protection casual breach of TOE by attackers possessing a low attack potential." The rationale for choosing SOF-basic was to be consistent with the assurance requirements included in this ST. Specifically, AVA_VLA. 1 requires that the TOE be resistant obvious vulnerabilities, this is consistent with SOF-basic, which is the lowest strength of function metric.

Consequently, security functions with probabilistic or permutational mechanisms chosen for inclusion in this ST were determined to adequately protect information in a Basic Robustness Environment with the low attack potential threat identified in Section 3 of this ST.

The TOE minimum strength of function is SOF-basic. The evaluated TOE is intended to operate in commercial and DoD low robustness environments processing unclassified information. This security function is in turn consistent with the security objectives described in section 4.

The SOF claim applies to the requirement FIA_UAU.2 and the password authentication that is described in the Identification and Authentication security function above in section 6.1.1.

## 8.7 Assurance Measures Rationale for TOE Assurance Requirements

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the TOE will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

Table 22 provides an EAL2 dependency analysis.

**Table 22: EAL2 SAR Dependencies**

| Assurance Component ID | Assurance Component Name | Dependencies | Satisfied |
|---|---|---|---|
| ACM_CAP.2 | Configuration items | None | N/A |
| ADO_DEL.1 | Delivery procedures | None | N/A |
| ADO_IGS.1 | Installation, generation, and start-up procedures | AGD_ADM.1 | Yes |
| ADV_FSP.1 | Informal functional specification | ADV_RCR.1 | Yes |
| ADV_HLD.1 | Descriptive high-level design | ADV_FSP.1,<br>ADV_RCR.1 | Yes |
| ADV_RCR.1 | Informal correspondence demonstration | None | N/A |
| AGD_ADM.1 | Administrator guidance | ADV_FSP.1 | Yes |
| AGD_USR.1 | User guidance | ADV_FSP.1 | Yes |
| ATE_COV.1 | Evidence of coverage | ADV_FSP.1,<br>ATE_FUN.1 | Yes |
| ATE_FUN.1 | Functional testing | None | Yes |
| ATE_IND.2 | Independent testing-sample | ADV_FSP.1,<br>AGD_ADM.1,<br>AGD_USR.1,<br>ATE_FUN.1 | Yes |
| AVA_SOF.1 | Strength of TOE security function evaluation | ADV_FSP.1,<br>ADV_HLD.1 | Yes |

| Assurance Component ID | Assurance Component Name | Dependencies | Satisfied |
|---|---|---|---|
| AVA_VLA.1 | Developer vulnerability analysis | ADV_FSP.1,<br>ATE_HLD.1<br>AGD_ADM.1,<br>AGD_USR.1 | Yes |