Cisco Systems, Inc.

Cisco Intrusion Detection System Module (IDSM2) V4.1 (3) Security Target

Version: 1.0

Status: Final

Release Date: June 16, 2004

Cisco Systems, Inc.

Table of Contents

List of Figures

List of Tables

1 SECURITY TARGET INTRODUCTION

The Security Target (ST) introduction section presents introductory information on the Security Target, the Target of Evaluation (TOE) referenced in this Security Target, and a basic introduction to the TOE.

Intrusion detection is a security technology that attempts to identify and isolate "intrusions"; a system attempting to detect attacks against web servers might consider only malicious HTTP requests, while a system intended to monitor dynamic routing protocols might only consider RIP spoofing. Regardless, all intrusion detection systems share a general definition of "intrusion" as an unauthorized usage of or misuse of a computer system.

Intrusion detection is an important component of a security system, and it complements other security technologies. By providing information to site administration, intrusion detection allows not only for the detection of attacks explicitly addressed by other security components (such as firewalls and service wrappers), but also attempts to provide notification of attacks unforeseen by other components.

Intrusion detection systems also provide forensic information that potentially allows organizations to discover the origins of an attack. In this manner, intrusion detection systems attempt to make attackers more accountable for their actions, and, to some extent, act as a deterrent to future attacks.

1.1 ST and TOE Identification

This section provides information necessary to identify and control the Security Target and the TOE.

ST Title:	Cisco Intrusion Detection System Module (IDSM2) v4.1 (3) Security Target
ST Version	1.0 Final
ST Publication Date	June 16, 2004
ST Author	Corsec Security, Inc.
TOE Identification:	Cisco Intrusion Detection System Module (IDSM2) v4.1 (3)
Common Criteria (CC) Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999 (aligned with ISO/IEC 15408:1999) with the following CCIMB Interpretations applied (as of the evaluation

	kick-off on October 3, 2002): 003, 051 and 065.
Assurance Level:	Evaluation Assurance Level 2 augmented with ALC_FLR.1
Keywords:	Intrusion Detection System (IDS), vulnerability assessor, network based IDS, signature analysis

1.2 Security Target Overview

The Cisco Intrusion Detection System Module (IDSM2) v4.1(3) Security Target contains the following sections:

Security Target Introduction: Provides introductory information on the Security Target, the Target of Evaluation referenced in this Security Target, and a basic introduction to the TOE.

TOE Description: Provides an overview of the TOE security functions and describes the physical and logical boundaries of the TOE.

TOE Security Environment: Describes the threats, organizational security policies, and assumptions that pertain to the TOE and the TOE environment.

Security Objectives: Identifies the security objectives that are satisfied by the TOE and the TOE environment.

IT Security Requirements: Presents the Security Functional Requirements (SFRs) met by the TOE and the IT environment.

Assurance Requirements: Presents the Security Assurance Requirements (SARs) met by the TOE.

TOE Summary Specification: Describes the security functions provided by the TOE to satisfy the security requirements and objectives.

PP Claims: Presents a full comparison of the functional and assurance requirements claimed against that required by the Intrusion Detection System System Protection Profile (Full compliance with this PP is not being claimed).

Rationale: Presents the rationale for the security objectives, requirements, and the TOE summary specifications as to their consistency, completeness, and suitability.

References: Presents a list of acronyms used in this ST.

1.2.1 Common Criteria Conformance Claims

This ST claims conformance to CC Version 2.1 Part 2 extended with the following CCIMB Interpretations applied (as of the evaluation kick-off on October 03, 2002): 003, 051 and 065.

This ST claims conformance to CC Version 2.1 Part 3 conformant for EAL2 augmented with ALC_FLR.1 with the following CCIMB Interpretations applied (as of the evaluation kick-off on October 03, 2002): 003, 051 and 065.

1.2.2 Conventions

There are several font variations within this ST. The description below provides an explanation of the font conventions used to show operations, as defined in the Common Criteria, performed on the requirements. Acronyms used within this ST are defined in Section 10. These conventions are used throughout this ST to accurately reflect Assignments, Refinements, Selections and/or Iterations made to the requirements from the Common Criteria.

- Assignment: Allows the specification of an identified parameter. Indicated with [**bold text in brackets**].
- Refinement: Allows the addition of details. Indicated with [***bold text and italics in brackets***].
- Selection: Allows the specification of one or more elements from a list. Indicated with [underlined text in brackets].
- Iteration: Allows for a component to be clearly specified for each method of implementation. Iterations are identified by appending a number in parenthesis following the component title.

1.3 High-level Description of the TOE

The Cisco Intrusion Detection System Module (IDSM2) v4.1(3) is a network based Intrusion Detection System which passively monitors packets on a given target Information Technology (IT) network or system; looking for malicious activity. The primary means by which it detects malicious activity is by using signature analysis on captured packets to determine the type of attack. If a packet or series of packets triggers an alarm based on signature analysis, information related to this possible intrusion is collected in an event store, which can be viewed in real-time or

historically. This information allows the user of the IDS to detect real-time attacks, as well as perform forensic investigation on past attacks.

2 TOE DESCRIPTION

Intrusion detection is a security technology that attempts to identify and isolate "intrusions"; a system attempting to detect attacks against web servers might consider only malicious HTTP requests, while a system intended to monitor dynamic routing protocols might only consider RIP spoofing. Regardless, all intrusion detection systems share a general definition of "intrusion" as an unauthorized usage of or misuse of a computer system.

Intrusion detection is an important component of a security system, and it complements other security technologies. By providing information to site administration, intrusion detection allows not only for the detection of attacks explicitly addressed by other security components (such as firewalls and service wrappers), but also attempts to provide notification of attacks unforeseen by other components.

Intrusion detection systems also provide forensic information that potentially allows organizations to discover the origins of an attack. In this manner, intrusion detection systems attempt to make attackers more accountable for their actions, and, to some extent, act as a deterrent to future attacks.

This section provides a general overview of the TOE, in order to provide an understanding of how this TOE functions and to aid customers in determining whether this product meets their needs.

2.1 Cisco Intrusion Detection System

The TOE is the Cisco Intrusion Detection System Module (IDSM2) v4.1(3) and can be categorized as a real-time network-based Intrusion Detection System. The TOE can analyze both the header and content of each packet as well as analyze single packets or a complete flow of attacks while maintaining flow state (allowing for the detection of multi-packet attacks). The TOE uses a rule-based expert system to interrogate the packet information to determine the type of attack, be it simple or complex.

The TOE software is a product that provides data collection and analysis functions while being installed in a Cisco Catalyst 6500 series switch hardware device. These devices are to be placed at strategic points throughout a target IT system[1] and interrogate passing network traffic. In response to an attack, the TOE has several options that include generating an alarm, logging the alarm event, configuring an Access Control List to block the attacker and killing TCP sessions.

[1] Here and throughout this document, we use the terms IT system and IT network synonymously when we refer to what the IDS is monitoring.

The TOE can be managed remotely in two ways. The first is via web pages over a TLS connection. The second is through the Command Line Interface (CLI) over an SSH connection. Note that local command and control is performed via the CLI. It is to be noted that the Event Viewer and the IDS Management Center for IDS Sensors (IDS MC) are not included in the TOE.

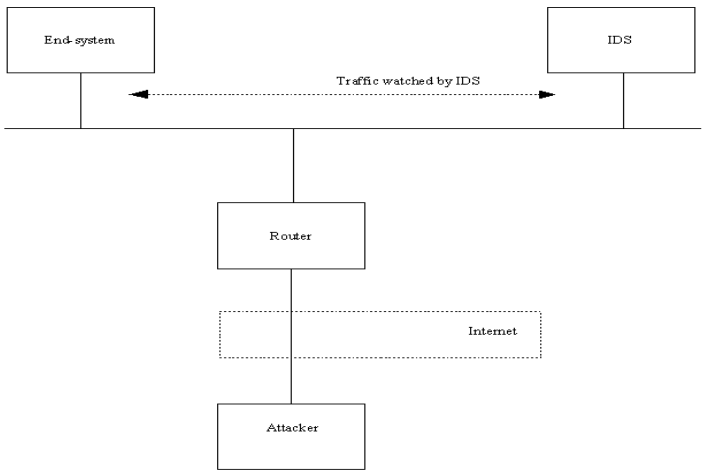

Figure 1: Example Network Topology Using an IDSM2

2.2 Physical Scope and Boundaries

The following is a description of the physical scope and boundaries of the Cisco Systems, Inc. IDSM2 Blade running the Intrusion Detection System v4.1(3) software. It is important that these are taken into account when examining the external interfaces in the TOE Security Functions. Note that throughout the TOE documentation references are made to the Device Manager. The Device Manager is not a program; rather it is the totality of HTML and JavaScript scripts provided to the user's browser by the Secure Web Server Subsystem.

The physical scope and boundaries of the Cisco Systems, Inc. IDSM2 Blade running the Intrusion Detection System v4.1(3) software include the Intrusion Detection System v4.1(3) application code, the resident Linux 7.3 operating system which the Intrusion Detection System application runs upon, and the IDSM2 Blade hardware that resides within a Cisco Catalyst 6500 series switch. The switch itself is not included within the TOE boundary. The Linux operating system cannot be installed separately from the Intrusion Detection System v4.1(3) application code, and is shipped and installed as one disk image.

The Cisco Systems, Inc. IDSM2 Blade running the Intrusion Detection System v4.1(3) software has the following hardware configuration.

IDSM2 Blade Switching Module

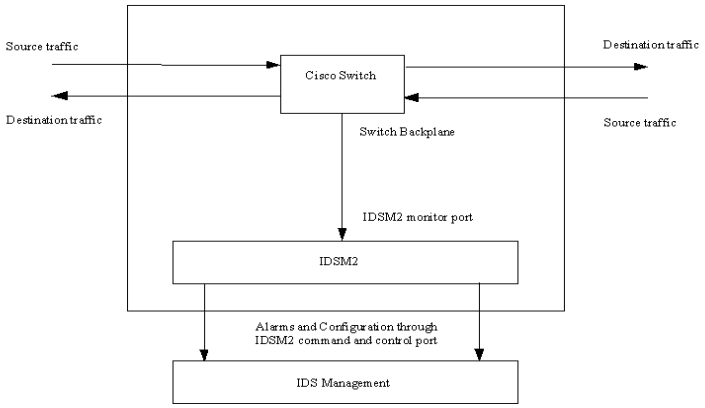

Figure 3: Physical Scope and Boundaries for the IDSM2 Blade

The TOE hardware includes an Intel x86 based IDSM2 Blade module which is installed within a Cisco Catalyst 6500 series switch.

Specific part numbers for the IDSM2 Switching Module (also referred to as a Blade) include: WS-SVC-IDS2-BUN-K9 and WS-SVC-IDS2BUNK9=. These two part numbers are for identical modules and the part numbers differ in the fact that the former is used when ordering the IDSM2 with the switch chassis as a system and the latter can be used to order an IDSM2 separately from the switch chassis.

The following are the Cisco Systems, Inc. IDSM2 Blade running the Intrusion Detection System v4.1(3) software and hardware requirements:

Catalyst Supervisor Software Requirements:

- Catalyst OS 7.6(1) (minimum)
- Cisco IOS Software Release 12.1(19)E or 12.2.(14)SY (minimum)

Catalyst Supervisor Hardware Options with IDSM-2:

Supervisor	Native IOS Branch	Cat OS Branch
Sup720 with MSFC3	12.2(14)SX1	Not yet available
Sup720 without MSFC3	N/A	N/A
Sup2 with MSFC2	12.1(13)E, 12.1(19)E, 12.2(14)SY	7.5(1), 7.6(1), 8.1(1)
Sup2 without MSFC2	N/A	7.5(1), 7.6(1), 8.1(1)
Sup2 without PFC2	N/A	N/A
Sup1a with MSFC2	12.1(19)E1	7.5(1), 7.6(1), 8.1(1); valid MSFC2 branches 12.1(13)E, 12.1(19)E
Sup1a without MSFC2	N/A	7.5(1), 7.6(1), 8.1(1)
Sup1a without PFC	N/A	N/A
Sup1a with MSFC1	No Support	7.5(1), 7.6(1), 8.1(1); valid MSFC1 branches 12.1(13)E, 12.1(19)E
Sup1a without MSFC1	N/A	7.5(1), 7.6(1), 8.1(1)

As indicated above, the Catalyst 6500 series switch chassis is not considered part of the TOE, although it does provide some functionality such as management of

security functions behavior for timestamps and the generation of timestamps as described in the security functional requirements appearing in Section 5.

Upon initial installation of the IDSM2 module in the switch, the supervisor module must be used to forward network traffic to the appropriate interfaces on the IDSM2 module. This network traffic must be either copied to the IDSM2 module based on security VLAN Access Control Lists (VACLs) in the switch or through the switch's Switching Port Analyzer (SPAN) port feature. These actions must be performed correctly in order for the TOE to function properly. Once these actions are performed, users can communicate with the TOE via a routable IP address.

Users can only physically connect to the IDSM2 module console through the supervisor module on the switch. Users must also enter a {username, password} in order to authenticate to the IDSM2 module. The IDSM2 {username, password} is separate from the supervisor enable password.

The IDSM2 module does not contain a hardware clock, and therefore must receive time from the switch. It is important to note that the IDSM2 module receives time generated from the switch upon boot-up or changed by the switch administrator, and then maintains the time locally.

Operating System

The TOE software includes a hardened version of Red Hat Linux 7.3 as its embedded Operating System (OS). This is to be included as part of the TOE. All Subsystems are built atop this OS. It should be noted that the Cisco Systems, Inc. IDSM2 Blade running the Intrusion Detection System v4.1(3) software receives time generation from the switch upon which the it is installed and then relies on the operating system's clock for the keeping of reliable time.

2.3 Logical Scope and Boundaries

The security functions implemented by the TOE software are grouped under the following components:

Sensor Application
The Sensor Application is used to monitor network packets from the target IT network. Received data is parsed for analysis and compared against signatures of known attacks. The version and revision level of the signatures used to identify known attacks is the same across all platforms.

Network Access Controller
The Network Access Controller provides analyzer react functionality. The TOE can be configured such that when an intrusion is detected, the Network

Access Controller can send a command to a Cisco router, Cisco switch, or PIX firewall to block traffic from the alleged source address of the intrusion.

Secure Web Server
The Secure Web Server provides a TLS encrypted interface between the client web browsers and the system. Requests arrive as HTML encapsulated by the TLS connection. These requests are parsed and formatted as control transactions to be passed to the appropriate component within the system. Responses are converted into HTML and returned to the web browser. After a user has been authenticated, the Secure Web Server is responsible for enforcing that the user is only able to issue requests at his/her privilege level (i.e., group).

Authentication Application
The Authentication Application is responsible for associating usernames with groups. It receives requests and processes responses in the form of Control Transactions. It is dynamically linked with the Pluggable Authentication Module (PAM) library which is part of the Linux OS, and depending on the path taken by the user to authenticate to the system, will interface with PAM which will authenticate the user.

Secure Shell
Secure Shell (SSH) provides confidentiality and integrity over an unsecured network. The sshd (daemon process for SSH) listens for connections from clients. SSH generally works as follows. The host generates an RSA public/private key pair. Whenever a client connects to the host, the host sends its public key to the client. The client generates a random number (nonce) which it encrypts with the hosts public key and sends this to the host. Both sides then use this random number as a session key to encrypt all data across the network. Users can authenticate with a {username, password} or via RSA authentication through sshd.

Command Line Interface
The Command Line Interface allows an authorized user to issue commands on the system and receive data from the system. This data is sent over an SSH encrypted session (except in the case of console connection, in which it is sent in clear text). The CLI presents the user with a restricted command set. User commands are parsed and formatted as control transactions to be passed to the appropriate component within the system. After a user has been authenticated the CLI is responsible for enforcing that the user is only able to issue commands at his/her privilege level (i.e., group).

Event Store
The Event Store, comprised of the event store file and the shared object libidapi.001.006.so, stores audit and system events. Libidapi, also called IDAPI, ensures that all events written to the event store conform to the

IDIOM specification. Libidapi is dynamically linked to all components required to write to and read from the event store file.

Operating System
The OS is responsible for maintaining reliable time stamps received from the switch and is also responsible for portions of the authentication process. The OS aids in authentication in two ways. When a user authenticates with a username and password this information is passed to PAM for authentication. Authentication data is stored in the etc/shadow file. In addition, PAM is responsible for authentication failure handling and account lockout. When a user authenticates with an RSA key (only available when authenticated via sshd), PAM is only called for authentication failure handling and account lockout. In addition when a user authenticates via the console, the login program is called which authenticates the user using PAM in the same manner as sshd.

Update Client
The update client uses an outbound connection only. It is used to retrieve attack signatures and software patches from Cisco. An administrator must manually configure the TOE to connect to a specified Cisco server to receive updates. It should be noted that in the evaluated configuration, only protocols which can ensure confidentiality and integrity of data can be used (i.e., HTTPS, and SCP).

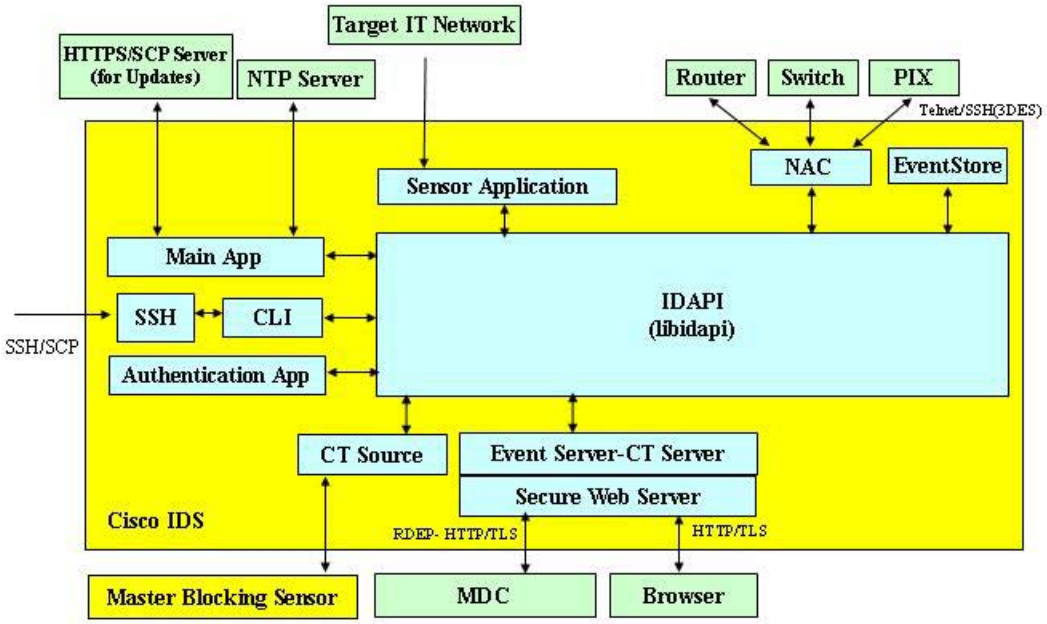

Figure 4: Logical Components of the TOE

3 TOE SECURITY ENVIRONMENT

This section identifies the following components for the TOE:

1) Significant assumptions about the TOEs operational environment

2) IT-related threats countered by TOE components

3) Organizational security policies for which this TOE is appropriate

This information provides the basis for the Security Objectives, the Security Requirements for the IT Environment, and the TOE Security Functional Requirements. The TOE Security Environment described below was derived from the Intrusion Detection System System Protection Profile Version 1.4, February 4, 2002. The additions to the Protection Profile requirements include T.TIME, as this threat is addressed by the IT environment.

3.1 Assumptions

This section contains assumptions regarding the security environment and the intended usage of the TOE.

3.1.1 Intended Usage Assumptions

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

3.1.2 Physical Assumptions

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 prevent unauthorized physical access.

3.1.3 Personnel Assumptions

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 accessed by authorized users.

3.2 Threats

The following are threats identified for, and addressed by, the TOE, the IT System the TOE monitors, and the environment in which the TOE resides. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

3.2.1 TOE Threats

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

T.NOHALT An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE through the TOE interfaces.

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 An unauthorized user may inappropriately change the configuration of the TOE 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.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.

3.2.2 IT System Threats

The following identifies threats to the IT System that may be indicative of vulnerabilities in or misuse of IT resources.

T.SCNCFG Improper security configuration settings may exist in the IT System the TOE monitors.

T.SCNMLC Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions.

T.SCNVUL Vulnerabilities may exist in the IT System the TOE monitors.

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 IDS data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources.

T.MISUSE Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors.

T.INADVE Inadvertent activity and access may occur on an IT System the TOE monitors.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

3.2.3 IT Environment Threats

T.TIME Unauthorized users could attempt to modify the time on the switch, thereby passing inaccurate timestamps to the TOE, which would reflect in inaccurate reporting of events in the generated audit records.

T.ENOHALT An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE through use of the TOE Environment.

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. This section identifies the organizational security policies that were derived from the Intrusion Detection System System Protection Profile.

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

P.MANAGE The TOE shall only be managed by authorized users.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

P.PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions through its own interfaces.

4 SECURITY OBJECTIVES

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs. The security objectives described below, with the exception of O.TIME, were derived from the Intrusion Detection System System Protection Profile Version 1.4, February 4, 2002.

4.1 Information Technology Security Objectives

The following are the TOE security objectives:

O.PTPROTCT The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.

O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.

O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.

O.IDANLZ The Analyzer must accept data from IDS Sensors or IDS Scanners 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 users prior to allowing access to TOE functions and data.

O.OFLOWS The TOE must appropriately handle potential audit and System data storage overflows.

O.AUDITS The TOE must record audit records for data accesses and use of the System functions.

O.INTEGR The TOE must ensure the integrity of all audit and System data.

O.EXPORT When any IDS component makes its data available to another IDS component, the TOE will ensure the confidentiality of the System data.

4.2 Security Objectives for the Environment

The TOE's operating environment must satisfy the following objectives.

O.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.

O.PHYCAL Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

O.CREDEN Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner that is consistent with IT security.

O.PERSON Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.

O.EIDAUTH The TOE environment must be able to identify and authenticate users prior to allowing the ability to halt or reconfigure the TOE.

O.EPROTCT The TOE environment will maintain a domain for its own execution that protects itself and the TOE from external interference, tampering, or unauthorized disclosure.

O.INTROP The TOE is interoperable with the IT System it monitors.

O.TIME Those responsible for the TOE must ensure that it is installed in a configured switch, which will be the source of time generation for use by the TOE.

5 IT SECURITY REQUIREMENTS

This section specifies the Security Functional Requirements for the TOE and the IT environment. The SFRs are organized into CC classes drawn from Part 2 of the CC extended. The Common Criteria standard defines four basic operations that can be performed on the requirements to further clarify and define them: Assignment, Selection, Iteration, and Refinement. This ST will highlight instantiations of the four operations used in the following manner:

- Assignment: Allows the specification of an identified parameter. Indicated with [**bold text in brackets**].
- Refinement: Allows the addition of details. Indicated with [***bold text and italics in brackets***].
- Selection: Allows the specification of one or more elements from a list. Indicated with [underlined text in brackets].
- Iteration: Allows for a component to be clearly specified for each method of implementation. Iterations are identified by appending a number in parenthesis following the component title.

Extensions to the Part 2 requirements are identified by appending (EXP) after the component identification.

5.1 TOE Security Functional Requirements

An overview of the TOE Security Functional Requirements is presented in Table 1.

ID	Functional Component	ST Operations
FAU_GEN.1	Audit data generation	Selection, assignment, assignment
FAU_SAR.1	Audit review	Assignment, assignment
FAU_SAR.2	Restricted audit review	None
FAU_SAR.3	Selectable audit review	Selection, assignment
FAU_SEL.1	Selective audit	Selection, assignment
FAU_STG.2	Guarantees of audit availability	Selection, assignment, selection
FAU_STG.4	Prevention of audit data loss	Selection, assignment
FIA_UAU.1	Timing of authentication	Assignment
FIA_AFL.1	Authentication failure handling	Assignment, assignment, assignment
FIA_ATD.1	User attribute definition	Assignment
FIA_UID.1	Timing of identification	Assignment

FMT_MOF.1(1)	Management of security functions behavior	Selection, assignment, assignment
FMT_MTD.1	Management of TSF data	Selection, assignment, assignment, assignment
FMT_SMR.1	Security roles	Assignment
FMT_SMF.1 (Interpretation 065)	Specification of Management Functions	Assignment
FPT_ITA.1	Inter-TSF availability within a defined availability metric	Assignment, assignment, assignment
FPT_ITC.1	Inter-TSF confidentiality during transmission	None
FPT_ITI.1	Inter-TSF detection of modification	Assignment, assignment
FPT_RVM .1	Non-bypassability of the TSP	None
FPT_SEP_EXP.1 (EXP)	TSF domain separation	Explicitly Stated
IDS_SDC.1 (EXP)	System data collection	Explicitly Stated
IDS_ANL.1 (EXP)	Analyser analysis	Explicitly Stated
IDS_RCT.1 (EXP)	Analyser react	Explicitly Stated
IDS_RDR.1 (EXP)	Restricted data review	Explicitly Stated
IDS_STG.1 (EXP)	Guarantee of system data availability	Explicitly Stated
IDS_STG.2 (EXP)	Prevention of system data loss	Explicitly Stated

Table 1: TOE Security Functional Requirements

The following sections present the TOE SFRs with any ST operations performed on them.

5.1.1 Security Audit (FAU)

5.1.1.1 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 [basic] level of audit; and

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

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to System	
FAU_GEN.1	Access to the TOE and System data	**Object IDS, Requested access**
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FIA_UAU.1	All use of the authentication mechanism	**User identity, location**
FIA_UID.1	All use of the user identification mechanism	**User identity, location**
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MDT.1	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**
FPT_ITI.1	The action taken upon detection of modification of transmitted TSF data	

Table 2: Auditable Events

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 2 Auditable Events**].

5.1.1.2 FAU_SAR.1: Audit review

FAU_SAR.1.1 The TSF shall provide [**Authorized Administrators, Operators, and Viewers**] with the capability to read [**all audit trail data**] 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.

5.1.1.3 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.

5.1.1.4 FAU_SAR.3: Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to perform [sorting] of audit data based on [date and time, subject identity, type of event, and success or failure of related event].

5.1.1.5 FAU_SEL.1: Selective audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a) [Event type];

b) [**No additional attributes**].

5.1.1.6 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] modification to the audit records.

FAU_STG.2.3 The TSF shall ensure that [**the total number of audit events in the event store minus the total number of audit events inserted in the event store**

subsequent to audit storage exhaustion] audit records will be maintained when the following conditions occur: [audit storage exhaustion].

5.1.1.7 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.

5.1.2 Identification and Authentication (FIA)

5.1.2.1 FIA_UAU.1: Timing of authentication

FIA_UAU.1.1 The TSF shall allow [**a) For the Web Interface: The TLS handshake to be performed, and input of authentication data b) For the CLI Interface: The SSH handshake to be performed, input of authentication data or in the case of the physical console interface, input of authentication data**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.1.2.2 FIA_AFL.1: Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [**a settable, non-zero number**] of unsuccessful authentication attempts occur related to [**external IT products attempting to authenticate**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**prevent the offending external IT product from successfully authenticating until an authorized administrator takes some action to make authentication possible for the external IT product in question**].

5.1.2.3 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; and**

c) [**Authorizations**].

5.1.2.4 FIA_UID.1: Timing of identification

FIA_UID.1.1 The TSF shall allow [**a) For the Web Interface: The TLS handshake to be performed, and input of authentication data b) For the CLI Interface: The SSH handshake to be performed, input of authentication data or in the case of the physical console interface, input of authentication data**] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.1.3 Security Management (FMT)

5.1.3.1 FMT_MOF.1(1): Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to [modify the behavior] of the functions [**of System data collection, analysis and reaction**] to [authorized System administrators].

5.1.3.2 FMT_MTD.1: Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [query [**and add System and audit data, and shall restrict the ability to query and modify all other TOE data**]] to [**Administrators and Operators who can query and modify all other TOE data; and Viewers who can only query all other TOE data**].

5.1.3.3 FMT_SMR.1: Security roles

FMT_SMR.1.1 The TSF shall maintain the roles: [**Administrator, Operator, and Viewer**].

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

5.1.3.4 FMT_SMF.1 (Interpretation 065): Specification of Management Functions

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

5.1.4 Protection of the TOE Security Functions (FPT)

5.1.4.1 FPT_ITA.1: Inter-TSF availability within a defined availability metric

FPT_ITA.1.1 The TSF shall ensure the availability of [**audit and System data**] provided to a remote trusted IT product within [**60 seconds**] given the following conditions [**(a) normal traffic on the communications network; (b) both IT products operational and available**].

5.1.4.2 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.

5.1.4.3 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: [**Message Authentication Code (MAC) in TLS and SSH**].

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 [**terminate the session**] if modifications are detected.

5.1.4.4 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.

5.1.4.5 TOE_SEP_EXP.1 (EXP): TSF domain separation

TOE_SEP_EXP.1.1 The TSF shall maintain a security domain that protects it from interference and tampering by untrusted subjects initiating actions through its own TSFI.

TOE_SEP_EXP.1.2 The TSF shall enforce separation between the security domains of subjects in the TOE Scope of Control.

5.1.5 IDS Component Requirements (IDS)

5.1.5.1 IDS_SDC.1: System data collection (EXP)

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resources:

a) [Network Traffic]

b) [**No additional events**]. (EXP)

IDS_SDC.1.2 At a minimum, the System shall collect and record 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) [**The additional information specified in the Details column of Table 3 System Events**]. (EXP)

Component	Event	Details
IDS_SDC.1	Start-up and shutdown	**none**
IDS_SDC.1	Identification and authentication events	**User identity, location, source address,**

Component	Event	Details
		destination address
IDS_SDC.1	Data accesses	**Object IDS, requested access, source address, destination address**
IDS_SDC.1	Service requests	**Specific service, source address, destination address**
IDS_SDC.1	Network traffic	**Protocol, source address, destination address**
IDS_SDC.1	Security configuration changes	**Source address, destination address**
IDS_SDC.1	Data introduction	**Object IDS, location of object, source address, destination address**
IDS_SDC.1	Start-up and shutdown of audit functions	**none**
IDS_SDC.1	Detected malicious code	**Location, identification of code**
IDS_SDC.1	Access control configuration	**Location, access settings**
IDS_SDC.1	Service configuration	**Service identification (name or port), interface, protocols**
IDS_SDC.1	Authentication configuration	**Account names for cracked passwords, account policy parameters**
IDS_SDC.1	Accountability policy configuration	**Accountability policy configuration parameters**
IDS_SDC.1	Detected known vulnerabilities	**Identification of the known vulnerability**

Table 3: System Events

5.1.5.2 IDS_ANL.1 Analyser analysis (EXP)

IDS_ANL.1.1 The System shall perform the following analysis function on all IDS data received:

a) [Signature]

b) [**No additional analytical functions**]. (EXP)

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

a) Date and time of the result, type of result, and identification of data source.

b) [**No additional security relevant information about the result**]. (EXP)

5.1.5.3 IDS_RCT.1: Analyser react (EXP)

IDS_RCT.1.1 The System shall send an alarm to [**The Event Store**] and take [**Send an alarm, and/or perform a TCP reset on the connection, and/or send a command to: a Cisco router, Cisco switch, or PIX firewall to block traffic**] when an intrusion is detected. (EXP)

5.1.5.4 IDS_RDR.1: Restricted data review (EXP)

IDS_RDR.1.1 The System shall provide [**Administrators, Operators and Viewers**] with the capability to read [**Event data**] from the System data. (EXP)

IDS_RDR.1.2 The System shall provide the System data in a manner suitable for the user to interpret the information. (EXP)

IDS_RDR.1.3 The System shall prohibit all users read access to the System data, except those users that have been granted explicit read-access. (EXP)

5.1.5.5 IDS_STG.1: Guarantee of system data availability (EXP)

IDS_STG.1.1 The System shall protect the stored System data from unauthorized deletion. (EXP)

IDS_STG.1.2 The System shall protect the stored System data from modification. (EXP)

IDS_STG.1.3 The System shall ensure that [**the total number of system events in the event store minus the total number of system events inserted in the event store subsequent to system storage exhaustion**] System data will be maintained when the following conditions occur: [System data storage exhaustion]. (EXP)

5.1.5.6 IDS_STG.2: Prevention of system data loss (EXP)

IDS_STG.2.1 The System shall [overwrite the oldest stored system data] and send an alarm if the storage capacity has been reached. (EXP)

5.2 Security Functional Requirements for the IT Environment

An overview of the Security Functional Requirements for the IT Environment is presented in Table 4.

ID	Functional Component	ST Operations
FMT_MOF.1(2)	Management of security functions behavior	Refinement/Assignment/Selection/Iteration
FPT_STM.1	Reliable time stamps	Refinement
FPT_SEP_ENV.1 (EXP)	Environment Domain Separation	Explicitly Stated

Table 4: Security Functional Requirements for the IT Environment

The following sections present the SFRs for the IT Environment with any ST operations performed on them.

5.2.1 Security Management (FMT)

5.2.1.1 FMT_MOF.1(2): Management of security functions behavior

FMT_MOF.1.1 The [***IT Environment***] shall restrict the ability to [modify the behavior] of the functions [**of power off and module re-imaging**] to [authorized Environment administrators].

5.2.2 Protection of the TOE Security Functions (FPT)

5.2.2.1 FPT_STM.1: Reliable time stamps

FPT_STM.1.1 The [***IT Environment***] shall be able to provide reliable time stamps for [***use by the TOE***].

5.2.2.2 FPT_SEP_ENV.1: Domain Separation

FPT_SEP_ENV.1 The TSF Environment shall provide hardware that has the ability to identify and authenticate environment administrators who have the ability to halt or reconfigure the TOE.

.

6 ASSURANCE REQUIREMENTS

This section specifies the Security Assurance Requirements (SAR) for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.1.

6.1 Configuration Management (ACM)

6.1.1 Authorization Controls (ACM_CAP.2)

ACM_CAP.2.1D The developer shall provide a reference for the TOE.

ACM_CAP.2.2D The developer shall use a CM system.

ACM_CAP.2.3D The developer shall provide CM documentation.

ACM_CAP.2.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.2.2C The TOE shall be labeled with its reference.

ACM_CAP.2.3C The CM documentation shall include a configuration list.

ACM_CAP.2.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.2.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.2.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2 Delivery and Operation (ADO)

6.2.1 Delivery Procedures (ADO_DEL.1)

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.2 Installation, Generation, and Start-up Procedures (ADO_IGS.1)

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

Interp Note: *The following element has changed as a result of Interpretation 051.*

ADO_IGS.1.1C The installation, generation and start-up documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start up procedures result in a secure configuration.

6.3 Development (ADV)

6.3.1 Informal Functional Specification (ADV_FSP.1)

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

6.3.2 Descriptive High-Level Design (ADV_HLD.1)

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.1.1C The presentation of the high-level design shall be informal.

ADV_HLD.1.2C The high-level design shall be internally consistent.

ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.1.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystem of the TSF are externally visible.

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

6.3.3 Informal Correspondence Demonstration (ADV_RCR.1)

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.4 Guidance Documents (AGD)

6.4.1 Administrator Guidance (AGD_ADM.1)

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.4.2 User Guidance (AGD_USR.1)

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.5 Life Cycle Support (ALC)

6.5.1 Basic Flaw Remediation (ALC_FLR.1)

ALC_FLR.1.1D The developer shall provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.1.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.1.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.1.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.6 Tests (ATE)

6.6.1 Evidence of Coverage (ATE_COV.1)

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.6.2 Functional Testing (ATE_FUN.1)

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.6.3 Independent Testing - Sample (ATE_IND.2)

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

6.7 Vulnerability Assessment (AVA)

6.7.1 Strength of TOE Security Function Evaluation (AVA_SOF.1)

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level of SOF-basic.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric of SOF-basic.

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

6.7.2 Developer Vulnerability Analysis (AVA_VLA.1)

Interp Note: *The following two elements are changed as a result of Interpretation 051.*

AVA_VLA.1.1D The developer shall perform a vulnerability analysis.

AVA_VLA.1.2D The developer shall provide vulnerability analysis documentation.

Interp Note: *The following element is replaced by three as a result of Interpretation 051.*

AVA_VLA.1.1C The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.

The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

7 TOE SUMMARY SPECIFICATIONS

This section provides a high-level definition of the IT Security Functions and the Assurance Measures provided by the TOE to meet the stated claims.

7.1 TOE Security Functions

The TOE provides the following security functions.

7.1.1 Audit

The Audit function monitors network activity and records events that are indicative of an intrusion attempt. In addition, unauthorized access to the audit events is prevented.

7.1.2 Identification & Authentication

The Identification & Authentication function requires users to provide credentials to the TOE in order to successfully be recognized as an authorized user.

7.1.3 Network Traffic Analysis

The Network Traffic Analysis function provides the capability to view or modify the behavior of the TOE. This includes the aspects of management, system data collection and the operations of analysis performed on network traffic.

7.1.4 Roles

The Roles function associates users that have been successfully identified and authenticated to one of three groups (i.e. Administrator, Operator or Viewer).

7.1.5 Self-protection

The Self-protection function provides non-bypassability and partial domain separation for the TSF. This partial separation ensures that the TOE protects itself

in accordance with its requirements and the interfaces that enforce them. The TSF relies on the environment to fully enforce domain separation because the environment administrators have the ability to halt and/or reinstall the IDSM2 in the Catalyst switch. In addition, all transmissions to remote trusted IT products are encrypted.

7.1.6 TOE Security Assurance Measures

The TOE was developed with the following security Assurance measures in place, which constitutes a Common Criteria EAL2 level of assurance augmented with ALC_FLR.1.

- Configuration management
- Delivery and operation
- Development
- Guidance documents
- Tests
- Vulnerability assessment

This section of the ST provides a mapping demonstrating that the Assurance Measures listed meet the Assurance Requirements necessary to achieve EAL2 augmented. In this case the specification of assurance measures is done by referencing the appropriate documentation. Analysis of the referenced documentation to ensure that the documentation listed meets the requirements of the Assurance Requirements for EAL2 augmented.

CC Assurance Requirements	TOE Assurance Measures	Justification
ACM_CAP.2	Cisco Systems, Inc. Cisco Intrusion Detection System Blade v4.1(3) Configuration Management, Version 0.3 Cisco Systems, Inc. Cisco Intrusion Detection System Blade v4.1(3) Configuration Management Plan, Version 0.2	These documents describe the processes and procedures that define how configuration management will be maintained at the development facility.
ADO_DEL.1	Cisco Systems, Inc. Cisco Intrusion Detection System Blade v4.1(3) Secure Delivery, Version 0.3	This document describes how the TOE is securely delivered to customers.
ADO_IGS.1	Release Notes for the Cisco Intrusion Detection System	These documents describe the product

CC Assurance Requirements	TOE Assurance Measures	Justification
	Version 4.1, 4029_03, April 22, 2004. Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1, 78-15597-01 Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.1, 78-15598-01 (excluding Chapter 6, IDS Event Viewer Introduction) Cisco Intrusion Detection System v4.1(3) readme.txt file	setup and basic initial configuration requirements. In addition, additional product release notes are provided to describe the configuration for the specific release of the product.
ADV_FSP.1	Cisco Systems, Inc. Cisco Intrusion Detection System Blade v4.1(3) Functional Specification, Version 0.3	This document describes the security functions and externally visible interfaces.
ADV_HLD.1	Cisco Systems, Inc. Cisco Intrusion Detection System Blade v4.1(3) High-Level Design Document, Version 0.3	This document describes the system interfaces and subsystems.
ADV_RCR.1	Cisco Systems, Inc. Cisco Intrusion Detection System Blade v4.1(3) Correspondence Document, Version 0.3	This document demonstrates the mapping of functionality to meet the requirements through all of the design documentation.
AGD_ADM.1	Release Notes for the Cisco Intrusion Detection System Version 4.1, 4029_03, April 22, 2004. Cisco Intrusion Detection System Command Reference Version 4.1, 78-15599-01 Cisco Intrusion Detection System Appliance and Module	These documents describe the product setup and basic initial configuration requirements. In addition, additional product release notes are provided to describe the configuration for the specific release of the

CC Assurance Requirements	TOE Assurance Measures	Justification
	Installation and Configuration Guide Version 4.1, 78-15597-01 Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.1, 78-15598-01 (excluding Chapter 6, IDS Event Viewer Introduction) Cisco Intrusion Detection System v4.1(3) readme.txt file	product.
AGD_USR.1	Release Notes for the Cisco Intrusion Detection System Version 4.1, 4029_03, April 22, 2004. Cisco Intrusion Detection System Command Reference Version 4.1, 78-15599-01 Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1, 78-15597-01 Installing and Using the Cisco Intrusion Detection System Device Manager and Event Viewer Version 4.1, 78-15598-01 (excluding Chapter 6, IDS Event Viewer Introduction) Cisco Intrusion Detection System v4.1(3) readme.txt file	These documents describe the product setup and basic initial configuration requirements. In addition, additional product release notes are provided to describe the configuration for the specific release of the product.
ALC_FLR.1	Development Security for the Cisco Intrusion Detection System Blade v4.1(3), Version 0.3	This document describes the procedures enforced by the developer to control access to the TOE development environment.

CC Assurance Requirements	TOE Assurance Measures	Justification
	Cisco Systems, Inc. Cisco Intrusion Detection System Blade v4.1(3) Configuration Management, Version 0.2 Cisco Systems, Inc. Cisco Intrusion Detection System Blade v4.1(3) Configuration Management Plan, Version 0.3	These documents describe the processes and procedures that define how configuration management will be maintained at the development facility.
	4.1(1)Sx System Level Detailed Test Plan, Procedures and Results	This document describes Cisco's Test Plans, Procedures and results.
	4.1(2)Sx Test Plan, Procedures and Results	This document is an incremental update to 4.1(1)Sx System Level Detailed Test Plan, Procedures and Results
	4.1(3)Sx Test Plan, Procedures and Results	This document is an incremental update to 4.1(2)Sx System Level Detailed Test Plan, Procedures and Results
ATE_COV.1	Cisco Systems, Inc. Cisco Intrusion Detection System Blade v4.1(3) Testing and Evidence of Coverage, Version 0.2	This document describes the functional test plan and identifies the coverage of functional tests against each security function performed by the developer on the TOE.
	4.1(1)Sx System Level Detailed Test Plan, Procedures and Results	This document describes Cisco's Test Plans, Procedures and results.

CC Assurance Requirements	TOE Assurance Measures	Justification
	4.1(2)Sx Test Plan, Procedures and Results	This document is an incremental update to 4.1(1)Sx System Level Detailed Test Plan, Procedures and Results
	4.1(3)Sx Test Plan, Procedures and Results	This document is an incremental update to 4.1(2)Sx System Level Detailed Test Plan, Procedures and Results
ATE_FUN.1	GEM HANDBOOK Great Engineering Methodology, EDCS - 173105, Rev. A.3 Cisco Systems, Inc. Cisco Intrusion Detection System Blade v4.1(3) Testing and Evidence of Coverage, Version 0.2	This document describes the functional test plan and functional tests performed by the developer of the TOE.
	4.1(1)Sx System Level Detailed Test Plan, Procedures and Results	This document describes Cisco's Test Plans, Procedures and results.
	4.1(2)Sx Test Plan, Procedures and Results	This document is an incremental update to 4.1(1)Sx System Level Detailed Test Plan, Procedures and Results
	4.1(3)Sx Test Plan, Procedures and Results	This document is an incremental update to 4.1(2)Sx System Level Detailed Test Plan, Procedures and Results
ATE_IND.2	GEM HANDBOOK Great Engineering Methodology, EDCS - 173105, Rev. A.3	This document describes the functional test plan

CC Assurance Requirements	TOE Assurance Measures	Justification
	Cisco Systems, Inc. Cisco Intrusion Detection System Blade v4.1(3) Testing and Evidence of Coverage, Version 0.2	and functional tests performed by the developer of the TOE.
AVA_SOF.1	Cisco Systems, Inc. Cisco Intrusion Detection System Blade v4.1(3) Strength of Function Analysis, Version 0.3	This document provides an analysis of the probabilistic or permutational mechanisms in the TOE.
AVA_VLA.1	Cisco Systems, Inc. Cisco Intrusion Detection System v4.1(3) Vulnerability Analysis, Version 0.2 SECURITY TECHNOLOGIES ASSESSMENT TEAM SECURITY EVALUATION FOR CIDS 4.0 Sensor, Version 1.0	This document addresses whether vulnerabilities identified could allow users to violate the TSP.

Table 5: Assurance Measures

7.2 Strength of Function Claims

The TOE incorporates user defined authentication tokens (i.e., passwords) that can be analyzed via probabilistic or permutational means. The TOE requires that the minimum password length used be equal to or greater than 6 alphanumeric characters. We also note that passwords are case sensitive. The number of possible passwords is on the order of $7*10^{-11}$. On average a brute force attack will have to try half of these values. The probability of guessing a password is low enough to be considered consistent with safe practice measures. This equates to at least an SOF-basic rating for the TOE security function Identification & Authentication that implements the FIA_UAU.1 security functional requirement component.

8 PP Claims

This ST, and its related TOE, does not claim conformance to any validated Protection Profile. However this ST is based upon the IDS System Protection Profile. Please see section 9 below for further details.

9 Relevant Protection Profiles

The TOE does not claim conformance to any validated Protection Profile. It does however meet a majority of the functional requirements and all of the assurance requirements as specified in the following Protection Profile:

Intrusion Detection System System (IDSS) Protection Profile, Version 1.4. Evaluation Assurance Level (EAL) 2 dated February 4, 2002.

The similarity between the functional requirements implemented by the TOE and those specified in the referenced Protection Profile are compared in the following table:

SFR Component	PP Requirement	Enforced in Totality by the TOE
FAU_GEN.1	Yes	Yes
FAU_SAR.1	Yes	Yes
FAU_SAR.2	Yes	Yes
FAU_SAR.3	Yes	Yes
FAU_SEL.1	Yes	Yes
FAU_STG.2	Yes	Yes
FAU_STG.4	Yes	Yes
FIA_UAU.1	Yes	Yes
FIA_AFL.1	Yes	Yes
FIA_ATD.1	Yes	Yes
FIA_UID.1	Yes	Yes
FMT_MOF.1	Yes	No[2]
FMT_MTD.1	Yes	Yes
FMT_SMF.1	Yes	Yes
FMT_SMR.1	Yes	Yes
FPT_ITA.1	Yes	Yes
FPT_ITC.1	Yes	Yes
FPT_ITI.1	Yes	Yes
FPT_RVM .1	Yes	Yes
FPT_SEP.1(1)	Yes	No[3]
FPT_STM.1	Yes	No[4]

[2] FMT_MOF.1 Management of Security Functions Behavior is a component that is required by the IDSS Protection Profile. Although this functionality is not entirely implemented by the TOE, limited, partial enforcement has instead been delegated to the IT environment. This was required as the TOE allows for limited remote management of some functionality (i.e., to power off and to reimage the module) that the IDSS Protection Profile would not allow.

[3] FPT_SEP.1 Domain Separation is a component that is required by the IDSS Protection Profile. Although this functionality is not entirely implemented by the TOE, limited, partial enforcement has instead been delegated to the IT environment. This was required as the TOE allows for limited remote management of some functionality (i.e., to power off and to reimage the module) that the IDSS Protection Profile would not allow.

IDS_SDC.1 (EXP)	Yes	Yes
IDS_ANL.1 (EXP)	Yes	Yes
IDS_RCT.1 (EXP)	Yes	Yes
IDS_RDR.1 (EXP)	Yes	Yes
IDS_STG.1 (EXP)	Yes	Yes
IDS_STG.2 (EXP)	Yes	Yes

Table 6: SFR Comparison between IDS System PP and IDSM2 ST

In addition to the functional requirement component comparison, the TOE further exceeds the assurance requirements mandated in the IDSS Protection Profile. The Protection Profile has an assurance requirement rating of EAL2 and the TOE additionally meets ALC_FLR.1 resulting in a rating of EAL2 Augmented.

[4] FPT_STM.1 Reliable Time Stamps is a component that is required by the IDSS Protection Profile. This was required as the TOE does not generate its own initial time. Instead, the TOE receives its time from the Catalyst Switch in which it has been installed.

10 RATIONALE

This section provides the rationale for the selection of the IT security requirements, objectives, assumptions, and threats. In particular, it shows that the IT security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment.

10.1 Rationale for IT Security Objectives

This section provides a rationale for the existence of each assumption, threat, and policy statement contained within this ST. Table 6 Security Environment vs. Objectives demonstrates the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

	O.PTPROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP
A.ACCESS																	X
A.DYNMIC																X	X
A.ASCOPE																	X
A.PROTCT														X			
A.LOCATE														X			
A.MANAGE																X	
A.NOEVIL													X	X	X		
A.NOTRST														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			X	X									
T.PRIVIL	X						X	X									
T.IMPCON						X	X	X					X				
T.INFLUX									X								
T.FACCNT										X							
T.SCNCFG		X															
T.SCNMLC		X															
T.SCNVUL		X															
T.FALACT					X												
T.FALREC				X													
T.FALASC				X													

T.MISUSE			X														
T.INADVE			X														
T.MISACT			X														
P.DETECT		X	X							X							
P.ANALYZ				X													
P.MANAGE	X					X	X	X					X		X	X	
P.ACCESS	X						X	X									
P.ACCACT								X		X							
P.INTGTY											X						
P.PROTCT									X					X			

Table 7: Security Environment vs. Objectives

A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.

The O.INTROP objective ensures the TOE has the needed access.

A.DYNMIC The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.

The O.INTROP objective ensures the TOE has the proper access to the IT System. The O.PERSON objective ensures that the TOE will managed appropriately.

A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.

The O.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.

A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

The O.PHYCAL provides for the physical protection of the TOE hardware and software.

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

The O.PHYCAL provides for the physical protection of the TOE.

A.MANAGE There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

The O.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

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.

The O.INSTAL objective ensures that the TOE is properly installed and operated and the O.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.

A.NOTRST The TOE can only be accessed by authorized users.

The O.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The O.CREDEN objective supports this assumption by requiring protection of all authentication data.

T.COMINT An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be modified. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.EXPORT objective ensures that confidentiality of TOE data will be maintained. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.

The O.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data. The O.INTEGR objective ensures no TOE data will be deleted. The O.PROTCT objective addresses this threat by providing TOE self-protection.

T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses through the TOE interfaces. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.IDSCAN, O.IDSENS, and O.IDANLZ objectives address this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt 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. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this threat by providing TOE self-protection.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. The O.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
T.INFLUX	An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle. The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.
T.FACCNT	Unauthorized attempts to access TOE data or security functions may go undetected. The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
T.SCNCFG	Improper security configuration settings may exist in the IT System the TOE monitors.

	The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change.
T.SCNMLC	Users could execute malicious code on an IT System that the TOE monitors which causes modification of the IT System protected data or undermines the IT System security functions. The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of malicious code.
T.SCNVUL	Vulnerabilities may exist in the IT System the TOE monitors. The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a vulnerability.
T.FALACT	The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity. The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.
T.FALREC	The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source. The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.
T.FALASC	The TOE may fail to identify vulnerabilities or inappropriate activity based on association of IDS data received from all data sources. The O. IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.
T.MISUSE	Unauthorized accesses and activity indicative of misuse may occur on an IT System the TOE monitors. The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.
T.INADVE	Inadvertent activity and access may occur on an IT System the TOE monitors.

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

T.MISACT Malicious activity, such as introductions of Trojan horses and viruses, may occur on an IT System the TOE monitors.

The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE, that contains a Sensor, collect audit and Sensor data.

P.DETECT Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.

The O.AUDITS, O.IDSENS, and O.IDSCAN objectives address this policy by requiring collection of audit, Sensor, and Scanner data.

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and appropriate response actions taken.

The O.IDANLZ objective requires analytical processes be applied to data collected from Sensors and Scanners.

P.MANAGE The TOE shall only be managed by authorized users.

The O.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN 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. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy by providing TOE self-protection.

P.ACCESS All data collected and produced by the TOE shall only be used for authorized purposes.

The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.PROTCT objective addresses this policy by providing TOE self-protection.

P.ACCACT Users of the TOE shall be accountable for their actions within the IDS.

The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated.

P.INTGTY Data collected and produced by the TOE shall be protected from modification.

The O.INTEGR objective ensures the protection of data from modification.

P. PROTCT The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions through its own interfaces

The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The O.PHYCAL objective protects the TOE from unauthorized physical modifications.

10.2 Rationale for Security Objectives for the Environment

The purpose for the environmental objectives is to provide protection for the TOE that cannot be addressed through IT measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. Together with the IT security objectives, these environmental objectives provide a complete description of the responsibilities of TOE in meeting security needs.

T.TIME Unauthorized users could attempt to modify the time on the switch, thereby passing inaccurate timestamps to the TOE, which would reflect in inaccurate reporting of events in the generated audit records.

The O.TIME objectives address this threat by requiring that the switch is configured in a known state, such that the reporting of time to the TOE is correct.

T.ENOHALT An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE through use of the TOE Environment.

The O.EIDAUTH objective addresses this threat by requiring that the environment require identification and authentication of catalyst administrators who have the capability of halting and/or reconfiguring the TOE.

10.3 Rationale For Security Requirements

This section demonstrates that the functional components selected for the TOE Security Target provide complete coverage of the defined security objectives. The following discussion provides detailed evidence of coverage for each security objective. The mapping of components to security objectives is depicted in the following table.

	O.PTPROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	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_SAR.3						X						
FAU_SEL.1						X				X		
FAU_STG.2	X						X	X	X		X	
FAU_STG.4									X	X		
FIA_UAU.1							X	X				
FIA_ATD.1								X				
FIA_UID.1							X	X				
FMT_MOF.1(1)	X						X	X				
FMT_MTD.1	X						X	X			X	
FMT_SMR.1								X				
FMT_SMF.1	X						X	X			X	
FPT_ITA.1												X
FPT_ITC.1											X	X
FPT_ITI.1											X	X
FPT_RVM.1	X					X		X		X	X	
FPT_SEP_EXP.1	X					X		X		X	X	
IDS_SDC.1		X	X									
IDS_ANL.1				X								
IDS_RCT.1					X							
IDS_RDR.1						X	X	X				
IDS_STG.1	X						X	X	X		X	
IDS_STG.2									X			

Table 8: TOE Requirements vs. Objectives Mapping

O.PTPROTCT The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage

exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1(1), FMT_SMF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1, FMT_SMF.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP_EXP.1].

O.IDSCAN The Scanner must collect and store static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System.

A System containing a Scanner is required to collect and store static configuration information of an IT System.

O.IDSENS The Sensor must collect and store information about all events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets and the IDS.

A System containing a Sensor is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System.

O.IDANLZ The Analyzer must accept data from IDS Sensors or IDS Scanners and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

The Analyzer is required to perform intrusion analysis and generate conclusions [IDS_ANL.1].

O.RESPON The TOE must respond appropriately to analytical conclusions.

The TOE is required to respond accordingly in the event an intrusion is detected [IDS_RCT.1].

O.EADMIN The TOE must include a set of functions that allow effective management of its functions and data.

The TOE must provide the ability to review and manage the audit trail of the System [FAU_SAR.1, FAU_SAR.3, FAU_SEL.1]. The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP_EXP.1].

O.ACCESS The TOE must allow authorized users to access only appropriate TOE functions and data.

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System 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.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1(1), FMT_SMF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1, FMT_SMF.1].

O.IDAUTH The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.

The TOE is required to restrict the review of audit data to those granted with explicit read-access [FAU_SAR.2]. The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the stored audit records from unauthorized deletion [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. Security attributes of subjects use to enforce the authentication policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.1, FIA_UAU.1]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1(1), FMT_SMF.1]. Only authorized administrators of the System may query and add System and audit data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1, FMT_SMF.1]. The TOE must be able to recognize the different administrative and user roles that exist for the TOE

[FMT_SMR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP_EXP.1].

O.OFLOWS The TOE must appropriately handle potential audit and System data storage overflows.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The TOE must prevent the loss of audit data in the event the audit trail is full [FAU_STG.4]. The System is required to protect the System data from any modification and unauthorized deletion, as well as guarantee the availability of the data in the event of storage exhaustion, failure or attack [IDS_STG.1]. The System must prevent the loss of audit data in the event the audit trail is full [IDS_STG.2].

O.AUDITS The TOE must record audit records for data accesses and use of the System functions.

Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The TOE must provide the capability to select which security-relevant events to audit [FAU.SEL.1]. The TOE must prevent the loss of collected data in the event the audit trail is full [FAU_STG.4]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP_EXP.1].

O.INTEGR The TOE must ensure the integrity of all audit and System data.

The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. Only authorized administrators of the System may query or add audit and System data [FMT_MTD.1, FMT_SMF.1]. The System must protect the collected data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1]. The TOE must ensure that all functions to protect the data are not bypassed [FPT_RVM.1]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP_EXP.1].

O.EXPORT When any IDS component makes its data available to another IDS component, the TOE will ensure the confidentiality of the System data.

The TOE must make the collected data available to other IT products [FPT_ITA.1]. The TOE must protect all data from modification and ensure its integrity when the data is transmitted to another IT product [FPT_ITC.1, FPT_ITI.1].

	O.EPROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.EADMIN	O.ACCESS	O.IDAUTH	O.AUDITS	O.INTEGR	O.TIME
ENV: FMT_MOF.1(2)	X	X	X	X		X	X			
ENV: FPT_STM.1										X
ENV: FPT_SEP_ENV.1 (EXP)	X				X		X	X	X	

Table 9: IT Environment Requirements vs. Objectives Mapping

O.EIDAUTH The TOE environment must be able to identify and authenticate users prior to allowing the ability to halt or reconfigure the TOE.

The environment is required to provide the ability to restrict the ability to halt or reconfigure the TOE authorized users of the environment [FMT_MOF.1(2)]

O.EPROTCT The TOE environment will maintain a domain for its own execution that protects itself and the TOE from external interference, tampering, or unauthorized disclosure.

The IT Environment must also protect itself from unauthorized modifications and access to its functions and data, in addition to restricting the management of the functions of the IT Environment to authorized users [FPT_SEP_ENV.1].

O.TIME Those responsible for the TOE must ensure that it is installed in a configured switch, which will be the source of time generation for use by the TOE

Those responsible for the TOE must assure that the time settings are managed and are accurately reflected on the switch. Management of time on the switch can be either configured manually, or set to automatically synchronize with an NTP server [FMT_MOF.1(2)]. The generated baseline time settings will then be pushed to the TOE either during initial boot-up or upon changes applied to the switch via manual changes or changes received from an NTP server [FPT_STM.1]. Once the generated baseline time has

been received from the switch, the TOE will then maintain these settings until an update is received from the switch.

10.4 TOE Summary Specification Rationale

The following table represents a mapping between the security functions to their related TOE security functional requirements and explicitly stated TOE security functional requirements.

Security Function	Security Functional Requirement
Audit	FAU_GEN.1
Audit	FAU_SAR.1
Audit	FAU_SAR.2
Audit	IDS_RDR.1
Audit	FAU_SAR.3
Audit	FAU_SEL.1
Audit	FAU_STG.2
Audit	IDS_STG.1
Audit	FAU_STG.4
Audit	IDS_STG.2
Identification & Authentication	FIA_UAU.1
Identification & Authentication	FIA_AFL.1
Identification & Authentication	FIA_ATD.1
Identification & Authentication	FIA_UID.1
Network Traffic Analysis	FMT_MOF.1(1)
Network Traffic Analysis	FMT_MTD.1
Network Traffic Analysis	FMT_SMF.1
Network Traffic Analysis	IDS_SDC.1
Network Traffic Analysis	IDS_ANL.1
Network Traffic Analysis	IDS_RCT.1
Roles	FMT_SMR.1
Self-protection	FPT_ITA.1
Self-protection	FPT_ITC.1
Self-protection	FPT_ITI.1
Self-protection	FPT_RVM.1
Self-protection	FPT_SEP_EXP.1 (EXP)

Table 9: Mapping of Security Functions to Security Functional Requirements

The following sections provide justification on how each of the security functional requirements is implemented by the TOE security functions.

10.4.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1 is implemented by the Audit security function. By default, all IDS signatures trigger an audit event; this default cannot be modified. The TOE provides continuously running audit functions which are used to record audit events. These audit events are then written to the fixed-size circular event store (that is all generated audit events are written to one event store). Each event is stored in XML format and can be viewed via the Web Interface and the CLI Interface. Each audit event contains the following information: date of the event, time of the event, type of event, subject identity, and outcome of the event. Additional information where appropriate includes: user identity, location, object IDS, and requested access. The following gives an example audit event.

```
evLogTransaction: command=getEventStoreStatistics
eventId=1040436066141672995 successful=true
  originator:
    hostId: cisco_ids
    appName: mainApp
    appInstanceId: 697
  time: 2003/01/10 16:51:22 2003/01/10 16:51:22 UTC
  requestor:
    user: cisco
    application:
      hostId: 192.168.0.23
      appName: -cidcli
      appInstanceId: 10254
```

The TOE audits all information described in Table 2: Audited Events. Below is a brief description of the categories of events the TOE defines:

alert
Display alerts. Provides notification of some suspicious activity that may indicate an intrusion attack is in progress or has been attempted. Alert events are generated by the analysis-engine whenever an IDS signature is triggered by network activity.

error
Display error events. Error events are generated by services when error conditions are encountered.

log
Display log events. These events are generated whenever a transaction is received and responded to by an application. It contains information about the request, response, and success or failure of the transaction.

status
Display status events.

NAC
Display Network Access Control requests (shun requests).

The table below presents a mapping of Events as defined in Table 2: Auditable Events to the categories of events as defined for the TOE. All of these events are audited and written to the event store.

Component	Event	Details	Category of Event
FAU_GEN.1	Start-up and shutdown of audit functions		log
FAU_GEN.1	Access to System		log
FAU_GEN.1	Access to the TOE and System data	**Object IDS, Requested access**	log
FAU_SAR.1	Reading of information from the audit records		log
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	**This is not applicable. All authenticated users have permission to read this data.**	N/A
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating		status
FIA_UAU.1	All use of the authentication mechanism	**User identity, location**	log status error
FIA_UID.1	All use of the user identification mechanism	**User identity, location**	log status error
FMT_MOF.1	All modifications in the behavior of the functions of the TSF		log
FMT_MTD.1	All modifications to the values of TSF data		status

Component	Event	Details	Category of Event
FMT_SMR.1	Modifications to the group of users that are part of a role	**User identity**	status log
FPT_ITI.1	The action taken upon detection of modification of transmitted TSF data		error

Table 10: Auditable Event Categories

The following examples provide generic audit record formats for the categories of events specified in the last column of the above table:

Log

evLogTransaction: command=<control transaction>
eventId=<event ID number> successful=<true|false>
originator:
hostId: <Cisco IDS name>
appName: <Cisco IDS Application>
appInstanceId: <appInstance ID number>
time: <time>
requestor:
user: <username>
application:
hostId: <IP address of requestor>
appName: -<requesting application>
appInstanceId: <appInstance ID of requesting application>

Status

evStatus: eventId=< event ID number>
originator:
hostId: <Cisco_IDS name>
appName: <Cisco IDS Application>
appInstanceId: <appInstance ID number>
time: <time>
configChanged:
description: <descriptive text>
requestor:
user: <username>
application:
hostId: <IP address of requester>
appName: <requesting application>
appInstanceId: <appInstance ID number>
configFile: <configuration file changed>

systemRestartRequired: <true|false>
overWriteWasForced: <true|false>

error

evError: eventId=<event ID number> severity=warning|error|fatal>
originator:
hostId: <Cisco IDS name>
appName: <originating application name>
appInstanceId: <appInstance ID number
time: <time>
errorMessage: <Message associated with error>

10.4.2 FAU_SAR.1 Audit Review

FAU_SAR.1 is implemented by the Audit security function. By default, all IDS signatures trigger an audit event that is then available for review; this default cannot be modified. Authorized administrators, operators and viewers are allowed access to the audit records and to read the following information from the audit records: date of the event, time of the event, type of event, subject identity, outcome of the event, and other relevant data (in this regard all authorized users of the TOE can read all information from the event store). Additional information where appropriate includes: user identity, location, object IDS, and requested access. Furthermore, as demonstrated by the example audit records presented above, the audit records are organized in a clear and concise manner.

10.4.3 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2 is implemented by the Audit security function. The TOE has in place sufficient access controls, described in this section, to ensure that only authorized users can read audit data, all others are denied access to this data. There are two ways in which to view audit records. One involves authenticating via the CLI Interface and the other via the Web Interface. In both cases, valid authentication credentials are required in order to authenticate to the TOE. Only after authentication is the user allowed to view audit records; and this is the only way by which users can view audit records.

10.4.4 IDS_RDR.1 Restricted Data Review

IDS_RDR.1 is implemented by the Audit security function. The TOE has in place sufficient access controls, described in this section, to ensure that only authorized users can read all event data generated by the IDS, all others are denied access to this data. There are two ways in which to view this event data. One involves authenticating via the CLI Interface and the other via the Web Interface. In both cases, valid authentication credentials are required in order to authenticate to the TOE. Only after authentication is the user allowed to view this event data; and this is the only way by which users can view event data generated by the IDS.

10.4.5 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3 is implemented by the Audit security function. The TOE provides functionality which allows authorized users the ability to sort audit records based on date and time, subject identity, type of event, and success or failure of related event. Some of these parameters can be specified through the Web Interface by selecting the appropriate fields or through the CLI Interface by augmenting the command show events with the appropriate parameters.

The following is a brief description of how events can be sorted through the CLI:

Note that in order to display all events through the CLI one must specify a time which is as old or older than the oldest event in the event store. Here we choose an arbitrary time in the past (May 1 2001).

Sorting based upon date and time of the event.
Enter the command: show event 00:00 May 1 2001

Sorting based upon category of event.
Enter the command: show event error 00:00 May 1 2001
Enter the command: show event log 00:00 May 1 2001
Enter the command: show event status 00:00 May 1 2001

Sorting based subject identity
Enter the command: show users all
For each user displayed under the User column after step 2 has been entered enter the command: show events 00:00 May 1 2001 | include user: <username>. Where username is replaced by each username displayed after step 2.

Sorting based upon Success or failure of the event.
Enter the command: show events 00:00 May 1 2001 | include successful=true.
Enter the command: show events 00:00 May 1 2001 | include successful=false.

Sorting based upon type of event as defined in Table 2 of the ST/PP
The table below presents the commands for sorting all events defined in Table 2.

Component	Command
Start-up and shutdown of audit functions	show events 00:00 May 1 2001 | include command=getHostConfig show events 00:00 May 1 2001 | include command=execShutdownHost
Access to System	show event log 00:00 May 1 2001
Access to the TOE and System data	show event log 00:00 May 1 2001
Reading of information from the audit records	show events log 00:00 May 1 2001 | include command=getAnalysisEngineConfig
Unsuccessful attempts to read information from the audit records	This is not applicable. All authenticated users have permission to read this data.
All modifications to the audit configuration that occur while the audit collection functions are operating	show events status 00:00 May 1 2001 | include configChanged
All use of the authentication mechanism	show events log 00:00 May 1 2001 | include command=execAuthenticateUser show events status 00:00 May 1 2001 | include loginAction show events error 00:00 May 1 2001 | include pam_unix
All use of the user identification mechanism	show events log 00:00 May 1 2001 | include command=execAuthenticateUser show events status 00:00 May 1 2001 | include loginAction show events error 00:00 May 1 2001 | include pam_unix
All modifications in the behavior of the functions of the TSF	show events log 00:00 May 1 2001 | include command=(addComponentConfig | addIpLog | addShunEntry |

Component	Command
	disableShunning | enableShunning | execAssignCertificate | execCreateCertificateRequest | execDowngradeSoftware | execEndIpLog | execGenerateHostCertificate | execGenerateHostSshkey | execIssueCertificate | execObtainCertificate | execRebootHost | execShutdownHost | execUpgradeSoftware | getAndResetComponentStatistics | removeComponentConfig | removeShunEntries | setComponentConfig | setEnableAuthenticationTokenStatus | setFailover | setTime | setUserAccountConfig)
All modifications to the values of TSF data	show events status 00:00 May 1 2001 | include configChanged
Modifications to the group of users that are part of a role	show events 00:00 May 1 2001 | include (etc/curHostConfig.xml | setUserAccountConfig)
The action taken upon detection of modification of transmitted TSF data	show events error 00:00 May 1 2001 | include (pam_unix | session closed for user)

Table 11: Audit Commands

10.4.6 FAU_SEL.1 Selective Audit

FAU_SEL.1 is implemented by the Audit security function. By default, all IDS signatures trigger an audit event; this default cannot be modified. This ensures that the TOE audits security relevant information allowing for complete auditing capabilities. In addition, the TOE has robust post selection capabilities, allowing authorized users to sort out all information defined in Table 2. This combination of full auditing and robust post selection meet the requirements for selective audit.

The TOE can also perform IP logging. Additionally, the logs generated from IP logging are a form of pre-selection which is supported by the TOE from the web interface.

When IP logging is configured as a response action for a signature and the signature is triggered, all packets to and from the source address of the alarm are logged for a specified period of time. You can set the number of minutes for which events are logged. These events are also searchable using the IP Logs feature of the CLI and the web interface.

10.4.7 FAU_STG.2 Guarantees of Audit Data Availability

FAU_STG.2 is implemented by the Audit security function. Only an authorized administrator can clear audit records via the clear events command through the CLI Interface. No other user (i.e., viewer, operator) is authorized to modify the audit records. Authorized users must authenticate to the TOE by providing valid authentication credentials. Authentication must be successful and the user must be authenticated at the privilege level of an Administrator before the clear event command can be issued. All users at a privilege level other than Administrator cannot issue this command. Both the CLI and Secure Web Server build a list of valid commands which can be issued when the user authenticates. These commands are determined by the user's privilege level. If the command to clear the audit records, (clear events) is issued by a unauthorized user which is not in the users privilege level (viewer or operator), the CLI (or Secure Web Server) will return a syntax error and will not execute the command. If an unauthenticated user provides invalid authentication data or attempts to issue a command prior to authentication the event is audited.

In the event of audit storage exhaustion (that is, when the event store becomes full) the number of records saved will be the total number of audit events in the event store minus the total number of audit events inserted in the event store subsequent to audit storage exhaustion. The actual bit size of the amount maintained is both proportional to the size of the event store and the actual bit size of the audit events inserted in the event store subsequent to audit storage exhaustion. This effectively means that the once the event store is full, the newest events will begin to overwrite the oldest events.

10.4.8 IDS_STG.1 Guarantee of System Data Availability

IDS_STG.1 is implemented by the Audit security function. Only an authorized administrator can clear IDS event data via the clear events command through the

CLI Interface. No other user is authorized to modify the IDS event data. When a user successfully authenticates to the TOE, the users privilege level is used to create the set of commands that the user is allowed to issue. If the user issues a command which is above his/her privilege level the command will not be recognized, and therefore will not be issued. In the event of IDS event storage exhaustion (that is, when the event store becomes full) the number of records saved will be the total number of IDS events in the event store minus the total number of IDS events inserted in the event store subsequent to IDS event storage exhaustion. The actual bit size of the amount maintained is both proportional to the size of the event store and the actual bit size of the IDS events inserted in the event store subsequent to IDS event storage exhaustion. This effectively means that the once the event store is full, the newest events will begin to overwrite the oldest events.

10.4.9 FAU_STG.4 Prevention of Audit Data Loss

FAU_STG.4 is implemented by the Audit security function. The TOE uses a fixed-size circular event store to store audit data. When the event store's capacity is reached, the TOE shall overwrite the oldest stored audit records and send an alarm (that is an event is generated stating that the event store is being overwritten. This event is written to the event store) to the Event Store, this alarm (or rather event) can then be viewed by an authorized user through the CLI Interface or the Web Interface.

10.4.10 IDS_STG.2 Prevention of System Data Loss

IDS_STG.2 is implemented by the Audit security function. The TOE uses a fixed-size circular event store. When the event store's capacity is reached the TOE shall overwrite the oldest stored records and send an alarm (that is an event is generated stating that the event store is being overwritten. This event is written to the event store) to the Event Store, this alarm (or rather event) can then be viewed by an authorized user through the CLI Interface or the Web Interface.

10.4.11 FIA_UAU.1 Timing of Authentication

FIA_UAU.1 is implemented by the Identification & Authentication security function. Prior to a user authenticating through both the CLI Interface and the Web Interface unauthenticated users are only allowed to establish an encrypted channel (or an unencrypted channel in the case of the console interface), and provide authentication data to the TOE.

In the case of the console interface, the user is prompted a login prompt, and allowed to enter authentication data In the case of the CLI Interface (over the Management Physical Interface), the user performs the SSH protocol handshake, is prompted with a login prompt, and is allowed to enter authentication data. Note that through this interface a user can also authenticate via RSA authentication, in which case the user is authenticated as part of the SSH protocol handshake using an RSA key pair.

In the case of the Web Interface, the user performs the TLS protocol handshake, is prompted with a login pop up window, and is allowed to enter authentication data.

10.4.12 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1 is implemented by the Identification & Authentication security function. The TOE provides logging of authentication attempts. In the evaluated configuration of the TOE, after a settable, non-zero number of unsuccessful authentication attempts have been made, the associated account is locked until an authorized administrator unlocks the account.

10.4.13 FIA_ATD.1 User Attribute Definition

FIA_ATD.1 is implemented by the Identification & Authentication security function. The TOE maintains user identity, authentication data, and authorizations on each user of the system. These take the form of the tuplet {username, password, group}. The username and password are stored in the underlying operation system. For clarification, the password is not stored directly, but rather as a cryptographic hash. The Authentication Application stores the users associated group, which essentially takes the form of the couplet {username, group}. In the case of RSA authentication an {RSA public key, username} is also stored in the underlying operating system, this is in addition to the above credentials.

10.4.14 FIA_UID.1 Timing of Identification

FIA_UID.1 is implemented by the Identification & Authentication security function. Prior to a user authenticating through both the CLI Interface and the Web Interface unauthenticated users are only allowed to establish an encrypted channel, and provide authentication data to the TOE[5]. In the case of the CLI Interface, the

[5] Note that in the case of the console physical interface this differs slightly in that the user is directly allowed to provide authentication data to the TOE.

user performs the SSH protocol handshake, is prompted with a login prompt, and is allowed to enter identification data. Note that through this interface a user can also authenticate via RSA authentication, in which case the user is authenticated as part of the SSH protocol handshake using an RSA key pair and the user is not given a login prompt. In the case of the Web Interface, the user performs the TLS protocol handshake, is prompted with a login pop up window, and is allowed to enter identification data.[6]

10.4.15 FMT_MOF.1(1) Management of Security Functions Behavior

FMT_MOF.1(1) is implemented by the Network Traffic Analysis security function. The protection mechanisms within the TOE provide assurance that only authorized administrators are allowed to modify the system data collection, analysis, and reaction functions. These modifications take the form of modifications as to how the TOE collects, analyzes, and reacts to event data collected on the target IT network. It is to be noted that the TOE includes a set of signatures that serve as pre-configured rule sets. This allows the administrator the capability to specify the policy configuration input to be used by the TOE. Additional signature updates are provided by Cisco.

The Web Server is a primary component that controls a user's access to services provided by the TOE. After the initial authentication process, the web server stores the user's access privileges and only presents the user with functionality which that user is authorized to perform. Tabs and links that the user is not authorized to perform are not displayed and inaccessible. The Web Server will simply not provide web pages that would allow the user to request data they are not permitted to access. The Web Server restricts management capabilities such as modifying the behavior of the system, querying or adding System and audit data to authorized users.

The CLI is another primary component that controls a user's access to services provided by the TOE. After the initial authentication process, the CLI stores the user's access privilege and only presents the user with functionality which that user is authorized to perform. Commands that the user is not authorized to perform are not recognized and are inaccessible. The CLI will not provide commands which would allow the user to request data they are not permitted to access. The CLI restricts management capabilities such as modifying the behavior of the system, querying or adding system and audit data to authorized users.

10.4.16 FMT_MTD.1 Management of TSF Data

[6] Within this feature of the TOE, there are no differences between FIA_UAU.1 and FIA_UID.1.

FMT_MTD.1 is implemented by the Network Traffic Analysis security function. Only an authorized administrator has sufficient privileges to query and add system and audit data. The Operator group only has sufficient privileges to query and modify data generated by the IDS from the targeted IT network, as well as query audit data. The Viewer group only has sufficient privileges to query data generated by the IDS from the targeted IT network, as well as query audit data. The protection mechanisms discussed above, in the section entitled 'Managements of security functions behavior' explains how the TOE ensures this requirement is enforced.

10.4.17 FMT_SMF.1 (Interpretation 065) Specification of Management Functions

FMT_SMF.1 is implemented by the Network Traffic Analysis security function. This function supports FMT_MOF.1(1) and FMT_MTD.1 by providing the specification of data protection attributes and management of security functions provided by the TOE. This function limits such modifications to the TOE to the roles managed by the TOE and specified in FMT_SMR.1.

10.4.18 IDS_SDC.1 System Data Collection

IDS_SDC.1 is implemented by the Network Traffic Analysis security function. The TOE is a network based Intrusion Detection System that passively scans nearly every packet on a given network segment. The TOE both analyzes single packets, and retains state on user sessions to detect multiple packet attacks and packet content string matches. It captures network packets with one of its own interfaces, then reassembles and compares this data against a rule set that indicates typical intrusion activity. The information collected with each event includes date and time of the event, type of event and severity, IP and port address of the event (both source and destination), protocol type, and data associated with the event. The fact that an event has been generated indicates the event has succeeded.

The example below demonstrates the format of a typical event:

```
    evAlert: eventId=1040415606141678787 severity=high
  originator:
    hostId: cisco_ids
    appName: sensorApp
    appInstanceId: 1023
  time: 2002/12/23 13:52:53 2002/12/23 13:52:53 UTC
  interfaceGroup: 0
  vlan: 0
  signature: sigId=4003 sigName=Nmap UDP Port Sweep subSigId=0 version=1.0
```

```
participants:
  attack:
    attacker:
      addr: locality=OUT 192.168.0.14
      port: 53
    victim:
      addr: locality=OUT 192.168.0.10
      port: 1674
      port: 1679
      port: 1683
      port: 1684
      port: 1690
      port: 1693
      port: 1698
      port: 1700
```

10.4.19 IDS_ANL.1 Analyser Analysis

IDS_ANL.1 is implemented by the Network Traffic Analysis security function. The TOE adheres to the signature analysis method. That is, it matches specific signatures or patterns that may characterize attack attempts to a database of known attacks. This data base can be updated and user customized to provide up to date coverage of known attacks. The table below summarizes examples of specific attacks the TOE attempts to defend against.

Category of Attack	Details	Example attacks
Named attacks	Single attacks that have specific names or common identities	- Smurf - PHF - Land
General Category attacks	Attacks that keep appearing in new variations with the same basic methodology	- Impossible IP Packet - IP fragmentation
Extraordinary attacks	Extremely complicated or multi-faceted attacks	- TCP hijacking - E-mail spam

Table 12: Attack Examples

Each analytical result is written to the event store. These events can then be viewed by authorized users through the CLI Interface or the Web Interface. The TOE is a network based Intrusion Detection System that passively scans nearly every pack on a give network segment. The TOE both analyzes single packets, and retains state on user sessions to detect multiple packet attacks and packet content string matches. It

captures network packets with one of its own interfaces, then reassembles and compares this data against a rule set that indicates typical intrusion activity. The example above demonstrates the typical format. Each event includes Date and time of the result, type of result, identification of the data source, and other pertinent information.

10.4.20 IDS_RCT.1 Analyser React

IDS_RCT.1 is implemented by the Network Traffic Analysis security function. When the TOE generates an alarm, it is automatically sent to the event store. By default the TOE only generates an alarm when an intrusion is detected, however it can also be configured to perform a TCP reset on the connection in question if an intrusion is detected. Another option is that the TOE can send a command to a Cisco router, switch, or PIX firewall to block specific offending network traffic.

10.4.21 FMT_SMR.1 Security Roles

FMT_SMR.1 is implemented by the Roles security function. The evaluated configuration of the TOE maintains three groups[7]. All users are assigned to one of these defined groups. In descending privilege level, these groups are:

- Administrator,
- Operator, and
- Viewer

The protection mechanisms discussed above, in the section entitled 'Managements of Security Functions behavior' explains how the TOE ensures this requirement is enforced.

In addition, the TOE has a special service account. Only one service account can be created. The service account corresponds to the root account on the underling Linux operating system. This account is not needed for any administration of the TOE, nor should it be used for meeting any of the requirements, unless otherwise stated in the guidance documentation, in this ST. Its purpose is for trouble shooting of the TOE.

10.4.22 FPT_ITA.1 Inter-TSF Availability Within a Defined Availability Metric

[7] Throughout the documentation we will refer to groups and roles interchangeably.

FPT_ITA.1 is implemented by the Self-protection security function. The availability of audit and system data provided to a remote trusted IT product is dependent on a number of factors. The two most dominating factors are the performance of the intervening network and the performance of the TOE and the remote trusted IT product. Because the performance of a given network is architecturally specific we assume that there is normal traffic on the communications network and that it is transmitting data at a rate of at least 10 Mbits per second. We also assume that the IT product is operating within its specified parameters. The TOE has been designed to provide fast and efficient analysis and reporting of all system data. Once the TOE has received a request, the response time will be less than 60 seconds.

10.4.23 FPT_ITC.1 Inter-TSF Confidentiality During Transmission

FPT_ITC.1 is implemented by the Self-protection security function. The TOE uses cryptographic mechanisms to ensure the confidentiality of all data transmitted to a remote trusted IT product. Specifically it relies on symmetric encryption provided by the SSH protocol and TLS v1.0.

10.4.24 FPT_ITI.1 Inter-TSF Detection of Modification

FPT_ITI.1 is implemented by the Self-protection security function. The TOE uses message authentication codes (MACs) within the SSH and TLS protocols to provide data integrity on all data transmitted to a remote trusted IT product. In both cases the MACs used are either HMAC-SHA1 or HMAC-MD5.

If modification is detected (i.e., verification of the MAC fails) the TOE will discard the packet.

10.4.25 FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1 is implemented by the 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. More specifically, once a user has been authenticated, the Authentication Application subsystem is queried and returns the user's group. If the user is authenticating through the CLI Interface, the CLI component will determine what functionality (depending on the user's group) is presented to the user. If the user is authenticating via the Web Interface, the Secure Web Sever will determine what functionality (again, depending on the user's group) is presented to the user.

This is not performed every time a user interacts with the TSFs, but rather every time a user authenticates to the TOE. Additionally, no other means, other than described above, are provided for the user to interact with the TOE.

10.4.26 FPT_SEP_EXP.1 TSF Domain Separation

FPT_SEP_EXP.1 is implemented by the Self-protection security function. The TOE is a hardware device that executes all of its processes internally. It is accessible only via the defined interfaces and only authorized administrators are able to modify the functionality of the TOE through its interfaces.

The Data Network interface is a dedicated physical and logical interface that is associated with network interface ports and used to passively monitor network packets from the target IT system. It does not implement a TCP/IP protocol stack and does not have a routable IP address. It simply receives raw packets for analysis within the TOE.

This interface enforces domain separation in that any data sent to this interface (which is presumed untrusted) is logically separated from all other TOE data. It is never executed but rather is parsed for analysis.

Traffic flowing through the TOE is subject to the policies as defined by the authorized administrators.

At all physical interfaces, the TOE intercedes to ensure domain separation. Traffic 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.

10.5 Rationale for Assurance Requirements

EAL2 augmented with ALC_FLR.1 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 System 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 System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment. This ST chose EAL2 augmented with ALC_FLR.1 in order to exceed the conformance requirement to the Assurance

Requirements specified in the Intrusion Detection System System Protection Profile Version 1.4, February 4, 2002.

10.6 Rationale For Explicitly Stated Requirements

A family of IDS requirements was created to specifically address the data collected and analyzed 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.

Due to the need to divide the FPT_SEP requirement between the TOE and the environment it was necessary to create two explicit requirements, FPT_SEP_EXP.1 for the TOE, and FPT_SEP_ENV.1 for the environment. This was done in accordance with the Basic Robustness guidance for software only TOEs. The FPT_SEP command was used as the model for creation of these requirements. The purpose was to ensure that the FPT_SEP requirement was accurately stated for that portion of the requirement allocated to the TOE and to its environment. There are no dependencies.

10.7 Rationale For Strength Of Function

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 as required by the Intrusion Detection System System Protection Profile Version 1.4, February 4, 2002.

10.8 Rational For Satisfying All Dependencies

The Intrusion Detection System System Protection Profile satisfies all of the requirement dependencies of the Common Criteria. Table 13: Requirement Dependencies lists each requirement from the Intrusion Detection System System Protection Profile with a dependency and indicates whether the dependent requirement was included. As the table indicates, not all of the dependencies have been met.

Functional Component	Dependency	Included
FAU_GEN.1	FPT_STM.1	NO
FAU_SAR.1	FAU_GEN.1	YES
FAU_SAR.2	FAU_SAR.1	YES
FAU_SAR.3	FAU_SAR.1	YES
FAU_SEL.1	FAU_GEN.1 and FMT_MTD.1	YES
FAU_STG.2	FAU_GEN.1	YES
FAU_STG.4	FAU_STG.2	YES
FIA_UAU.1	FIA_UID.1	YES
FMT_MTD.1	FMT_SMR.1	YES
FMT_SMR.1	FIA_UID.1	YES

Table 13: Requirement Dependencies

As identified in the above table, the only dependency not met by the TOE is FPT_STM.1. As a result, this security functional requirement component must be enforced by the IT environment (FPT_SEP.1(2)).

11 REFERENCES

11.1 Acronyms

This section provides a list of acronyms used within the ST.

ACL:	Access Control List
CC:	Common Criteria version 2.1 (ISO/IEC 15408:1999)
CLI:	Command Line Interface
Cisco IDS:	Cisco Intrusion Detection System
EAL:	Evaluation Assurance Level
ID:	Intrusion Detection
IDAPI:	Intrusion Detection Application Program Interface
IDIOM:	Intrusion Detection Interaction and Operations Messages
IDS:	Intrusion Detection System
IOS:	Internetwork Operating System Software
IT:	Information Technology
MAC:	Message Authentication Code
NTP:	Network Time Protocol
OS:	Operating System
PAM:	Pluggable Authentication Module
PP:	Protection Profile
SAR:	Security Assurance Requirements
SFP:	Security Function Policy
SFR:	Security Functional Requirements
SOF:	Strength Of Function
SPAN:	Switching Port Analyzer
SSL:	Secure Socket Layer v3.0
SSH:	Secure Shell
ST:	Security Target
TCP:	Transmission Control Protocol
TLS:	Transport Layer Security v1.0
TOE:	Target Of Evaluation
TSF:	TOE Security Function(s)
TSP:	TOE Security Policy