Cisco Intrusion Prevention System (IPS) Version 6.0 Security Target

Version 7.0
May 30, 2007

Document No. EDCS-606769

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco IPS Version 6.0 Security Target

Prepared By:	Prepared For:
Tresys Technology, LLC	Cisco Systems, Inc.
8840 Stanford Blvd., Suite 2100	170 West Tasman Dr.
Columbia, MD 21045	San Jose, CA 95134

Document Introduction

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Intrusion Prevention System (IPS) Sensor Software version 6.0 (IPSv6.0) executing on the following platforms: Cisco IPS 4200 Series sensors, Cisco Catalyst 6500 Series IDSM-2, Advanced Inspection and Prevention (AIP) Security Services Module (SSM) for the Cisco Adaptive Security Appliance (ASA), and the Cisco Intrusion Detection System Network Module (NM-CIDS) for Cisco Routers. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements.

Revision History

Rev	Date	Description
1.0	January 13, 2006	Draft release
1.1	February 13, 2006	Updated in response to CCTL comments dated 01/13/06
1.2	February 13, 2006	Incorporated PD-0097
1.3	March 17, 2006	Revisions based on CCTL verdicts (Cycle 1)
2.0	September 5, 2006	PP version change and deleted audit descriptions relating to the log file. Checked for ASDM references.
3.0	October 30, 2006	Revisions based on CCTL verdicts (Cycle 2)
4.0	December 1, 2006	Updated version 6.0 references
5.0	February 9, 2007	Revisions based on CCTL verdicts Cycle 3
6.0	April 23, 2007	Updated based on CCTL final comments
7.0	May 30, 2007	Address Final VOR comments

CONTENTS

CHAPTER 1

Security Target Introduction

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

- A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the product is intended to counter, and any known rules with which the product must comply (Chapter 3, Security Environment).
- A set of security objectives and a set of security requirements to address the security problem (Chapters 4 and 5, Security Objectives and Security Requirements, respectively).
- The IT security functions provided by the TOE that meet the set of requirements (Chapter 6, TOE Summary Specification).

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

ST and TOE Identification

This section provides information needed to identify and control this ST and its TOE. This ST targets Evaluation Assurance Level (EAL)2 augmented with ALC_FLR.1.

ST Title	Cisco Intrusion Prevention System (IPS) Version 6.0
ST Version	Version 7.0
Publication Date	May 30, 2007
Kick-off Date	March 24, 2006
Vendor	Cisco Systems, Inc
ST Authors	Tresys Technology, LLC
TOE Identification	Cisco IPS v6.0 (IDS 4200 Series Sensors (IPS 4255, IDS 4250, IPS4240, IDS4215, IPS4260); Cisco AIP-SSM-10 and AIP-SSM-20; NM-CIDS, IDSM-2)
CC Identification	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

Common Criteria Conformance Claim	The ST is compliant with the Common Criteria (CC) Version 2.3. with the following NIAP Interpretation applied (as of the evaluation kick-off on March 24 2006): I-0407 This ST uses the CCEVS Precedents PD-0097 to address excluded PP requirements, PD-0106 to allow no user guide to meet AGD_USR.1, and PD-108 to specify trusted channel for remote administration. The ST is EAL2, Part 2 extended, and Part 3 augmented (ALC_FLR.1).
Protection Profile Conformance	Intrusion Detection System System Protection Profile, Version 1.6, dated April 4, 2006
Security Target Evaluation Status	Currently under evaluation.
Keywords	Intrusion Detection System (IDS), Intrusion Prevention System (IPS), signatures, sensor, analyzer, signature analysis, security target

Since the TOE can be implemented either in an appliance configuration or in a module configuration, it may be necessary in this ST to make a distinction between the two. When it is necessary to differentiate the appliance configuration, the ST authors will refer to it as the “Appliance TOE.” When it is necessary to differentiate the module configuration, the ST authors will refer to it as the “Module TOE.” If no distinction is necessary, the ST authors will refer to it simply as the “TOE”. When the ST authors use “TOE,” the reader should understand it to mean any and all of the appliance and module TOE configurations.

Security Target Overview

The TOE consists of hardware and software used to provide an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) solution that is designed to identify, classify, and stop malicious traffic before they affect network continuity.

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.

Intrusion prevention takes real time actions by stopping attacks before they reach the intended target. Intrusion prevention systems offer a deeper analysis of network traffic to identify and stop and/or block attacks that would normally pass through other security components.

This ST is based on the IDS System Protection Profile (PP) Version 1.6 and describes the Cisco IPSv6.0 features that satisfy the security functional and assurance requirements identified in the PP.

References

The following documentation was used to prepare this ST:

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 2005, version 2.3, CCMB-2005-08-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, version 2.3, CCMB--2005-08-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, version 2.3, CCMB-2005-08-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated August 2005, version 2.3 CCMB-2005-08-004
[IDSPP]	Intrusion Detection System System Protection Profile, Version 1.6, dated April 4, 2006

Acronyms and Abbreviations

Table 1-1 presents the acronyms and abbreviations are used in this Security Target:

Table 1-1 **Acronyms and Abbreviations**

Acronyms / Abbreviations	Definition
ACL	Access Control List
AIP	Advanced Inspection and Prevention
ASA	Adaptive Security Appliance
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
EAL	Evaluation Assurance Level
FSP	Functional Specification
HLD	High Level Design
HMAC	Hashed Message Authentication Code
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IDSM-2	Intrusion Detection System Services Module

Table 1-1 Acronyms and Abbreviations *(continued)*

Acronyms / Abbreviations	Definition
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
MAC	Message Authentication Code
NAC	Network Access Control
NIAP	National Information Assurance Partnership
NM-CIDS	Cisco Network Module IDS
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
RSA	Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SOF	Strength of Function
SPAN	Switched Port Analyzer
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TCP	Transfer Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
VACL	VLAN Access Control Lists
VLAN	Virtual Local Area Network
XML	Extensible Markup Language

CHAPTER 2

TOE Description

This chapter provides an overview of the TOE to assist potential users in determining whether it meets their needs for intrusion detection and prevention functionality. The TOE for this ST consists of the following Cisco Sensors that support Cisco IPSv6.0: Cisco IPS 4200 Series sensors, Cisco Catalyst 6500 Series IDSM-2, Advanced Inspection and Prevention (AIP) Security Services Module (AIP SSM) for the Cisco Adaptive Security Appliance ASA, and the NM-CIDS for Cisco Routers. This chapter also defines the physical and logical boundaries; summarizes the security functions; and describes the evaluated configuration.

TOE Product Type

The TOE is a network-based Intrusion Detection and Prevention System that monitors traffic in real-time. It can analyze both the header and content of each packet. The TOE can analyze single packets or a complete flow for 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.

All data collection and analysis is performed by the TOE which is to be placed at strategic points throughout a target IT system[1] to interrogate passing network traffic. In response to an attack, the TOE has several options that include generating an alarm, logging the alarm event, configuring access control lists (ACLs) to block attackers, dropping and modifying packets, and killing Transfer Control Protocol (TCP) sessions.

TOE Overview

The TOE for this ST is Cisco IPSv6.0 software executing on an appliance (i.e., Cisco IPS 4200 Series Sensors) or a module. Modules for this ST include the AIP SSM Module for the Cisco ASA, the IDSM-2 module for the Catalyst 6500 Series switches, or the NM-CIDS network module for Cisco routers.

Intrusion Detection and Prevention System Concept

Traditionally, an IDS passively monitors packets on a given target network looking for malicious activity. The typical means by which the IDS detects malicious activity is by using signature analysis on captured packets to determine the type of attack. In promiscuous mode, the IDS analyzes a copy of

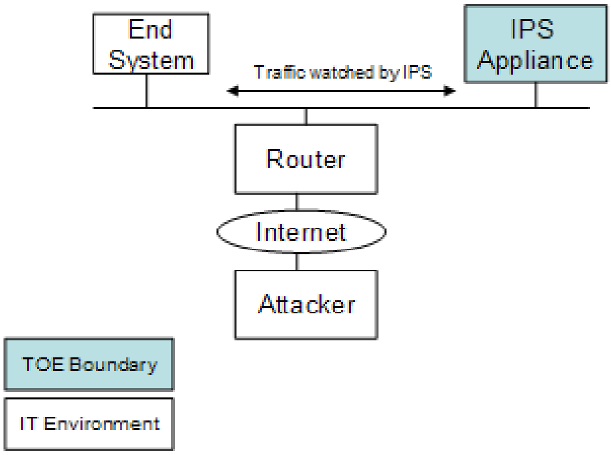
[1] Here and throughout this document, we use the terms IT system and IT network synonymously when we refer to what the TOE is monitoring.

the monitored traffic rather than the actual packet. If a packet or series of packets triggers an alarm based on signature analysis, information related to this possible intrusion is collected to be reviewed in real-time or historically. This information allows the administrator of the IDS to detect real time attacks, as well as perform forensic investigation on past attacks. Additional administrator configurable actions could be taken by the IDS to include connection resets and configuring access control lists to block the attacker.

The disadvantage of intrusion detection is that the IDS cannot stop malicious traffic from reaching its intended target for certain types of attacks. The response actions by the IDS are post-event responses and often require assistance from other networking devices (routers and firewalls) to respond to an attack.

Intrusion prevention directly affects traffic flow to stop attacks from reaching the intended target. In inline mode, the IPS sits on the network which allows the IPS to stop attacks by dropping detected malicious traffic. The IPS analyzes the actual packet. If a packet or series of packets triggers an alarm, packet drop actions could be taken in addition to IDS actions. Figure 2-1 illustrates an example network topology using the IPSv6.0.

Figure 2-1 Example Network Topology Using IPSv6.0



TOE Physical Boundary

The evaluated configuration of the TOE includes four representations. Figure 2-2 below shows an actual picture of the physical TOE representations. On the left side of the picture is the Cisco IPS 4200 Series appliance, representative of all appliance models covered in this ST. The appliance is a self contained unit which provides all TOE functionality for the Appliance TOE. The Cisco NM-CIDS and Cisco IDSM-2 shown in the picture are the plug-in modules sitting atop the router appliance and switch appliance respectively. The plug-in modules each provide all TOE functionality for the Module TOE. Though the Cisco AIP SSM is not pictured, it is similar to the Cisco NM-CIDS and the Cisco IDSM-2 in that the AIP SSM is a plug in module for the ASA appliance and provides all TOE functionality for the Module TOE. The specific module and appliance models for the TOE are listed below in Table 2-1. These models only differ in hardware configuration and throughput and do not affect how the security functions specified in the ST are met.

Figure 2-2 TOE Implementations

Table 2-1 TOE Appliances and Modules

Model Name	Part Number
Appliances	
IDS-4215	IDS-4215-4FE-K9
IDS-4250	IDS-4250-TX-K9 IDS-4250-SX-K9 IDS-4250-XL-K9
IPS-4240	IPS-4240-K9
IPS-4255	IPS-4255-K9
IPS-4260	IPS-4260-K9
Modules	
AIP-SSM-10	ASA-SSM-AIP-10-K9
AIP-SSM-20	ASA-SSM-AIP-20-K9
IDSM-2	WS-SVC-IDSM2-K9
NM-CIDS	NM-CIDS-K9

The following subsections describe the physical boundary for each TOE representation.

Appliance TOE

The Appliance TOE includes all Cisco IPSv6.0 application code, the resident Linux operating system (Modified Linux version 2.4 kernel) which the Cisco IPSv6.0 application runs upon, and all hardware which the IPS application code and the Linux operating system run upon. The Linux operating system (OS) cannot be installed separately from the Cisco IPSv6.0 application code, and is shipped and installed as one disk image.

An Intel x86 based platform which is encapsulated in a thin one U rack mountable case is the hardware configuration for the Appliance TOE. The Appliance TOE comes with at least three physical interfaces, a serial port, one command and control interface and at least one sensor interface. The command and control interface has an IP address that is used for configuring the appliance. The command and control interface is permanently enabled and mapped to a specific physical interface which depends on the specific model of the appliance. The command and control interface cannot be used as a sensor or TCP reset interface. Sensor interfaces are used to analyze traffic for security violations. Sensor interfaces can operate individually in promiscuous mode or can be paired to create inline interfaces for IPS processing.

The Appliance TOE includes a Modified Linux Version 2.4 kernel as its embedded Operating System (OS). All Subsystems are built atop this OS. The Appliance TOE uses the OS clock to generate timestamps for audit records.

Module TOE

Cisco IDSM-2

The physical scope and boundaries of the Cisco IDSM-2 include the Cisco IPSv6.0 application code, the resident Linux operating system, and the IDSM2 hardware that resides within a Cisco Catalyst 6500 series switch. The switch itself is not included within the TOE physical boundary. The Linux operating system cannot be installed separately from the Cisco IPSv6.0 application code, and is shipped and installed as one disk image.

The Cisco IDSM-2 hardware includes an Intel x86 based module which is installed within a Cisco Catalyst 6500 series switch. The Cisco IDSM-2 comes with five physical interfaces: one command and control interface, two sensor interfaces, one backplane interface, and one TCP reset interface. The command and control interface has an IP address and is used for configuring the appliance. The command and control interface is permanently enabled and mapped to a specific physical interface. The command and control interface cannot be used as a sensing or TCP reset interface. Sensing interfaces are used to analyze traffic for security violations. Sensing interfaces can operate individually in promiscuous mode or can be paired to create inline interfaces for IPS processing. The Cisco IDSM-2 has a specific TCP reset interface because it cannot send TCP resets on its sensor ports.

The Cisco IDSM-2 Module TOE includes a Modified Linux Version 2.4 kernel as its embedded Operating System (OS). All Subsystems are built atop this OS. The Cisco IDSM-2 Module TOE does not contain a hardware clock. It receives time generation from the switch upon which it is installed and then uses the OS clock for keeping the time.

The following are the software and hardware IT Environment requirements for the Cisco IDSM-2:

Catalyst Supervisor Software Requirements:

- Catalyst OS 7.5(1) (minimum)
- Cisco IOS Software Release 12.1(19)E; 12.2(14)SX1, or 12.2.(14)SY (minimum)

Catalyst Supervisor hardware requirements are shown in Table 2-2.

Table 2-2 Catalyst Supervisor Hardware Options with IDSM-2

Supervisor	Catalyst Software	Cisco IOS Software
Supervisor 1A	7.5(1)	-
Supervisor 1A with PFC1	7.5(1)	-
Supervisor 1A with PFC1 or MSFC1	7.5(1)	-

Table 2-2 Catalyst Supervisor Hardware Options with IDSM-2 (continued)

Supervisor	Catalyst Software	Cisco IOS Software
Supervisor 1A-PFC2 or MSFC2	7.5(1)	12.1(19)E1
Supervisor 2 with PFC2	7.5(1)	-
Supervisor 2 with PFC1 or MSFC1	7.5(1)	12.1(19)E, 12.2(14)SY
Supervisor 720 (integrated PFC3 and MSFC3)	-	12.2(14)SX1 or later

Cisco AIP SSM

The physical scope and boundaries of the AIP SSM include the Cisco IPSv6.0 application code, the resident Linux operating system, and the AIP SSM hardware that resides within a Cisco ASA 5500 Series Appliance. The ASA Appliance itself is not included within the TOE physical boundary. The Linux operating system cannot be installed separately from the Cisco IPSv6.0 application code, and is shipped and installed as one disk image. The AIP SSM comes in two models: AIP-SSM-10 and AIP-SSM-20. AIP-SSM-10 supports approximately 100 Mbps throughput and AIP-SSM-20 supports approximately 200 Mbps. Only one module can populate the slot in an ASA Appliance at a time.

The Cisco AIP SSM comes with three physical interfaces, one command and control interface, one backplane interface and one sensor interface. The command and control interface has an IP address and is used for configuring the module. The command and control interface is permanently enabled and mapped to a specific physical interface. The command and control interface cannot be used as a sensor or TCP reset interface. The Sensor interface is used to analyze traffic for security violations. The sensor interface can operate in promiscuous mode or inline mode.

The Cisco AIP SSM includes a Modified Linux Version 2.4 kernel as its embedded Operating System (OS). All Subsystems are built atop this OS. The Cisco AIP SSM does not contain a hardware clock. It receives time generation from the ASA Appliance upon which it is installed and then uses the OS clock for keeping the time.

The following are the software and hardware IT Environment requirements for the AIP SSM:

Cisco ASA Appliance software requirements:

- Cisco Adaptive Security Appliance Software 7.0 or higher

Cisco ASA Appliance hardware requirements:

- Cisco ASA 5500 series adaptive security appliance (ASA)
  - ASA 5510 (AIP-SSM-10)
  - ASA 5520 (AIP-SSM-10 and AIP-SSM-20)
  - ASA 5540 (AIP-SSM-20)

Cisco NM-CIDS

The physical scope and boundaries of the Cisco NM-CIDS include the Cisco IPSv6.0 application code, the resident Linux operating system, and the NM-CIDS hardware that resides within a Cisco router. The router itself is not included within the TOE physical boundary. The Linux operating system cannot be installed separately from the Cisco IPSv6.0 application code, and is shipped and installed as one disk image.

The Cisco NM-CIDS comes with two physical interfaces, one command and control interface, and one sensor interface. The command and control interface has an IP address and is used for configuring the module. The command and control interface is permanently enabled and mapped to a specific physical interface. The command and control interface cannot be used as a sensor or TCP reset interface. The Sensor interface is used to analyze traffic for security violations. The sensor interface can only operate in promiscuous mode.

The Cisco NM-CIDS includes a modified Linux version 2.4 kernel as its embedded Operating System (OS). All Subsystems are built atop this OS. The Cisco NM-CIDS does not contain a hardware clock. It receives time generation from the router upon which it is installed and then uses the OS clock for keeping the time.

The following are the software and hardware IT Environment requirements for the Cisco NM-CIDS:

Cisco Router software requirements:

- Cisco IOS software 12.2(15)ZJ or later
- Cisco IOS software 12.3(4)T or later

Cisco Router hardware requirements:

- Cisco 2600XM Series
- Cisco 2961
- Cisco 3660
- Cisco 3725
- Cisco 3745

TOE Logical Boundary

The TOE consists of a Cisco IPSv6.0 application executing on top of a modified Linux version 2.4 kernel that is shipped and installed as one disk image. All the TOE representations are loaded with the same set of binaries along with a capabilities file. The capabilities file is used to configure what features are available for a particular TOE implementation. At startup, the TOE will determine what hardware platform it is executing on and configure itself according to the specifications in the capabilities file.

In promiscuous mode, the TOE is providing IDS services. The packets do not flow through the TOE but rather the TOE is analyzing a copy of the monitored traffic. The received data is parsed for analysis and compared against known attacks (signatures). The version and revision level of the signatures used to identify known attacks is the same across all TOE representations. The response actions implemented in promiscuous mode are post-event responses and include generating an alarm, logging the alarm event, killing TCP sessions, and/or sending a command to a Cisco router, Cisco switch, or Cisco firewall to block traffic. In inline mode, the TOE is providing IPS services. The packets do flow through the TOE. The TOE performs real-time analysis of the network traffic by looking for anomalies and misuse based on an extensive, embedded signature library and inspection policy rules. When the TOE detects unauthorized activity, the TOE can in addition to the IDS response actions[1], drop the packets preventing the packets from reaching its intended target. In inline mode, a packet normally comes in through the first interface of a pair on the TOE and out the second interface of the pair. The packet is sent to the second interface of the pair unless the packet is being denied or modified by a signature. Note that the AIP SSM only has one sensor interface but can still operate in inline mode.

The TOE can be managed remotely in two ways. The first is via web pages over a TLS/SSL connection. The second is through the Command Line Interface (CLI) over an SSH connection. Telnet is disabled by default and is not allowed in the evaluated configuration. The administrator is only allowed to remotely

[1] TCP resets are not supported in inline mode

administer the TOE via SSH. Note that the local command and control is performed via CLI. The TOE allows authorized users to configure and issue commands on the system based on the users privileges (role).

The Cisco NM-CIDS operates in promiscuous mode (IDS mode) only. All other TOE configurations operate in both promiscuous and inline mode.

The TOE generates security relevant events and system events (alarm events) and stores them to an internal event store. All events written to the event store conform to the Security Device Event Exchange (SDEE) format. The Event Viewer and the IDS Management Center are not included in the TOE. The TOE maintains reliable time which in turn is used to generate a timestamp for all event records.

Unlike the Appliance TOE, the Module TOE evaluates traffic received from their host IT environment (i.e., Catalyst switch, ASA, and/or router). The Cisco ASA Appliance diverts packets to the AIP SSM just before the packet exits the egress interface and after other firewall polices are applied. For example, packets that are blocked by the Cisco ASA Appliance access list are not forwarded to the AIP SSM. For the Cisco IDSM-2, network traffic is either copied to the Cisco IDSM-2 based on security VACLs in the switch or is copied to the Cisco IDSM-2 through the switch's SPAN port feature. The Cisco NM-CIDS processes packets that are forwarded (copied) from selected interfaces on the router to the sensor interface on the Cisco NM-CIDS.

The Module TOE does not contain a hardware clock and therefore must receive initial time from their host IT environment (i.e., Catalyst switch, ASA, or router) via a trusted channel. The Module TOE receives time generated from the host IT environment upon boot-up or when changed by the host IT environment administrator, and then maintains the time locally.

TOE Features Not Evaluated

TOE Features that are outside the scope of the defined TOE Security Functions (TSF) and thus not evaluated are:

- VLAN separation and enforcement of protection features offered by VLANs is not included in this evaluation.

TOE Security Architecture

The following sections provide details about how the security architecture of the TOE for this ST cannot be bypassed, corrupted, or otherwise compromised. An explanation is provided for how each TOE type supports the secure operation of the TSF and where applicable, how the IT environment also supports secure operation of the TSF.

Appliance TOE

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

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

Module TOE

The Module TOE is a hardware plug-in module. The parent chassis of the module (host IT environment) is not part of the Module TOE and is considered to be a remote trusted IT product. The Module TOE and the trusted IT product communicate via a trusted channel that is protected from modification and disclosure. The channel is a registered logical and physical interface that is not visible to the external target network. The trusted channel is used by the Module TOE to receive a time value upon boot up. The trusted IT product can use the trusted channel to change the time on the Module TOE and halt execution of the Module TOE. The Module TOE protects itself from external interference and tampering by untrusted subjects by controlling all its administrative and network interfaces. The module has no general purpose capability or programming interface. The administrative and network interfaces support the flow of packets from the host (switch, ASA, and router) as well as administration of the Module TOE itself. The protection mechanisms employed by the Module 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 TOE will determine which functionality (by role) is presented to the user. The host IT environment administrator can access the TOE to change the time and halt the execution of the module. Because the host IT environment is considered to be a trusted IT entity and the interface established to change the time and halt the module is via a trusted channel, the security domain for the Module TOE is still considered protected from interference and tampering. No other means, other than described, are provided for the user to interact with the Module TOE.

Since the Module TOE component mediates its own interfaces to ensure only authorized communications occur related to the module's ability to perform its functions, and the trusted channel between the Module TOE and the host IT environment is not considered an unauthorized unprotected channel, the Module TOE component operates in a protected and non-bypassable security domain and cannot be compromised.

Security Functions Claimed by the TOE

The TOE's security functions (TSF) summary and the identification of TOE data are described below.

TOE Data

Data in the TOE is categorized as either user data or TSF data. The following sections identify the data included in the TOE.

TSF Data

The TSF data for the TOE are the audit records (security relevant events and system events), signature data, analytical results, capabilities files, time, and user identification and authentication (I&A) credentials.

User Data

The user data for the TOE is network traffic information that is being monitored, analyzed and/ or processed by the TOE.

Security Management

The TOE's security management functions provides security capabilities that guarantees all authorized users are required to identify and authenticate to the TOE before any administrative actions can be performed. Thus, an authorized user is one who has been successfully identified and authenticated by the TOE. The TOE provides administrator support functionality that enables a human user to manage and configure the TOE. The TOE manages roles for authorized users to ensure restricted access to the security functions and data for the TOE.

Audit

The TOE's Audit security function supports audit record generation, storage, and review. The TOE maintains time to generate a reliable timestamp which is applied to each audit event record. Note that the Module TOE must receive an initial time from its host IT environment via a trusted channel to set its internal clock. Audit capabilities of the TOE include selective audit review by authorized users, audit storage, and protection of audit records from unauthorized deletion. Note that "Audit Trail", "Audit Events", "Audit Trail Data", "Audit Data", "Audit Records", and "event data" are used interchangeably to refer to the Audit records defined as TSF data.

Network Traffic Sensing and Analysis

The TOE monitors network traffic from the target IT network. The TOE collects and stores information about all events that are indicative of inappropriate activity. Received data is parsed for analysis and compared against known attacks. The TOE utilizes advance methods for the inspection and analysis of traffic to include event correlation, risk rating calculation, and threat identification (e.g., protocol analysis, pattern recognition, anomaly detection). Based on the analytical result, the TOE has several options for reaction (depending on the interface mode) that include generating an alarm, logging the alarm event, dropping or modifying packets, sending a command to a Cisco router, switch, or firewall to block traffic specific offending network traffic, or killing TCP sessions.

Identification and Authentication

The TOE Identification and Authentication function requires users to provide credentials to the TOE in order to successfully be recognized as an authorized user. The user identifies and authenticates themselves through both the command line interface (CLI) and the Web interface using SSH and TLS/SSL respectively. Note that through the CLI interface, the user can also authenticate via RSA authentication. In the case of the physical console interface the user is directly allowed to provide a username and password to the TOE. The TOE maintains and stores user identity, authentication data, and authorizations in the underlying operating system.

TOE Evaluated Configuration

The TOE's evaluated configuration requires:

1. Cisco 4200 Series Sensor Appliance

OR

1. Cisco IDSM-2
2. Host IT environment (Cisco Catalyst Switch)

OR

1. Cisco AIP SSM
2. Host IT environment (Cisco ASA Appliance)
3. DES or 3 DES enabled

OR

1. Cisco NM-CIDS
2. Host IT environment (Cisco Router)

The software version "6.0(1)E1" is the evaluated version and is an internal version that maps to IPSv 6.0.

Note that the Cisco router, switch and ASA Appliance functionalities provided by the host IT environments are outside the scope of the TOE Security Functions and are therefore not evaluated.

CHAPTER 3

Security Environment

This chapter identifies the following:

- Significant assumptions about the TOE's operational environment.
- IT related threats to the organization countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.
- Organizational security policies for the TOE as appropriate.

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

Assumptions

The specific conditions listed in Table 3-1 are assumed to exist in the TOE's IT environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 3-1 TOE Assumptions

Name	Assumption
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.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

Table 3-1 TOE Assumptions (continued)

Name	Assumption
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.

Threats

Table 3-2 and Table 3-3 list the threats addressed by the TOE. The following are threats identified for the TOE and the IT System the TOE monitors. The assumed level of expertise of the attacker for all the threats is unsophisticated.

TOE Threats

Table 3-2 TOE Threats

Threat Name	Threat Definition
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.
T.PRIVIL	An unauthorized use 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.

Table 3-2 TOE Threats (continued)

Threat Name	Threat Definition
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.

IT System Threats

Table 3-3 Threats to the IT System

Threat Name	Threat Definition
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.

Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. Table 3-4 identifies the organizational security policies applicable to the TOE.

Table 3-4 Organizational Security Policies

Policy Name	Policy Definition
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.

CHAPTER 4

Security Objectives

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

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

Security Objectives for the TOE

Table 4-1 identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 4-1 Security Objectives for the TOE

Name	TOE Security Objective
O.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
O.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 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.

Table 4-1 Security Objectives for the TOE (continued)

Name	TOE Security Objective
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.

Security Objectives for the Environment

The assumptions identified in Assumptions, page 3-1 are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. Table 4-2 identifies the security objectives for the environment. Note the OE. convention varies from the PP but does not change the actual wording of the PP Environment Objectives.

Table 4-2 Security Objectives for the Environment

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

CHAPTER 5

Security Requirements

This section identifies the Security Functional Requirements for the TOE and for the IT Environment. The Security Functional Requirements included in this section are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 2.3.*

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

- Assignments: indicated by showing the value bolded in square brackets [**Assignment_value**].
- Selections: indicated by underlined text.
- Assignments within selections: indicated in italics and underlined text.
- Refinements: indicated in **bold text** with the addition of details and ~~**bold text**~~ when details are deleted.

Multiple Security Functional Requirement instances (iterations) are identified by the Security Functional Requirement component identification followed by the instance number in parenthesis (e.g. FTP_ITC.1(1)) and the Security Functional Requirement element name followed by the instance number in parenthesis (e.g. FTP_ITC.1.1(1)). This document continues the iteration numbering for Security Functional Requirements that apply to both the TOE and the IT Environment.

Explicitly stated SFRs are identified by having a label (EXP) meaning 'Explicit Stated SFR for the TOE' after the requirement name for TOE SFRs. Because the explicit IDS requirements are transcribed from the PP, the conventions are applied accordingly.

TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in Table 5-1 are described in more detail in the following subsections.

Table 5-1 TOE Security Functional Requirements

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

Table 5-1 TOE Security Functional Requirements (continued)

ID	Functional Component	ST Operations
FAU_SAR.3	Selectable audit review	Selection, assignment
FAU_SEL.1	Selective audit	Selection, assignment
FAU_STG.2	Guarantees of audit data availability	Selection, assignment, selection
FAU_STG.4	Prevention of audit data loss	Selection, assignment
FCS_CKM.1	Cryptographic Key Generation	Assignment, assignment, assignment
FCS_CKM.4	Cryptographic Key Destruction	Assignment, assignment
FCS_COP.1(1)	Cryptographic Operation - SSH	Assignment, assignment, assignment, assignment
FCS_COP.1(2)	Cryptographic Operation-SSL	Assignment, assignment, assignment, assignment
FIA_UAU.1	Timing of authentication	Assignment
FIA_ATD.1	User attribute definition	Assignment
FIA_UID.1	Timing of identification	Selection, assignment, assignment
FMT_MOF.1	Management of security functions behavior	Assignment
FMT_MSA.2	Secure security attributes	None
FMT_MTD.1	Management of TSF data	Selection, assignment, assignment, assignment
FMT_SMR.1	Security roles	Assignment
FMT_SMF.1	Specification of Management Functions	Assignment
FPT_RVM .1(1)	Non-bypassability of the TSP	None
FPT_SEP.1(1)	TSF domain separation	None
FPT_STM.1(1)	Reliable time stamps	None
FTP_ITC.1(1)	Inter-TSF trusted channel	Selection, assignment
FTP_ITC.1(2)	Inter-TSF trusted channel	Selection, assignment
FTP_RTC.1 (EXP)	Remote administration trusted channel	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

Security Audit (FAU)

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]**.

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 ST, [the additional information specified in the Details column of Table 5-2 Auditable Events].

Table 5-2 Auditable Events

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	

Table 5-2 Auditable Events (continued)

Component	Event	Details
FMT_MTD.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
FTP_ITC.1(1)	All attempted uses of the trusted channel functions	Initiator and target identifier
FTP_ITC.1(2)	All attempted uses of the trusted channel functions	Initiator and target identifier

FAU_SAR.1: Audit review

FAU_SAR.1.1

The TSF shall provide [**authorized Administrators and authorized System administrators**] 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.

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.

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.**]

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**].

FAU_STG.2: Guarantees of audit data availability

FAU_STG.2.1

The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.2.2

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

FAU_STG.2.3

The TSF shall ensure that [**the most recent, limited by available storage space**] audit records will be maintained when the following conditions occur: audit storage exhaustion.

FAU_STG.4: Prevention of audit data loss

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

Cryptographic Support (FCS)

FCS_CKM.1: Cryptographic key generation

FCS_CKM.1.1

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

Application note: This SFR support key generation for both SSH and TLS/SSL.

FCS_CKM.4: Cryptographic key destruction

FCS_CKM.4.1

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

Application note: This SFR support key destruction for both SSH and TLS/SSL.

FCS_COP.1(1): Cryptographic operation - SSH

FCS_COP.1.1(1)

The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [3DES] and cryptographic key sizes [168 bits] that meet the following: [FIPS 46-3].

FCS_COP.1(2): Cryptographic operation - SSL

FCS_COP.1.1(2)

The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [3DES-EDE-CBC] and cryptographic key sizes [168 bits] that meet the following: [FIPS 46-3].

Identification and Authentication (FIA)

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.

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**].

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 identification data b) For the CLI Interface: The SSH handshake to be performed, input of identification data or in the case of the physical console interface, input of identification 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.

Security Management (FMT)

FMT_MOF.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**].

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 [**authorized System administrators; and authorized administrators who can only query all other TOE data**].

FMT_MSA.2: Secure security attributes

FMT_MSA.2.1

The TSF shall ensure that only secure values are accepted for security attributes.

FMT_SMR.1: Security roles

FMT_SMR.1.1

The TSF shall maintain the **following** roles [**authorized administrator, and authorized System administrators**].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

FMT_SMF.1: Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions:

a. [**the ability to modify behavior of System data collection, analysis and reaction; and**
b. **the ability to query and add System and audit data; and**
c. **the ability to query and modify all other TOE data**].

Protection of the TOE Security Functions (FPT)

FPT_RVM.1(1): Non-bypassability of the TSP

FPT_RVM.1.1(1)

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

FPT_SEP.1(1): TSF domain separation

FPT_SEP.1.1(1)

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

FPT_SEP.1.2(1)

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

FPT_STM.1(1): Reliable Time Stamps

FPT_STM.1.1(1)

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

Trusted Path/ Channels (FTP)

FTP_ITC.1(1): Inter-TSF trusted channel

FTP_ITC.1.1(1)

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

FTP_ITC.1.2(1)

The TSF shall permit TSF to initiate communication via the trusted channel.

FTP_ITC.1.3(1)

The TSF shall initiate communication via the trusted channel for [**signature updates**].

Application note: Signature updates are transmitted outbound using SCP over SSH or TLS/SSL via HTTPS.

FTP_ITC.1(2): Inter-TSF trusted channel

FTP_ITC.1.1(2)

The **Module** TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

FTP_ITC.1.2(2)

The **Module** TSF shall permit <u>the remote trusted IT product</u> to initiate communication via the trusted channel **to set clock and halt execution**.

FTP_ITC.1.3(2)

The **Module** TSF shall initiate communication via the trusted channel for [**clock settings from the remote trusted IT product upon start-up and reboot**].

Application note: Depending on the module, the remote trusted IT product is either the Catalyst switch, ASA appliance, or Cisco router.

FTP_RTC.1: Remote administration trusted channel (EXP)

FTP_RTC.1.1

The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

FTP_RTC.1.2

The TSF shall permit <u>the remote trusted IT product</u> to initiate communication via the trusted channel.

FTP_RTC.1.3

The TSF shall use a trusted channel for the following functions: secure remote administration.

Application note: Secure remote administration is provided by SSH and TLS/SSL.

IDS Component Requirements (IDS)

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. <u>Network Traffic</u>; and

b. [**No additional events**].

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 5-3 System Events**.**

Table 5-3 System Events

Component	Event	Details
IDS_SDC.1	Network traffic	Protocol, source address, destination address

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; and

b. [**Event correlation**].

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; and

b. [**Risk rating**].

IDS_RCT.1: Analyzer react (EXP)

IDS_RCT.1.1

The System shall send an alarm to [**The Event Store**] and take [**the following actions:**

a. In promiscuous mode: Send an alarm, and/or perform a TCP reset and/or send a command to: a Cisco router, Cisco switch, or ASA firewall to block traffic, and/or create an event

OR

b. In inline mode: Send an alarm, configure an ACL to block attacker, drop and/or modify packets, and/or create an event]

when an intrusion is detected.

Application Note: The NM-CIDS module TOE does not operate in inline mode.

IDS_RDR.1: Restricted data review (EXP)

IDS_RDR.1.1

The System shall provide [**authorized System administrators and authorized administrators**] with the capability to read [**Event data**] from the System data**.**

IDS_RDR.1.2

The System shall provide the System data in a manner suitable for the user to interpret the information.

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.

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

IDS_STG.1.1

The System shall protect the stored System data from unauthorized deletion.

IDS_STG.1.2

The System shall protect the stored System data from modification.

IDS_STG.1.3

The System shall ensure that [**the most recent, limited by available storage space**] System data will be maintained when the following conditions occur: System data storage exhaustion.

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.

TOE Security Assurance Requirements

The TOE security assurance requirements listed in Table 5-4 are drawn from Part 3 of the CC. They identify the management and evaluative activities required to address the threats and policies identified in Security Environment, page 3-1 of this ST. This ST complies with assurance level EAL2 augmented with ALC_FLR.1 (Basic Flaw Remediation).

Table 5-4 TOE Assurance Requirements

Assurance Class	Component ID	Component Description
Configuration Management	ACM_CAP.2	Configuration Items
Delivery and Operation	ADO_DEL.1	Delivery Procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal Functional Specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User Guidance
Life cycle support	ALC_FLR.1	Basic Flaw Remediation
Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

SFRs With SOF Declarations

The claimed minimum strength of function for the TOE is SOF-basic. SOF-basic is claimed as a specific strength of function metric for the FIA_UAU.1 password authentication mechanism.

Security Requirements for the IT Environment

The following functional requirements are met by the IT Environment of the module TOE.

ID	Functional Component	Dependencies	ST Operations
FPT_RVM .1(2)	Non-bypassability of the TSP	None	Refinement
FPT_SEP.1(2)	TSF domain separation	None	Refinement
FPT_STM.1(2)	Reliable time stamps	None	Refinement

FPT_RVM.1(2): Non-bypassability of the TSP

FPT_RVM.1.1(2)

The IT Environment shall ensure that module TOE enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1(2): TSF domain separation

FPT_SEP.1.1(2)

The **IT Environment** shall maintain a security domain for its own execution that protects it **and the module TOE** from interference and tampering by untrusted subjects.

FPT_SEP.1.2(2)

The **IT Environment** shall enforce separation between the security domains of subjects in the TSC.

FPT_STM.1(2): Reliable Time Stamps

FPT_STM.1.1(2)

The **IT Environment** shall be able to provide reliable time stamps for **module TOE** use.

CHAPTER 6

TOE Summary Specification

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

TOE Security Functions

Audit

Functional Requirements satisfied: FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, IDS_RDR.1, FAU_SEL.1, FAU_STG.2, FAU_STG.4, IDS_STG.1, IDS_STG.2, FPT_STM.1

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.

The Audit function generates audit records containing all information described in Table 6-1.

Table 6-1 presents a mapping of Events defined in Table 5-2 and Table 5-3 (Network Traffic) to the TOE defined event types. An event type consists of a set of events. An event is identified under one event type. No event overlaps into two or more event types. The following TOE defined event types are:

- **evAlert**

  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.

- **evError**

  Display error events. Error events are generated by services when error conditions are encountered. EvError is further divided into levels: warning, error, and fatal.

- **evStatus**

  Display status 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 of the transaction.

The Audit function provides a pre-selection capability allowing authorized users to select events to be audited by event types. This means that the authorized user could include or exclude the generation of a set of auditable events by selecting an event type. The TOE only supports pre-selection for evError and evStatus event types. For example if the evStatus event type were excluded, then all events associated with evStatus would not be audited. Some events listed in Table 6-1 are mapped to both evStatus and evError. This means that the failures for the events are captured as evError records and the others are evStatus records. Turning off one event type does not affect the generation of another event type. The Audit function also provides a pre-selection capability for the levels of evError. This means the authorized user can specify to include or exclude evError event types at the warning, error, or fatal level.

Table 6-1 Auditable Event Categories

Component	Event [1]	Details	IPSv6.0 Event Type
FAU_GEN.1	Start-up and shutdown of audit functions		evStatus evError
FAU_GEN.1	Access to System		evStatus evError
FAU_GEN.1	Access to the TOE and System data	**Object IDS, Requested access**	evStatus
FAU_SAR.1	Reading of information from the audit records		evStatus
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		evStatus
FIA_UAU.1	All use of the authentication mechanism	**User identity, location**	evStatus, evError
FIA_UID.1	All use of the user identification mechanism	**User identity, location**	evStatus, evError
FMT_MOF.1	All modifications in the behavior of the functions of the TSF		evStatus
FMT_MTD.1	All modifications to the values of TSF data		evStatus
FMT_SMR.1	Modifications to the group of users that are part of a role	**User identity**	evStatus
FTP_ITC.1(1)	All attempted uses of the trusted channel functions	**Initiator and target identifier**	evStatus
FTP_ITC.1(2)	All attempted uses of the trusted channel functions	**Initiator and target identifier**	evStatus
IDS_SDC.1	Network Traffic	**Protocol, source address, destination address**	evAlert

[1] The Event column identifies auditable events as defined by FAU_GEN.1 in this ST and should not be confused with IPS events.

By default, all IDS signatures trigger an evAlert 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 Extensible Markup Language (XML) format and can be viewed via the Web Interface and the CLI Interface.

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, initiator and target identifier, and requested access. Because the events captured must have a reliable timestamp, the TOE maintains its own internal clock. For the Module TOE, a time value is received from the host IT environment to initialize the TOE's internal clock as part of boot up. The Module TOE then maintains the time until the next reboot when a new time value is received. Note, the host IT environment administrator has the ability to change the time on the Module TOE.

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 authenticating is the user allowed to view audit records; and this is the only way by which users can view audit records. Only an 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.

The TOE's Web Interface 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. .

The Audit function 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.

In the event of audit storage exhaustion (that is, when the event store becomes full) the number of records saved will be the the most recent audit events stored in the event store limited by the storage space allocated to the event store. 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. When the event store's capacity is reached, the TOE overwrites the oldest stored audit records and sends 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.

Identification and Authentication

Functional Requirements: FIA_UAU.1, FIA_ATD.1, FIA_UID.1

Strength of Function Claim: SOF-basic for the probabilistic permutational password authentication mechanism.

The Identification and Authentication function requires users to provide credentials to the TOE in order to successfully be recognized as an authorized user. Thus, an authorized user is one who has been successfully identified and authenticated by the TOE. Authorized users can include Administrators, Operators and Viewers. Administrator and Operator groups correspond to the authorized System administrator role and the Viewer group corresponds to the authorized administrator role as defined in FMT_SMR.1. Further explanation of the authorized user role is provided in Security Management, page 6-4 of this ST. 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 I&A credentials to the TOE.

In the case of the console interface, the user is prompted to login, and allowed to enter I&A credentials. 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 I&A credentials. Note that through this interface a user can also authenticate via Rivest, Shamir and Adleman (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 Server Interface, the user performs the TLS protocol handshake, is prompted with a login pop up window, and is allowed to enter I&A credentials.

The TOE maintains user identity, authentication data (I&A credentials), 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 Identification and Authentication function stores the users associated role, 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.

Security Management

Functional Requirements: FMT_MOF.1, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1

The protection mechanisms within the TOE provide assurance that only authorized users 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 interface 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 also 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.

Only an administrator has sufficient privileges to query and add system and audit data. The Operator role only has sufficient privileges to query and modify data generated by the TOE from the targeted IT network, as well as query audit data. The Viewer role only has sufficient privileges to query data generated by the TOE from the targeted IT network, as well as query audit data.

The evaluated configuration of the TOE maintains three groups of authorized users[1]. All users are assigned to one of these defined groups. In descending privilege level, these groups are:

- Administrator – have unrestricted view access and can perform the following functions: add users and assign passwords, enable and disable control of physical interfaces and virtual sensors, modify sensor address configuration, tune signatures, clear the event store, set the clock, and assign configuration to a virtual sensor,
- Operator – have unrestricted view access and can perform the following functions: modify their passwords, tune signatures, assign configuration to a virtual sensor, and
- Viewer – can view configuration and event data and can modify their passwords.

With respect to the IDS System PP, The Administrator and Operator groups correspond to the authorized System administrator role and the Viewer group corresponds to the authorized administrator role. 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 in the evaluated configuration and is not used for meeting any of the requirements, in this ST. Its purpose is for trouble shooting of the TOE. Any use of the service account will take the TOE out of the evaluated configuration.

Network Traffic Analysis

Functional Requirements: IDS_SDC.1, IDS_ANL.1, IDS_RCT.1

The Network Traffic Analysis function provides the capability of the TOE to collect and analyze data. This includes system data collection and the operations of analysis performed on network traffic. In addition the Network Traffic Analysis function responds to an attack as configured by the administrator.

The TOE is a network based Intrusion Detection and Prevention System that scans network traffic. The Network Traffic Analysis function is used to collect and analyze 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 risk rating, IP and port address of the event (both source and destination), protocol type, and data associated with the event. The risk rating is used to indicate the relative risk of the traffic or offending host continuing to access the IT network. This rating can be used either to illuminate the events that require immediate administrator attention in promiscuous mode (IDS) or to provide a means for developing risk-oriented event action policies when the TOE is employed in the inline mode (IPS). The risk rating is an integer value in the range from 0 to 100. The higher the value, the greater the security risk of the trigger event for the associated alert.

The Network Traffic Analysis function applies a signature analysis method, different threat identification methods, and event correlation to analyze network traffic. For signature analysis method, 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 (Table 6-2) summarizes examples of specific attacks the TOE attempts to defend against.

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

Table 6-2 Attack Examples

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

Threat Identification Methods include stateful pattern recognition to identify vulnerability-based attacks through the use of mulipacket inspection across all protocols; protocol analysis to provide protocol decoding and validation for network traffic; traffic and protocol anomaly detection that identify attacks based on observed deviations from normal traffic or protocol behavior; Layer 2 detection; anti-IPS evasion techniques to provide traffic normalization, IP defragmentation, TCP stream reassembly, and deobfuscation. The Threat Identification Methods used by the Network Traffic Analysis function is dependent on whether the interface examined is configured for IPS or IDS services.

The Network Traffic Analysis function provides the Meta Event Generator to correctly classify malicious activity detected by the TOE by event correlation. Event correlation addresses those types of attacks that set off multiple low severity alarms which together results into a single event at a higher severity level. Classification of malicious activity is accomplished through:

- correlation of alarms pertaining to worms that exploit multiple vulnerabilities,
- correlation of a sequence of actions that lead up to worm infestation,
- correlation of multiple event at low severity level to result in a single event of higher severity, and
- enhancement of alarm fidelity through simultaneous triggers based on hybrid detection algorithms.

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.

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 in promiscuous mode (IDS), 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 ASA firewall to block specific offending network traffic. In inline mode, the TOE can block and/or modify the traffic (e.g., defragmentation, TCP stream reassembly).

Self-protection

Functional Requirements: FPT_STM.1(1), FPT_RVM.1(1), FPT_SEP.1(1), FTP_ITC.1(1), FTP_ITC.1(2), FTP_RTC.1, FCS_CKM.1, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FMT_MSA.2

To receive a reliable time source from a remote trusted IT product, the Module TOE and host IT environment communicate via an internal configuration protocol through a registered logical and physical interface (slot id, processor id, MAC address) that is not exposed to the external target network.

To receive signature updates the TOE communicates via an outbound connection only. It is used to retrieve attack signature updates from Cisco. An administrator must manually configure the TOE to connect to a specified server to retrieve updates. The TOE will then make an outbound connection to the specified server. This connection can use FTP, HTTP, SCP, or HTTPS. However in the evaluated configuration only HTTPS or SCP must be allowed. Secure Copy (scp) utilizes the ssh functionality of the TOE to ensure confidentiality and integrity of data transmitted. Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) utilizes the TLS/SSL functionality (implemented in the Secure Web Server) of the TOE to ensure confidentiality and integrity of data transmitted.

The TOE can be managed remotely in two ways. The first is via web pages over a TLS/SSL connection. The second is through the Command Line Interface (CLI) over an SSH connection. Telnet is disabled by default and is not allowed in the evaluated configuration. The administrator is only allowed to remotely administer the TOE via SSH. The TOE only accepts valid parameter values for the configuration of TLS/SSL and SSH.

The TOE implements TLSv1.0/SSLv3.0 using RSA key exchange, 3DES-EDE-CBC encryption, and SHA digest algorithm. The TOE implements a Cisco modified SSHv1.5 using RSA key generation and 3DES data encryption algorithm. The TOE overwrites (zeroizes) key values for key destruction. The cryptography used by the TOE has not been FIPS certified nor has it been analyzed or tested to conform to cryptographic standards as part of this evaluation. All cryptography has been asserted as tested by Cisco.

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 via the CLI or Web interface, the Identification and Authentication is used to query and return the user's role. The role is used to determine what functionality is presented to the user. For the Module TOE, the host IT environment administrator can access the TOE to change the time and halt the execution of the module. Because the host IT environment is considered to be a trusted IT entity and the interface established to change the time and halt the module is via a trusted channel, the security domain for the Module TOE is still considered protected from interference and tampering. No other means, other than described above, are provided for the user to interact with the TOE.

The Self-protection function is responsible for providing an execution domain that is protected from interference and tampering by unauthorized users. The TOE is a hardware device that executes all of its processes internally. It is accessible only via the defined interfaces and only authorized users and the host IT environment for the Module TOEs are able to modify the functionality of the TOE. The sensor 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 users. At all physical interfaces, the TOE intercedes to ensure domain separation. Traffic can only come into the TOE via three physical interfaces: the Serial Port (which is used only during initial setup and configuration of the TOE), the command and control interface (access to which is controlled by a username and a password), or the sensor interface (where the traffic is monitored and analyzed by the TOE but no actions can be executed). 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.

The self protection function of the Module TOE and the self protection features of the host IT environment work together to satisfy the self protection requirements. The reliable time value is received upon boot up or modified via a trusted channel from the host IT Environment. The host IT Environment mediates its interfaces to only allowed authorized modifications while protecting those interfaces from interference and tampering. Once the clock is initialized or modified via the trusted channel, the Module TOE maintains the time to produce a reliable timestamp for audit records. The Module TOE component mediates its own interfaces to ensure only authorized communications occur related to the module's ability to perform its functions, and the trusted channel between the Module TOE and the host IT environment is considered a protected channel.

Assurance Measures

The TOE was developed with security Assurance measures in place that constitute Common Criteria EAL2 level of assurance augmented with ALC_FLR.1. These are identified in Table 6-3.

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. The justification is provided to ensure that the documentation listed meets the specific assurance requirement.

Table 6-3 Assurance Measures

Assurance Class	Assurance Components	Cisco IPSv6.0 Assurance Measures	Justification
Configuration Management	ACM_CAP.2	Cisco Intrusion Prevention System (IPS) Version 6.0 Configuration Management and Flaw Remediation Documentation, Version 6.0	This document described the processes and procedures that define how configuration management will be maintained at the development facility.
Delivery and Operation	ADO_DEL.1	Cisco Intrusion Prevention System (IPS) Version 6.0 Delivery Documentation, Version 1.0	This document describes how the TOE is securely delivered to customers.
	ADO_IGS.1	Release Notes for Cisco Intrusion Prevention System 6.0 Cisco Intrusion Prevention System (IPS) Version 6.0 Installation, Generation and Start-up Documentation, Version 5.0 Installing and Using Cisco Intrusion Prevention System Device Manager 6.0	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.

Table 6-3 Assurance Measures (continued)

Assurance Class	Assurance Components	Cisco IPSv6.0 Assurance Measures	Justification
Development	ADV_FSP.1	Cisco Intrusion Prevention System (IPS) Version 6.0 Functional Specification Documentation, Version 7.0	This document describes the security functions and externally visible interfaces.
	ADV_HLD.1	Cisco Intrusion Prevention System (IPS) Version 6.0 High Level Design Documentation, Version 6.0	This document describes the subsystem interfaces and subsystems.
	ADV_RCR.1	Cisco Intrusion Prevention System (IPS) Version 6.0 Representation Correspondence, Version 6.0	This document demonstrates the mapping of functionality to meet the requirements through all of the design documentation.
Guidance Documents	AGD_ADM.1	Release Notes for Cisco Intrusion Prevention System 6.0 Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 6.0 Command Reference for Cisco Intrusion Prevention System 6.0 Installing and Using Cisco Intrusion Prevention System Device Manager 6.0 Cisco Intrusion Prevention System (IPS) Version 6.0 Administrator Guide, Version 6.0	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.
	AGD_USR.1	No user guidance is provided by the TOE as there are no non-administrative user (PD-0106)	Not Applicable
Life Cycle Support	ALC_FLR.1	Cisco Intrusion Prevention System (IPS) Version 6.0 Configuration Management and Flaw Remediation Documentation, Version 5.0	This document describes flaw remediation procedures.

Table 6-3 Assurance Measures (continued)

Assurance Class	Assurance Components	Cisco IPSv6.0 Assurance Measures	Justification
Tests	ATE_COV.1	Cisco Intrusion Prevention System (IPS) Version 6.0 Test Coverage, Version 5.0 Nubra Master Test Plan.doc (EDCS-470870) Nubra_CLI_Enhancements_Detailed_Test_Plan.doc (EDCS-490612) Nubra_Regression_Authentication_Test_Plan.doc (EDCS-486899) Nubra_Regression_Event_Actions.doc (EDCS- 487525) Nubra_Regression_Signature_Engines_Test_Plan.doc (EDCS-476853) Nubra_Regression_SSM_F1_Interoperability_Test_Plan.doc (EDCS-477946) Nubra_Regression_IDSM2_IOS_Interoperability_Test_Plan.doc (EDCS-477942)	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.

Table 6-3 Assurance Measures (continued)

Assurance Class	Assurance Components	Cisco IPSv6.0 Assurance Measures	Justification
Tests (continued)	ATE_FUN.1	Cisco Intrusion Prevention System (IPS) Version 6.0 Test Coverage, Version 5.0	This document describes the functional test plan and functional tests performed by the developer of the TOE.
		Nubra Master Test Plan.doc (EDCS-470870) Nubra_CLI_Enhancements_Detailed_Test_Plan.doc (EDCS-490612) Nubra_Regression_Authentication_Test_Plan.doc (EDCS-486899) Nubra_Regression_Event_Actions.doc (EDCS- 487525) Nubra_Regression_Signature_Engines_Test_Plan.doc (EDCS-476853) Nubra_Regression_SSM_F1_Interoperability_Test_Plan.doc (EDCS-477946) Nubra_Regression_IDSM2_IOS_Interoperability_Test_Plan.doc (EDCS-477942) EDCS_476853_Results.xls EDCS_477946_Results.xls EDCS_486899_Results.xls EDCS_487525_Results.xls EDCS_490612_Results.xls EDCS_477942_Results.xls	These document describes a system level detailed test plan, procedures and results.

Table 6-3 Assurance Measures (continued)

Assurance Class	Assurance Components	Cisco IPSv6.0 Assurance Measures	Justification
Tests (continued)	ATE_IND.2	Cisco Intrusion Prevention System (IPS) Version 6.0 Test Coverage, Version 5.0 Nubra Master Test Plan.doc (EDCS-470870) Nubra_CLI_Enhancements_Detailed_Test_Plan.doc (EDCS-490612) Nubra_Regression_Authentication_Test_Plan.doc (EDCS-486899) Nubra_Regression_Event_Actions.doc (EDCS- 487525) Nubra_Regression_Signature_Engines_Test_Plan.doc (EDCS-476853) Nubra_Regression_SSM_F1_Interoperability_Test_Plan.doc (EDCS-477946) Nubra_Regression_IDSM2_IOS_Interoperability_Test_Plan.doc (EDCS-477942) EDCS_476853_Results.xls EDCS_477946_Results.xls EDCS_486899_Results.xls EDCS_487525_Results.xls EDCS_490612_Results.xls EDCS_477942_Results.xls	This document describes the functional test plan and functional tests performed by the developer of the TOE.
Vulnerability Assessment	AVA_SOF.1	Cisco Intrusion Prevention System (IPS) Version 6.0 Strength of Function Version 5.0	This document provides an analysis of the probabilistic or permutational mechanisms in the TOE.
	AVA_VLA.1	Cisco Intrusion Prevention System (IPS) Version 6.0 Vulnerability Analysis, Version 6.0	This document addresses whether vulnerabilities identified could allow users to violate the TSP.

CHAPTER 7

Protection Profile Claims

This section provides PP conformance claims.

PP Conformance

The TOE conforms to the following PP:

Intrusion Detection System System Protection Profile Version 1.6, dated April 4, 2006. Security level EAL2.

The PP listed above requires TOEs claiming compliance to the PP to have "one or more sensors and/ or scanners". The IPSv6.0 TOE for this ST does not include scanner functionality. Since this ST does not claim scanning as part of TOE functionality, all of the threats and objectives from the PP that would correspond to that functionality are not claimed in the ST. This includes all items in Table 7-1 and the additional item described below the table.

Table 7-1 PP Threats and Objectives not Included in the ST

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.
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.

Additionally, O.IDANLZ was edited to remove "or IDS Scanners" from the definition.

- O.IDANLZ

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

FAU_STG.2 was transcribed per CCv2.3, and the operations were completed to maintain the integrity and intent of the requirement as stated in the PP.

PP Tailoring

All the security environment, security objectives, and IT requirements described in the PP have been incorporated into this ST except for the security objective and the following SFRs: FPT_ITA.1, FPT_ITC.1, FPT_ITI.1 and FIA_AFL.1. The objective and requirements were not included because the TOE is not a distributed TOE and is not communicating with other IDS components and because of PD-0097. PD-0097 (http://niap.nist.gov/cc-scheme/PD/0097.html) states that the inter-TOE SFRs (FPT FPT_ITA.1, FPT_ITC.1, FPT_ITI.1) were incorrectly included in the IDS system PP. PD-0097 also states that O.EXPORT objective was erroneously replicated in the IDS system PP. In addition, PD-0097 goes on to say that FIA_AFL.1 was incorrectly included in the system PP. PD-0097 does note that FPT_ITT.1 should be included in the ST if the TOE is a distributed TOE. The TOE described in this ST is not a distributed TOE. Although PD-0097 was originally written for the IDS System PP version 1.4, the difference between IDS System PP version 1.6 and version 1.4 is the errata sheet that is included in version 1.6. Therefore, the decision from PD-0097 for excluding these requirements and objective from an ST still applies when conforming to the IDS System PP version 1.6.

The uncompleted operations in the PP were completed in this ST to further qualify the PP requirements. The operations performed do not change the spirit and intent of the requirement but rather describes TOE implementation details.

The effected IT requirements are as follows:

FAU_GEN.1, FAU_SAR.1, FAU_STG.2, FAU_STG.4, FIA_UAU.1, FIA_UID.1, FMT_MTD.1, FMT_SMF.1, IDS_SDC.1, IDS_ANL.1, IDS_RCT.1, IDS_RDR.1, IDS_STG.1, and IDS_STG.2.

Because the module TOE is considered to be a software implementation, the PP Errata Sheets are applied to iterate the following requirements on the IT environment for the module TOE only: FPT_STM.1, FPT_SEP.1 and FPT_RVM.1. The following objectives were added to allow the addition of IT environment requirements: OE.TIME and OE.PROTECT.

PP Additions

There are no additional Security environment details or security objectives presented in this ST other than those in the PP. However, FTP_ITC.1(1), FTP_ITC.1(2) and FTP_RTC.1, FCS_CKM.1, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), and FMT_MSA.2 were added to the ST. FTP_ITC.1(1) was added to require that signature updates for the TOE are provided via a trusted channel. Since signature data is considered TSF data, the TOE must be able to protect it. Because it is necessary for the Module TOE to receive initial time settings from the host IT environment, and to ensure protection of the TOE's execution domain, FTP_ITC.1(2) was added. Since time is considered TSF data the TOE must be able to protect it. The TSF initiates the trusted channel which provides identification of end points as well as protection of data traveling through the channel. Because the Catalyst switch, ASA Appliance, and router are considered to be remote trusted IT products, communicating over a trusted channel, the execution domain of the TOE is not considered to be compromised by an untrusted subject. This requirement was added in support of the O.PROTCT objective. FTP_RTC.1 was added to address remote administration via a protected channel. The FCS requirements specify the crypto requirements for SSH and TLS/SSL, the two forms of protected communications offered by the TOE for remote administration. FMT_MSA.2 is included to ensure valid parameter values are used to properly implement SSH and TLS/SSL protocols.

FMT_SMF.1 was added to satisfy the dependencies of FMT_MTD.1 and FMT_MOF.1. FMT_SMF.1 was introduced in CC version 2.2 and remains in CC version 2.3.

CHAPTER 8

Rationale

Security Objectives Rationale

This section demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat and assumption is addressed by a security objective. Table 8-1 andTable 8-2 provide the mapping and rationale for the security objectives identified in Chapter 4 and the assumptions, threats and policies identified in Chapter 3.

Table 8-1 Threats, Assumptions, and Policies to Security Objectives Mapping

	O. PROTCT	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME	OE.PROTECT
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							X
T.COMDIS	X					X	X										X
T.LOSSOF	X					X	X			X							
T.NOHALT		X	X			X	X										
T.PRIVIL	X					X	X										
T.IMPCON					X	X	X				X						
T.INFLUX								X									
T.FACCNT									X								
T.FALACT				X													

Table 8-1 ***Threats, Assumptions, and Policies to Security Objectives Mapping (continued)***

	O. PROTCT	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	OE.INSTAL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTROP	OE.TIME	OE.PROTECT
T.FALREC			X														
T.FALASC			X														
T.MISUSE		X							X								
T.INADVE		X							X								
T.MISACT		X							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							X	
P.INTGTY										X							
P.PROTCT								X				X					X

Table 8-2 ***Threats, Assumptions, and Policies to Security Objectives Rationale***

Threat/Assumption/Policy	Security Objectives Rationale
A.ACCESS The TOE has access to all the IT System data it needs to perform its functions.	The OE.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 OE.INTROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will manage appropriately.
	The OE.INTROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.ASCOPE The TOE is appropriately scalable to the IT System the TOE monitors.	The OE.PHYCAL provides for the physical protection of the TOE hardware and software.
	The OE.PHYCAL provides for the physical protection of the TOE.
A.PROTCT The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.	The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.
	The OE.INSTAL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.

Table 8-2 Threats, Assumptions, and Policies to Security Objectives Rationale (continued)

Threat/Assumption/Policy	Security Objectives Rationale
A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	The OE.PHYCAL objective provides for physical protection of the TOE to protect against unauthorized access. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
	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. OE.PROTECT objective addresses this threat by providing IT Environment self-protection to address the module TOE from being vulnerable to bypass attacks.
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.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.PROTCT objective addresses this threat by providing TOE self-protection. OE.PROTECT objective addresses this threat by providing IT Environment self-protection to address the module TOE from being vulnerable to bypass attacks.
	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.
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.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.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.
	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.

Table 8-2 Threats, Assumptions, and Policies to Security Objectives Rationale (continued)

Threat/Assumption/Policy	Security Objectives Rationale
A.NOTRST The TOE can only be accessed by authorized users	The OE.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.
	The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.
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.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.
	The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.
T.COMDIS An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.	The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.
	The O. IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.
T.LOSSOF An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.	The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE to collect system data.
	The O.AUDITS and O.IDSENS objectives address this threat by requiring a TOE to collect system data.
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.AUDITS and O.IDSENS objectives address this threat by requiring a TOE to collect system data.
	The O.AUDITS and O.IDSENS objectives address this policy by requiring collection of system data. OE.TIME objective supports the collection of system data by ensuring the IT Environment for the module TOE provides a reliable time source.

Table 8-2 Threats, Assumptions, and Policies to Security Objectives Rationale (continued)

Threat/Assumption/Policy	Security Objectives Rationale
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.IDANLZ objective requires analytical processes be applied to data collected from Sensors.
	The OE.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 OE.INSTAL objective supports the OE.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 OE.CREDEN objective requires administrators to protect all authentication data. The O.PROTCT objective addresses this policy 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.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.
	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. OE.TIME objective supports the implementation of audit records by ensuring the IT Environment for the module TOE provides a reliable time source.
T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.	The O.INTEGR objective ensures the protection of data from modification.
	The O.OFLOWS objective counters this policy by requiring the TOE handle disruptions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications. OE.PROTECT ensures the IT Environment of the module TOE provides protection from unauthorized external entities.

Security Requirements Rationale

The purpose of this section is to show that the identified security requirements (Security Requirements, page 5-1) are *suitable* to meet the security objectives (Security Objectives, page 4-1). The following tables show that each security requirement (and SFRs in particular) is *necessary,* that is, each security objective is addressed by at least one security requirement, and vice versa.

Table 8-3 identifies each Security Requirement identified in TOE Security Functional Requirements, page 5-1 and SFRs With SOF Declarations, page 5-12, and the TOE security objective(s) identified in Security Objectives for the TOE, page 4-1 that address it. Table 8-4 provides the mapping and rationale for inclusion of each requirement in this ST.

Table 8-3 TOE Security Requirement to TOE Security Objectives Mapping

	O. PROTCT	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR
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	
FCS_CKM.1	X									
FCS_CKM.4	X									
FCS_COP.1(1)	X									
FCS_COP.1(2)	X									
FIA_UAU.1						X	X			
FIA_ATD.1							X			
FIA_UID.1						X	X			
FMT_MOF.1	X					X	X			
FMT_MTD.1	X					X	X			X
FMT_MSA.2	X									
FMT_SMR.1							X			
FMT_SMF.1	X					X	X			X
FPT_RVM.1(1)	X				X		X		X	X
FPT_SEP.1(1)	X				X		X		X	X
FPT_STM.1(1)									X	
FTP_ITC.1(1)	X									
FTP_ITC.1(2)	X									
FTP_RTC.1	X									
IDS_SDC.1		X								
IDS_ANL.1			X							
IDS_RCT.1				X						
IDS_RDR.1					X	X	X			

Table 8-3 TOE Security Requirement to TOE Security Objectives Mapping (continued)

	O. PROTCT	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR
IDS_STG.1	X					X	X	X		X
IDS_STG.2								X		

Table 8-4 TOE Requirements to TOE Security Objectives Rationale

Security Objective (TOE)	Security Requirement Rationale
O.PROTCT The TOE must protect itself from unauthorized modifications and access to its functions and 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, 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, FMT_SMF.1]. Only authorized system administrators of the System may query and add System and audit data, and 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(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(1)]. The Module TSF requests time from the host IT environment and receives it via a trusted channel [FTP_ITC.1(2)]. The execution of the Module TOE is also protected by allowing the host IT environment to halt execution the module through a trusted channel [FTP_ITC.1(2)]. The TOE provides a trusted channel between itself and a remote trusted IT product (signature server) in order for the TOE to receive signature updates [FTP_ITC.1(1)]. The TOE provides a trusted channel for remote administration protected by cryptography [FTP_RTC.1, FCS_CKM.1, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FMT_MSA.2]
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 [IDS_SDC.1].

Table 8-4 TOE Requirements to TOE Security Objectives Rationale (continued)

Security Objective (TOE)	Security Requirement Rationale
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 users 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(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(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, FMT_SMF.1]. Only authorized system administrators of the System may query and add System and audit data, and may query and modify all other TOE data [FMT_MTD.1, FMT_SMF.1].

Table 8-4 TOE Requirements to TOE Security Objectives Rationale (continued)

Security Objective (TOE)	Security Requirement Rationale
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, FMT_SMF.1]. Only authorized system administrators of the System may query and add System and audit data, and may query and modify all other TOE data [FMT_MTD.1, FMT_SMF.1]. The TOE must be able to recognize the different 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(1)]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1(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].

Table 8-4 TOE Requirements to TOE Security Objectives Rationale (continued)

Security Objective (TOE)	Security Requirement Rationale
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(1)]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1(1)]. Time stamps associated with an audit record must be reliable[FPT_STM.1(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 users of the System may query or add audit and System data [FMT_MTD.1, FMT_SMF.1]. The TOE must ensure that all functions to protect the data are not bypassed [FPT_RVM.1(1)]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1(1)].

TOE Security Functional Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified TOE and IT Security Functional Requirements include the appropriate hierarchical SFRs and dependent SFRs. Table 8-5 lists the TOE Security Functional Components and the Security Functional Components each are hierarchical to and dependent upon and any necessary rationale.

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

Table 8-5 TOE Security Functional Requirements Dependency Rationale

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FAU_GEN.1	No other components	FPT_STM.1(1), FPT_STM.1(2)	Satisfied
FAU_SAR.1	No other components	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components	FAU_SAR.1	Satisfied
FAU_SAR.3	No other components	FAU_SAR.1	Satisfied

Table 8-5 TOE Security Functional Requirements Dependency Rationale (continued)

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
FAU_SEL.1	No other components	FAU_GEN.1, FMT_MTD.1	Satisfied
FAU_STG.2	FAU_STG.1	FAU_GEN.1	Satisfied
FAU_STG.4	FAU_STG.3	FAU_STG.1	Satisfied
FCS_CKM.1	No other components	FCS_COP.1(1) FCS_COP.1(2), FCS_CKM.4, FMT_MSA.2	Satisfied
FCS_CKM.4	No other components	FCS_CKM.1, FMT_MSA.2	Satisfied
FCS_COP.1(1)	No other components	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	Satisfied
FCS_COP.1(2)	No other components	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	Satisfied
FIA_UAU.1	No other components	FIA_UID.1	Satisfied
FIA_ATD.1	No other components	None	N/A
FIA_UID.1	No other components	None	Satisfied
FMT_MOF.1	No other components	FMT_SMF.1, FMT_SMR.1	Satisfied
FMT_MTD.1	No other components	FMT_SMF.1, FMT_SMR.1	Satisfied
FMT_MSA.2	No other components	ADV_SPM.1, FDP_ACC.1 or FDP_IFC.1, FMT_MSA.1, FMT_SMR.1	FMT_MSA.2 is included to satisfy the dependency for FCS requirements. ADV_SPM.1, FDP_ACC.1, FDP_IFC.1, and FMT_MSA.1 are not applicable with regards to supporting cryptographic functionality and are not included in this ST.
FMT_SMR.1	No other components	FIA_UID.1	Satisfied
FMT_SMF.1	No other components	None	N/A
FPT_RVM .1(1)	No other components	None	Satisfied
FPT_SEP.1(1)	No other components	None	Satisfied
FPT_STM.1(1)	No other components	None	N/A
FTP_ITC.1(1)	No other components	None	N/A
FTP_ITC.1(2)	No other components	None	N/A
FTP_RTC.1 (EXP)	No other components	None	N/A

Table 8-5 TOE Security Functional Requirements Dependency Rationale (continued)

Security Functional Requirement (TOE)	Hierarchical To	Dependency	Rationale
IDS_SDC.1 (EXP)	N/A	N/A	N/A
IDS_ANL.1 (EXP)	N/A	N/A	N/A
IDS_RCT.1 (EXP)	N/A	N/A	N/A
IDS_RDR.1 (EXP)	N/A	N/A	N/A
IDS_STG.1 (EXP)	N/A	N/A	N/A
IDS_STG.2 (EXP)	N/A	N/A	N/A

TOE Security Assurance Component Dependencies

Table 8-6 lists the TOE Security Assurance Components and the Security Assurance Components each are dependent upon and any necessary rationale.

Table 8-6 EAL2 Assurance Requirement Dependency Satisfaction

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

Rationale for Strength of Function Claim

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 1.6, April 2006.

Rationale for TOE 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 1.6 April, 2006.

Rationale for Explicitly Stated SFRs for the TOE

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.

FTP_RTC.1 was created to correctly specify the TOE's use of a protected channel for remote administration. Per PD-0108, an explicit SFR based on FTP_ITC.1 is specified.

TOE Summary Specification Rationale

This section demonstrates the suitability of the security functions defined in TOE Security Functions, page 6-1 of meeting the TOE's Security Functional Requirements identified in TOE Security Functional Requirements, page 5-1 and that the security functional requirements are completely and accurately met by the TOE's Security Functions identified in TOE Security Functions, page 6-1.

Table 8-7 demonstrates the correspondence between the Security Functions and the TOE Security Functional Requirements. With the demonstration of correspondence given in Table 8-8 and the descriptions of the security functions given in TOE Security Functions, page 6-1 on how the security functions are providing the functionality to meet the security functional requirements in Table 8-8 this provides the evidence of suitability of the security functions in meeting the security functional requirements stated in TOE Security Functional Requirements, page 5-1.

The mutually supportive nature of the IT security functions can be derived from the mutually support of the SFRs (demonstrated in Security Requirements Rationale, page 8-5), as each of the security functions can be mapped to one or more SFRs, as demonstrated in Table 8-7.

Table 8-7 TOE Security Functional Requirement to TOE Security Functions Mapping

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
Audit	FPT_STM.1
Identification & Authentication	FIA_UAU.1
Identification & Authentication	FIA_ATD.1
Identification & Authentication	FIA_UID.1
Security Management	FMT_MOF.1
Security Management	FMT_MTD.1
Security Management	FMT_SMF.1
Security Management	FMT_SMR.1
Network Traffic Analysis	IDS_SDC.1
Network Traffic Analysis	IDS_ANL.1
Network Traffic Analysis	IDS_RCT.1
Self-protection	FPT_RVM.1(1)
Self-protection	FPT_SEP.1(1)
Self-protection	FPT_STM.1(1)
Self-protection	FTP_ITC.1(1)
Self-protection	FTP_ITC.1(2)
Self-protection	FTP_RTC.1
Self-protection	FCS_CKM.1
Self-protection	FCS_CKM.4
Self-protection	FCS_COP.1(1)
Self-protection	FCS_COP.1(2)
Self-protection	FMT_MSA.2

Table 8-8 Rationale of how the Security Functions meet the Security Functional Requirements

SFR	SF and Rationale
FAU_GEN.1	Is implemented by the Audit Function. The Audit Function generates audit records for security related events with specific information captured for each event.
FAU_SAR.1	Is implemented by the Audit Function. The Audit Function stores audit records in the Event Store. Authorized administrators, operators, and viewers are allowed read access to the audit records. Audit records are presented in a readable format.
FAU_SAR.2	Is implemented by the Audit Function. Through the use of roles, the Audit Function ensures that only authorized users can read audit data, and all others are denied access to his data.
FAU_SAR.3	Is implemented by the Audit Function. The Audit security function allows authorized users the ability to sort audit records based on data and time, subject identity, type of event, and success or failure of related event.
FAU_SEL.1	Is implemented by the Audit Function. The Audit Function allows the authorized user to pre-select the audit events that are generated by the TOE by event type. The TOE event types are a set of event records and include evAlert, evError, and evStatus event types.

Table 8-8 Rationale of how the Security Functions meet the Security Functional Requirements

SFR	SF and Rationale
FAU_STG.2	Is implemented by the Audit Function. Only an administrator can clear audit records via the clear events command through the CLI. If the command to clear the audit records is issued by an unauthorized user which is not in the user privilege level, the CLI (or Web Server) will return an syntax error and will not execute the command. In the event of audit storage exhaustion, the number of records saved will be the most recent saved and inserted in the Event Store limited by the storage space of the event store.
FAU_STG.4	Is implemented by the Audit Function. When the Event Store's capacity is reached, the TOE overwrites the oldest stored audit records and sends 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.
FCS_CKM.1	Is implemented by the Self Protection Function. The TOE implements the cryptographic key generation functions of the SSH and TLS/SSL protocols to protect the communication channel for remote administration.
FCS_CKM.4	Is implemented by the Self Protection Function. The TOE implements the cryptographic key destruction functions of the both the SSH and TLS/SSL protocols to protect the communication channel for remote administration.
FCS_COP.1(1)	Is implemented by the Self Protection Function. The TOE implements SSH crypto operations to protect the communication channel for remote administration.

Table 8-8 Rationale of how the Security Functions meet the Security Functional Requirements

SFR	SF and Rationale
FCS_COP.1(2)	Is implemented by the Self Protection Function. The TOE implements SSL crypto operations to protect the communication channel for remote administration.
FIA_UAU.1	Is implemented by the Identification and Authentication Function. The Identification and Authentication Function requires users to undergo authentication before access to its management interfaces is granted.
FIA_ATD.1	Is implemented by the Identification and Authentication Function. The Identification and Authentication maintains user identity, authentication data, and authorizations on each user of the system.
FIA_UID.1	Is implemented by the Identification and Authentication Function. The Identification and Authentication Function requires users to undergo a TLS or SSH handshake or input of authentication data as part of identification.
FMT_MOF.1	Is implemented by the Security Management Function. The Security Management Function permits only authorized system administrators to modify the behavior of functions for system data collection, analysis and reaction.
FMT_MTD.1	Is implemented by the Security Management Function. The Security Management Function only permits the authorized administrators and operators to query and add System and audit data and query and modify all other TOE data. Viewers can only query all other TOE data.
FMT_MSA.2	Is implemented by the Self Protection Function. The TOE implements crypto operations using valid parameter values.

Table 8-8 Rationale of how the Security Functions meet the Security Functional Requirements

SFR	SF and Rationale
FMT_SMR.1	Is implemented by the Security Management Function. The Security Management Function maintains three roles that correspond to the authorized administrator and authorized system administrator privilege levels defined in the SFRs and ensures that a user is authenticated before allowing them to perform functions only provided for each role.
FMT_SMF.1	Is implemented by the Security Management Function. The Security Management Function provides the security management functions to modify the behavior of system data collection, analysis, and reaction, to query and add system and audit data and query and modify TOE data.
FPT_RVM .1(1)	Is implemented by the Self-Protection Function. The TOE makes sure that security enforcing functions are invoked and succeed before allowing any other mediated action to occur.
FPT_SEP.1(1)	Is implemented by the Self-Protection Function. The Self-Protection Function provides a protected execution domain and a separation of traffic streams traversing the TOE. The TOE is a dedicated device, with no general purpose operating system, or programming interface. No untrusted processes are permitted on the TOE.
FPT_STM.1(1)	Is implemented by the Audit Function and Self-Protection Function. The TOE has an internal system clock which is used to generate timestamps for audit records. For the Module TOE, the initial setting of the clock is received from the host IT environment via a trusted channel. The Module TOE maintains the time until a reset or time change occurs. Upon reboot the clock is resynchronized with the host IT environment. Via the trusted channel, the administrator of the host IT environment can change the clock of the Module TOE.

Table 8-8 Rationale of how the Security Functions meet the Security Functional Requirements

SFR	SF and Rationale
FTP_ITC.1(1)	Is implemented by the Self-Protection Function. The TOE provides a trusted channel for signature updates.
FTP_ITC.1(2)	Is implemented by the Self-Protection Function. The Module TOE and its host IT environment communicate via a trusted channel to receive time and to allow execution control of the module (power off).
FTP_RTC.1 (EXP)	Is implemented by the Self-Protection Function. The TOE supports a protected communication channel via SSH and SSL for remote administration.
IDS_SDC.1 (EXP)	Is implemented by the Network Traffic Analysis Function. The Network Traffic Analysis Function generates event for IDS, IPS, related events with specific information captured for each event.
IDS_ANL.1 (EXP)	Is implemented by the Network Traffic Analysis Function. The Network Traffic Analysis Function performs signature based and event correlation analysis methods to identify malicious activities on the IT network. Analytical results are stored with specific information.
IDS_RCT.1 (EXP)	Is implemented by the Network Traffic Analysis Function. If an alarm is generated it is automatically sent to the Event Store. The TOE can be configured to take specific response actions depending on the mode (promiscuous and inline modes) of the analyzed interface.
IDS_RDR.1 (EXP)	Is implemented by the Audit Function. The Audit Function stores IDS/IPS related event data. Administrators, operators, and viewers are allowed read access to the event data. Event data is presented in a readable format.

Table 8-8 Rationale of how the Security Functions meet the Security Functional Requirements

SFR	SF and Rationale
IDS_STG.1 (EXP)	Is implemented by the Audit Function. Only an administrator can clear IDS/IPS event data via the clear events command through the CLI. If the command to clear the event data is issued by an unauthorized user which is not in the user privilege level, the CLI (or Web Server) will return an syntax error and will not execute the command. In the event of audit storage exhaustion, the number of records saved will be most recent saved and inserted in the Event Store limited by the storage space of the event store.
IDS_STG.2 (EXP)	Is implemented by the Audit Function. When the Event Store's capacity is reached, the TOE overwrites the oldest stored records and sends 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.