Cisco IronPort S-Series Web Security Appliance
Security Target

Version 1.0
October 12, 2009

Prepared for:
Cisco IronPort Systems

1100 Grundy Lane
San Bruno, CA 94066

Prepared By:
Science Applications International Corporation

Common Criteria Testing Laboratory

7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE), ST conventions, ST conformance claims, and the ST organization. The TOE is the Cisco IronPort S-Series Web Security Appliance (WSA) (S160, S360, S660) running IronPort Async Operating System (AsyncOS) 5.6.1 provided by IronPort Systems. The TOE is an Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) that protects the enterprise against web-based malware and spyware programs, as well as providing protection for standard communication protocols.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Environment (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 0).

1.1 Security Target, TOE and CC Identification

ST Title – Cisco IronPort S-Series Web Security Appliance Security Target

ST Version – Version 0.98

ST Date – October 12, 2009

TOE Identification – Cisco IronPort S-Series Web Security Appliance (WSA) (S160, S360, S660) running AsyncOS 5.6.1

TOE Developer – IronPort Systems

Evaluation Sponsor – IronPort Systems

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005.
    - Part 3 Conformant
    - Assurance Level: EAL 2
    - Strength of Function (SOF) Claim: SOF-Basic
- Additionally, this ST is conformant with the U.S. Government Intrusion Detection System (IDS) System Protection Profile (IDSSPP), Version 1.6, April 4, 2006.

1.3 Conventions and Terminology

This section specifies the formatting information used in the Security Target.

1.3.1 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, refinement and explicit.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a letter placed at the end of the component. For example FDP_ACC.1a and FDP_ACC.1b indicate that the ST includes two iterations of the FDP_ACC.1 requirement, a and b.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
    - Explicit: defines explicitly stated Security Functional Requirements (SFRs) that end with (EXP) and the end of the element.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.2 Terminology and Acronyms

BSD	Berkely Software Distribution
CC	Common Criteria
CIDR	Classless Inter-Domain Routing
CLI	Command Line Interface
DVS	Dynamic Vectoring and Streaming
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hyper-text Transfer Protocol
HTTPS	Secure HTTP
ID	Identity / Identification
IDS	Intrusion Detection System
IDSSPP	IDS System PP
IE	Internet Explorer
IP	Internet Protocol
IPS	Intrusion Prevention System
IRC	Internet Relay Chat

IT	Information Technology
L4	Layer 4
LDAP	Lightweight Directory Access Protocol
LAN	Local Area Network
MIB	Management Information Base
NTLM	NT LAN Manager
OS	Operating System
P2P	Peer-to-Peer
PC	Personal Computer
PD	Precedent Decision
PP	Protection Profile
WBNP	SenderBase Network Participation
SFR	Security Functional Requirement
SHD	System Health Daemon
SNMP	Simple Network Management Protocol
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WBNP	SenderBase Network Participation
WBRS	Web Reputation Score
WCCP	Web Cache Coordination Protocol
WSA	Web Security Appliance
XML	eXtensible Markup Language

2. TOE Description

The Target of Evaluation is the Cisco IronPort S-Series Web Security Appliance (WSA) (S160, S360, S660) running AsyncOS 5.6.1 for Web, hereon referred to as the TOE, WSA, or IronPort WSA. The three variants of the S-Series are identical except with respect to performance tuning settings which optimize the S660 for use in the highest bandwidth environments. The S160 is designed for environments with up to 1,000 users. The S360 is designed for environments with 1,000 to 10,000 users. The S660 is designed for environments with more than 10,000 users. The TOE includes both the physical hardware device and the operating system which underlies the IronPort custom application software. AsyncOS 5.6.1 for Web is a proprietary computer operating system developed by IronPort Systems and based on a hardened Free Berkely Software Distribution (FreeBSD) Unix kernel.

The TOE is an Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) that protects the enterprise against web-based malware and spyware.

The TOE provides protection for the following standard communication protocols: Hyper-Text Transfer Protocol (HTTP), Secure HTTP (HTTPS) and File Transfer Protocol (FTP). Additionally, the TOE can be characterized as a network application security and gateway device.

The remainder of this section summarizes the TOE architecture.

2.1 TOE Overview

The TOE analyzes the characteristics of web requests and responses and makes determinations regarding whether the request or response will be blocked, monitored, or allowed. The TOE provides two independent sets of security services to fulfill its objectives, Web Proxy Services and the Layer 4 (L4) Traffic Monitor.

Web Proxy Services examine outbound client requests and consist of four features which work in concert to prevent users from accessing known or suspected malware distribution vectors. The four features of Web Proxy Services are:

- Policy Groups – administrator defined groups of users which specify exceptions to global policy settings based on client IP address, authentication group, or username.
- Uniform Resource Locator (URL) Filters – control user access to URLs based on the category of a particular HTTP request.
- Web Reputation Filters – analyze web server behavior and characteristics to identify suspicious activity.
- Anti-Malware Scanning – when a URL has a questionable reputation, the HTTP traffic receives an in-depth inspection using the IronPort Dynamic Vectoring and Streaming (DVS) engine in concert with the Webroot Signature database.

The L4 Traffic Monitor detects rogue traffic by monitoring all network traffic received on all Transmission Control Protocol (TCP) ports on the appliance and matching that traffic to an internal database based on domain names and Internet Protocol (IP) addresses.

2.2 TOE Architecture

2.2.1 Software Architecture

Web Proxy Services and the L4 Traffic Monitor are independent services which are enabled and configured separately.

Web Proxy Services monitor and control traffic that originates from clients on the internal network. Web Access Policies are a combination of Policy Groups and URL Filters that provide a variety of options for controlling user access to the Internet and impose restrictions inside the intranet domain.

Policy Groups provide the administrator with a mechanism for grouping users. Membership in groups can be specified based on client IP address, username, or authorization group. Note that in the evaluated configuration username and authorization group are not valid group types because global authentication is disabled. Global authentication requires that the TOE have access to either a Lightweight Directory Access Protocol (LDAP) directory or an NT Local Area Network (LAN) Manager (NTLM) server and that the LDAP directory or NTLM server is configured to authorize clients. This capability is not provided by the IT environment in the evaluated configuration. Note that this authentication is separate from authenticating to the TOE for purposes of administration. Administration of the TOE can only be performed by authorized administrators after having logged on to the TOE with a valid username and password. The TOE maintains the authentication information for all authorized administrators.

URL Filters provide the administrator with a mechanism for determining how the TOE responds to each web request. URL Filters have the following components which are compared, in order, with URL requests each time the policy is evaluated.

Table 1 – URL Filters

Filter Components	Description
Applications	Applications control Policy Group access to specific protocols and configure blocking for Internet applications such as instant messaging and Internet phone service.
URL Categories	URL Categories control Policy Group access based on the URL category of the HTTP request. A decision is made to either monitor or block the request depending on settings for a set of pre-defined URL categories. The pre-defined URL categories are: Adult/Sexually Explicit, Advertisements/Popups, Alcohol/Tobacco, Arts, Blogs/Forums, Business, Chat, and Computing/Internet. Custom URL Categories can be defined.
Objects	Objects control Policy Group access to file downloads based on file characteristics such as file size and file type.
Web Reputation	Web Reputation filters calculate a numerical score for a web request that predicts the likelihood that the URL contains malware. Based on the value calculated, a determination to either allow, block, or scan the URL request is made. This determination is made by comparing the calculated value with settings specified by the administrator.
Anti-Malware	If the result of a Web Reputation filter is to scan, then the DVS engine inspects the URL request and the server response using signatures from the Webroot signature database.

The URL Categories, Web Reputation and Anti-Malware filter components all utilize database tables that are maintained by the TOE. The TOE periodically updates those tables by contacting the vendor over an HTTPS connection and requesting updates. The integrity of these updates is assured using integrity mechanisms inherent in the SSL protocol (e.g. SHA1 or MD5).

The L4 Traffic Monitor scans all ports at wire speed, detecting and blocking malware spyware 'phone-home' activity. The L4 Traffic Monitor tracks all 65,535 TCP and User Datagram Protocol (UDP) ports to block malware that attempts to bypass Port 80 and prevents rogue Peer-to-Peer (P2P) and Internet Relay Chat (IRC) related activity. The TOE L4 Traffic Monitor allow list is a manually populated list of trusted IP addresses and domain names that the monitor does not need to monitor or block that is configured by an authorized Administrator. The L4 Traffic Monitor uses and maintains its own internal database that is updated with matched results for IP addresses and domain names. It also receives periodic updates from the vendor by means of an HTTPS connection.

2.2.2 Hardware Architecture

The TOE is a computer network hardware appliance in a 2U, 19" rack mountable chassis. Its physical interfaces consist of six (6) RJ45 Interfaces operating at gigabit speeds. The interfaces are detailed below:

Table 2 – TOE Physical Interfaces

Label	Purpose
T1	L4 Traffic Monitor (passive): In simplex mode – monitors all outgoing network traffic In duplex mode – monitors all incoming and outgoing network traffic
T2	L4 Traffic Monitor (passive): Simplex mode only – monitors all incoming network traffic
P1	Proxy port (active) – connects the TOE to an L4 switch or Web Cache Coordination Protocol (WCCP) router in the environment
P2	Unused – disabled
M1	Management port (active) – connects the appliance Personal Computer (PC) or management network for configuration and administration of the TOE
M2	Unused – disabled

The TOE is intended to monitor a computer network which is considered part of its Information Technology (IT) environment. There are expectations that the environment provides hardware to which the TOE can attach so that monitoring can take place and so that HTTP traffic is routed through the TOE. The intended hardware environment and suggested configuration are detailed in the following diagram. Note, the connection for passive monitoring in the diagram below is to illustrate the connection to the TOE itself, not a separate device.

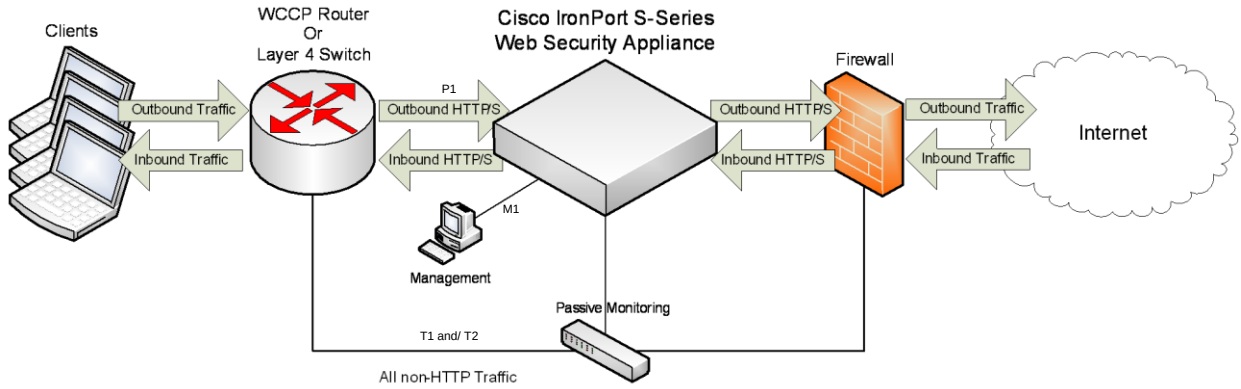

Figure 1 – TOE Environment and Traffic Flow

2.2.3 Physical Boundaries

The TOE is installed as self contained network appliance. The physical boundary of the TOE extends to the RJ45 network interface connections which serve as the connection point between the TOE and the IT environment. The TOE requires either a L4 switch or a WCCP router in the IT environment to direct client traffic to the appliance.

The Graphical User Interface (GUI) used for TOE administration requires a web browser which is installed on a dedicated PC physically connected via an isolated (private) Ethernet management network. There are no limitations on the selection of the web browser. The CLI is available via a terminal physically connected to the serial port.

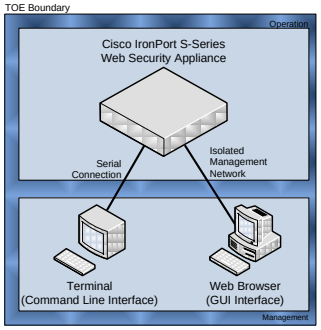

Figure 2 - TOE Boundary

2.2.4 Logical Boundaries

This section summarizes the security functions provided by WSA:

- Security Audit
- Identification and Authentication
- Security Management
- Protection of the TSF
- Intrusion Detection System

2.2.4.1 Security Audit

The TOE generates audit events for the basic level of audit. Note that the IDS_SDC and IDS_ANL requirements address the recording of results from IDS scanning, sensing and analyzing tasks (e.g., System data).

Refer to Section 6.1.1 for additional information on security audit.

2.2.4.2 Identification and Authentication

The TOE maintains user identities, authentication data, authorizations and groups. The administrative console provides the single TOE logon mechanisms for authorized Administrator to manage security functions. No user is allowed access to the security functions without being authenticated and identified by the system.

Refer to Section 6.1.2 for additional information on identification and authentication.

2.2.4.3 Security Management

The TOE restricts the ability to administer functions related to auditing, use of the authentication mechanism, user security attributes, information flow control policy, scanning, sensing and analyzing tasks data (e.g., System data) to authorized Administrator.

Refer to Section 6.1.3 for additional information on security management.

2.2.4.4 Protection of the TSF

The TOE provides a reliable timestamp for logging purposes and provides a security domain for its own use. The TOE also provides the ability to detect modification and to verify the integrity of all signature updates received from a remote update server in the IT environment of the TOE.

Refer to Section 6.1.4 for additional information on protection of the TSF.

2.2.4.5 Intrusion Detection System (EXP)

The TOE monitors network traffic on containing malware and/or reputation policy data, acting as an IDS scanner. The TOE performs signature and integrity analysis on network traffic, security configuration changes, data

introduction, detected known vulnerabilities and detected malware on monitored web traffic and records corresponding event data.

Refer to Section 6.1.5 for additional information on IDS.

2.3 TOE Documentation

IronPort offers a series of documents that describe the installation process for the TOE, as well as guidance for subsequent use and administration of system security features. Refer to Section 6.2 for information about these and other evidence assurance documents.

3. Security Environment

3.1 Assumptions

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

3.1.1 Intended Usage 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.

3.1.2 Physical Assumptions

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

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

3.1.3 Personnel Assumptions

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

A.NOEVIL The authorized Administrator are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

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

3.2 Threats

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

3.2.1 TOE Threats

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

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

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

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

T.PRIVIL An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data

T.IMPCON An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

T.INFLUX An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

T.FACCNT Unauthorized attempts to access TOE data or security functions may go undetected.

3.2.2 IT System Threats

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

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

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

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

T.FALACT The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

T.FALREC The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

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

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

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

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

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. This section identifies the organizational security policies applicable to the IDSSPP.

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.

4. Security Objectives

This section identifies the security objectives of the TOE and its supporting environment. The security objectives identify the responsibilities of the TOE and its environment in meeting the security needs.

4.1 Security Objectives for the TOE

The following are the TOE security objectives:

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

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

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

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

O.IMPORT When a remote trusted IT product makes TSF system data available to an IDS component, the TOE will ensure the integrity of the TSF system data.

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

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

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

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

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

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

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

4.2 Security Objectives for the IT Environment

The TOEs operating environment must satisfy the following objectives.

O.INSTAL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.

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

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

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

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

5. IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) for the TOE.

5.1 TOE Security Functional Requirements

The following SFRs are drawn from the CC, Part 2 where these requirements are relevant to supporting the secure operation of the TOE. Functional requirements pertaining to the system collection, analysis and reaction mechanisms are derived from the U.S. Government IDSSPP, V1.6 and are identified by the short name IDS. U.S. English has been used, as authorized.

The following table describes the SFRs that are satisfied by WSA.

Table 3 - TOE Security Functional Components

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
	FAU_SAR.1: Audit Review
	FAU_SAR.2: Restricted Audit Review
	FAU_SAR.3: Selectable Audit Review
	FAU_SEL.1: Selective Audit
	FAU_STG.2: Guarantees of audit data availability
	FAU_STG.4: Prevention of Audit Data Loss
FIA: Identification and Authentication	FIA_UAU.2: User authentication before any action
	FIA_ATD.1: User Attribute Definition
	FIA_UID.2: User identification before any action
FMT: Security Management	FMT_MOF.1: Management of Security Functions Behavior
	FMT_MTD.1a: Management of TSF Data
	FMT_MTD.1b: Management of TSF Data
	FMT_MTD.1c: Management of TSF Data
	FMT_MTD.1d: Management of TSF Data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Roles
FPT: Protection of the TOE Security Functions	FPT_RVM.1: Non-bypassability of the TSP
	FPT_SEP.1: Domain separation
	FPT_STM.1: Reliable time stamps
	FPT_ITI.1: Integrity of exported TSF data
IDS: Intrusion Detection System	IDS_SDC.1: System Data Collection (EXP)
	IDS_ANL.1: Analyzer analysis (EXP)
	IDS_RCT.1: Analyzer react (EXP)
	IDS_RDR.1: Restricted Data Review (EXP)
	IDS_STG.1: Guarantee of System Data Availability (EXP)
	IDS_STG.2: Prevention of System data loss (EXP)

5.1.1 Security Audit (FAU)

5.1.1.1 Audit Data Generation (FAU_GEN.1)

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 PP/ST, [**the additional information specified in the Details column of the following table**].

Table 4 – 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.2	All use of the authentication mechanism	User identity, location
FIA_UID.2	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1a-d	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

5.1.1.2 Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**authorized Administrators**] with the capability to read [**all audit information**] from the audit records.

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

5.1.1.3 Restricted Audit Review (FAU_SAR.2)

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

5.1.1.4 Selectable Audit Review (FAU_SAR.3)

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

5.1.1.5 Selective Audit (FAU_SEL.1)

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
a) [***event type***];
b) [**no additional attributes**].

5.1.1.6 Guarantees of Audit Data Availability (FAU_STG.2)

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 [***prevent***] unauthorized modifications to the stored audit records in the audit trail.

FAU_STG.2.3 The TSF shall ensure that [**at least 10MB per log file**] audit records will be maintained when the following conditions occur: [***audit storage exhaustion***].

5.1.1.7 Prevention of Audit Data Loss (FAU_STG.4)

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

5.1.2 Identification and Authentication (FIA)

5.1.2.1 User authentication before any action (FIA_UAU.2)

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

5.1.2.2 User Attribute Definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [
a) User identity;
b) Authentication data;
c) Authorizations; and
d) Role].

Application Note: The TOE applies permissions (e.g., authorizations) to three (3) default groups (i.e., Administrators, Operators, Guests) where users are assigned to each of these groups based on role (e.g., access authorizations) required. All users of the TOE are considered authorized Administrator. Further, the TOE has four (4) unique roles as there is one default System Administrator and all other authorized Administrators are assigned to a role based on group assignment.

5.1.2.3 User identification before any action (FIA_UID.2)

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

5.1.3 Security Management (FMT)

5.1.3.1 Management of Security Functions Behavior (FMT_MOF.1)

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 Administrator and authorized Administrators**].

5.1.3.2 Management of TSF Data (FMT_MTD.1a)

FMT_MTD.1.1a The TSF shall restrict the ability to [***query, modify, delete, clear,*** [**and add**] the **[System configuration settings and groups to which a user belongs**]] to [**the authorized System Administrator**].

Application Note: The TOE has one System Administrator account by default that cannot be edited or deleted. All other users are associated to a default group (i.e., Administrators, Operators, Guests) based on level of default permissions needed.

5.1.3.3 Management of TSF Data (FMT_MTD.1b)

FMT_MTD.1.1b The TSF shall restrict the ability to [***query, modify, delete, clear,*** [**and add**]] the **[System configuration settings except issuing the upgrade and upgradeconfig commands and groups to which a user belongs**] to [**the Administrators group**].

5.1.3.4 Management of TSF Data (FMT_MTD.1c)

FMT_MTD.1.1c The TSF shall restrict the ability to [***query, modify, delete, clear,*** [**and add**]] the [**System configuration settings except the ability to create, edit or remove user accounts and issue the**

upgrade, upgradeconfig, resetconfig, systemsetup, and userconfig commands or running the System Setup Wizard] to [**the Operators group**].

5.1.3.5 Management of TSF Data (FMT_MTD.1d)

FMT_MTD.1.1d The TSF shall restrict the ability to [***query***] the [**system status information**] to [**the Guests group**].

5.1.3.6 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [**management of audit data; management of user security attributes (roles and groups); management of system configuration settings; manage functions and data related to scanning, sensing and analyzing tasks**].

5.1.3.7 Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the **following** roles: [**authorized Administrators, authorized System Administrator, and authorized Operators, and authorized Guests**].

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

Application Note: All users of the TOE are considered administrators but the level of access is determined by role, where there is one System Administrator account that cannot be deleted and all other users are considered administrative in nature and are granted access based on the group assigned to for the role. The System Administrator role has full system control.

5.1.4 Protection of the TOE Security Functions (FPT)

5.1.4.1 Integrity of exported TSF data (FPT_ITI.1)

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between ~~the TSF~~ **a remote trusted IT product** and ~~a remote trusted IT product~~ **the TSF** within the following metric [**the strength must be conformant to the strength offered by SHA1 (160 bit) or MD5 (128 bit) hash algorithms**].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between ~~the TSF~~ **a remote trusted IT product** and ~~a remote trusted IT product~~ **the TSF** and perform [**ignore the TSF data, and request the originating trusted product to send the TSF data again**] if modifications are detected.

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

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

5.1.4.3 TSF domain separation (FPT_SEP.1)

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

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

5.1.4.4 Reliable time stamps (FPT_STM.1)

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

5.1.5 Intrusion Detection System (IDS)

5.1.5.1 System Data Collection (EXP) (IDS_SDC.1)

IDS_SDC.1.1 The System shall be able to collect the following information from the targeted IT System resource(s):
a) [***detected malicious code; access control configuration; service configuration***]; and
b) **[no additional information]**. (EXP)

IDS_SDC.1.2 At a minimum, the System shall collect and record the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) The additional information specified in the Details column of **the following** Table ~~3 System Events~~. (EXP)

Table 5 – System Events

Component	Event	Details
IDS_SDC.1	Detected malicious code	Location, identification of code
IDS_SDC.1	Access control configuration	Location, access settings
IDS_SDC.1	Service configuration	Service identification (name or port), interface, protocols

5.1.5.2 Analyzer analysis (EXP) (IDS_ANL.1)

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all IDS data received:
a) [*signature, integrity*]; and
b) [**no additional analytical functions**]. (EXP)

IDS_ANL.1.2 The System shall record within each analytical result at least the following information:
a. Date and time of the result, type of result, identification of data source; and
b. [identity of the malware/spyware]. (EXP)

5.1.5.3 Analyzer react (EXP) (IDS_RCT.1)

IDS_RCT.1.1 The System shall send an alarm to [**the admin console**] and take [**action to block or monitor the traffic (based on configuration)**] when an intrusion is detected. (EXP)

5.1.5.4 Restricted Data Review (EXP) (IDS_RDR.1)

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

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

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

5.1.5.5 Guarantee of System Data Availability (EXP) (IDS_STG.1)

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

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

IDS_STG.1.3 The System shall ensure that [**at least 10MB per log file of**] System data will be maintained when the following conditions occur: [***System data storage exhaustion***]. (EXP)

5.1.5.6 Prevention of System data loss (EXP) (IDS_STG.2)

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

5.2 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Table 6 - EAL 2 Assurance Components

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.2: Configuration items
ADO: Delivery and operation	ADO_DEL.1: Delivery procedures
	ADO_IGS.1: Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.1: Informal functional specification
	ADV_HLD.1: Descriptive high-level design
	ADV_RCR.1: Informal correspondence demonstration
AGD: Guidance documents	AGD_ADM.1: Administrator guidance
	AGD_USR.1: User guidance
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_SOF.1: Strength of TOE security function evaluation
	AVA_VLA.1: Developer vulnerability analysis

5.2.1 Configuration management (ACM)

5.2.1.1 Configuration items (ACM_CAP.2)

ACM_CAP.2.1d The developer shall provide a reference for the TOE.
ACM_CAP.2.2d The developer shall use a CM system.
ACM_CAP.2.3d The developer shall provide CM documentation.
ACM_CAP.2.1c The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.2.2c The TOE shall be labeled with its reference.
ACM_CAP.2.3c The CM documentation shall include a configuration list.
ACM_CAP.2.4c The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.5c The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.2.6c The CM documentation shall describe the method used to uniquely identify the configuration items that comprise the TOE.
ACM_CAP.2.7c The CM system shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2 Delivery and operation (ADO)

5.2.2.1 Delivery procedures (ADO_DEL.1)

ADO_DEL.1.1d The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2d The developer shall use the delivery procedures.
ADO_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.
ADO_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

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

ADO_IGS.1.1c The installation, generation and start-up documentation shall describe all the steps necessary for secure installation, generation and start-up of the TOE.
ADO_IGS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2e The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

5.2.3 Development (ADV)

5.2.3.1 Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1d The developer shall provide a functional specification.
ADV_FSP.1.1c The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2c The functional specification shall be internally consistent.
ADV_FSP.1.3c The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4c The functional specification shall completely represent the TSF.
ADV_FSP.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.2 Descriptive high-level design (ADV_HLD.1)

ADV_HLD.1.1d The developer shall provide the high-level design of the TSF.
ADV_HLD.1.1c The presentation of the high-level design shall be informal.
ADV_HLD.1.2c The high-level design shall be internally consistent.
ADV_HLD.1.3c The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.1.4c The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.1.5c The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.1.6c The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.1.7c The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
ADV_HLD.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.1.2e The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

5.2.3.3 Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1d The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.
ADV_RCR.1.1c For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.
ADV_RCR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Guidance documents (AGD)

5.2.4.1 Administrator guidance (AGD_ADM.1)

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

AGD_ADM.1.1c The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.
AGD_ADM.1.2c The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3c The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4c The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.
AGD_ADM.1.5c The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.
AGD_ADM.1.6c The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7c The administrator guidance shall be consistent with all other documentation supplied for evaluation.
AGD_ADM.1.8c The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.
AGD_ADM.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4.2 User guidance (AGD_USR.1)

AGD_USR.1.1d The developer shall provide user guidance.
AGD_USR.1.1c The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2c The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3c The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4c The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.
AGD_USR.1.5c The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6c The user guidance shall describe all security requirements for the IT environment that are relevant to the user.
AGD_USR.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5 Tests (ATE)

5.2.5.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.
ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.5.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
ATE_FUN.1.1c The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

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

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

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

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

5.2.5.3 Independent testing - sample (ATE_IND.2)

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

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

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

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

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

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

5.2.6 Vulnerability assessment (AVA)

5.2.6.1 Strength of TOE security function evaluation (AVA_SOF.1)

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

AVA_SOF.1.1c For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2c For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

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

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

5.2.6.2 Developer vulnerability analysis (AVA_VLA.1)

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

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

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

AVA_VLA.1.2c The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.

AVA_VLA.1.3c The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

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

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

6. TOE Summary Specification

This chapter describes the security functions and associated assurance measures.

6.1 TOE Security Functions

6.1.1 Security Audit

The TOE provides its own audit mechanism that can generate audit records for the basic level of audit that are stored in database tables in its AsyncOS component. Access to audit trail files are restricted using AsyncOS administrator command line interfaces. Access to the console is restricted to administrators and is protected both by the physical environment and IT access controls on the console. The command line interface provides the administrator with the ability to review the audit information, sort the audit data, and configure the audit mechanism including the ability to exclude auditable events based on event type.

Each audit record includes date and time of the event, type of event, subject identity, the outcome (success or failure) of the event. Events in the reporting logs can be correlated and searched by on date and time, subject identity, type of event, and success or failure of event and the auditable events include:

- Start-up and shutdown of the audit function
- Access to System
- Access to the TOE and System data
- Reading of information from the audit records
- Unsuccessful attempts to read information from the audit records
- All modifications to the audit configuration that occur while the audit collection functions are operating
- All use of the authentication mechanism
- All use of the user identification mechanism
- All modifications in the behavior of the functions of the TSF
- All modifications to the values of TSF data
- Modifications to the group of users that are part of a role

The TOE is capable of sending email alert messages to email addresses configured via the alertconfig command line interface.

Note that event details for each of the above are specified in Table 2 of the IDSSPP. Also, note that IDS_SDC (EXP) and IDS_ANL (EXP) requirements address the recording of results from IDS scanning, sensing, and analyzing tasks (i.e. auditing of System data).

Note also that Sections 6.1.2 and 6.1.3 clarify identification and authentication and security management aspects of the TOE as they relate to authorized users and configuration of security audit parameters by users.

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE generates audit events for the basic level of audit.
- FAU_SAR.1: The TOE provides administrator console interfaces that are used by authorized Administrators to read all audit information from the audit trail.
- FAU_SAR.2: The TOE restricts access to the audit trail to authorized Administrators using the administrator console interfaces.
- FAU_SAR.3: The TOE provides administrator console interfaces that can be used to sort audit data based on date and time, subject identity, type of event and success or failure of related event so that authorized Administrators and the System Administrator may review all audit data.
- FAU_SEL.1: The TOE provides administrator console interfaces that can be used to include or exclude auditable events based on event type.

- FAU_STG.2: The TOE prevents unauthorized modifications to the stored audit records from unauthorized deletion by requiring the (authorized) user to be identified and authenticated and be assigned to an authorized role/group. The TOE does not provide an interface to modify the audit logs. The most current (e.g., at least 10MB per log file) audit records are maintained when audit storage exhaustion occurs. The default log size is 10MB before the log is rolled over. The TOE supports up to 100MB of space for the log files. Therefore, it is possible to have the current log file and nine rolled over (saved) log files before any rolled over log is overwritten.
- FAU_STG.4: The TOE generates an alarm via e-mail configuration to authorized Administrators and begins overwriting the oldest stored audit records when the audit trail becomes full and does not stop collecting or producing system data.

6.1.2 Identification and Authentication

Only authorized Administrators assigned to the designated groups, and the System Administrator may access TOE functions and system data. However, they are required to log on with a unique user ID and password in order to proceed to TOE administrative interfaces via the web browser or the CLI. The TOE defines users in terms of user identity, authentication data and role, and provides its own username/password authentication mechanism. Users are assigned to groups based on role. The password mechanism requires passwords to be a minimum of six (6) characters. No administrative actions are allowed until the user has been successfully identified and authenticated.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: The TOE maintains user identities, authentication data, authorizations, and roles where users are assigned to groups based on permissions required.
- FIA_UAU.2: The TOE offers no TSF-mediated functions until the user is authenticated.
- FIA_UID.2: The TOE offers no TSF-mediated functions until the user is identified.

6.1.3 Security Management

The Command Line Interface (CLI) is used to perform all security management functions of the TOE and is available via a dedicated terminal physically connected to the serial port. The CLI can be used by authorized Administrators to manage functions related to system data collection, analysis and reaction; manage audit data and log reports; manage users (groups and roles); as well as manage network connections. The TOE also provides a Graphical User Interface (GUI)-based which can be used for all other TOE functions. The GUI requires a web browser which is installed on a dedicated PC physically connected via a private Ethernet management network. The TOE restricts access to its interfaces by requiring users to logon before allowing access to administrator console interfaces.

An authorized Administrator can monitor system/client activity, create custom reports, configure custom log files and view interactivity data and manage runtime events, as well as track overall trends in TOE behavior via the monitor tab.

Client and destination filtering policies can be configured via the Web Security Manager tab—Web Proxy Policies page by an authorized Administrator that includes requests blocked by policy; requests blocked by web reputation filters; and transactions detected by anti-malware.

Reports can be scheduled to provide summary statistics that can be viewed by an authorized Administrator using the graphical display pages located in the Monitor tab. TOE log file options include: access log file; Command Line Interface (CLI) audit logs; user interface logs; proxy logs; reporting logs; reporting query logs; SHD logs; system logs; traffic monitor error logs; traffic monitor logs; component updater logs; WBNP logs; WBRS logs; and Webroot logs.

An authorized Administrator manages proxy traffic with a set of acceptable use policy options and access control rules using the Web Security Manager where source and destination block and allow lists can be configured, along with URI regular expression-based filtering and object-type filtering to create secure policies that are consistent with enterprise requirements. Further, the Web Security Manager configures the actions (e.g., anti-malware settings) that the DVS engine takes based on its scanning verdicts for requests and responses through the proxy; and can be used

to configure the proxy to block file downloads based on file characteristics (e.g., file blocking), including file size and file type where these evaluation occur after Web Reputation Filtering and before DVS engine scanning. Valid actions are to monitor (log, but do not block) and block where these actions are configured for each verdict type.

The TOE provides four (4) user roles as: System Administrator, Administrators, Operators and Guests where the following pertains:

- System Administrator has full access to all system configuration settings, as well as ability to issue the upgrade and upgradeconfig commands, and the System Administrator is assigned to the Administrators group;
- Administrators have full access to all system configuration settings but can not issue the upgrade and upgradeconfig commands;
- Operators are restricted from creating, editing removing user accounts and can not use the following commands: resetconfig, upgrade, upgradeconfig, systemsetup or running the System Setup Wizard; and
- Guests can only view system status information.

All of the above roles, with the exception of Guests, may view audit records at the console.

The System Administrator is assigned to the Administrators group but has additional privileges than all other users in the Administrators group as identified above. The TOE has one System Administrator account by default that cannot be deleted. All users of the TOE are considered "Authorized Administrators" as they have access to TOE data based on group assignment. Users are added to a group based on the permissions they require to perform their security management responsibilities.

Although there are four (4) user roles, the TOE only has three (3) default groups defines as the Administrators group, Operators group and Guests group. These default groups can be renamed; however, the permissions are granted to these default groups based on permissions. Additional groups can be created by authorized TOE administrators, as required, based on other permission parameters specified.

An authorized Administrator can view L4 Traffic Monitor activity (e.g., reports) such as statistics on clients, malware and ports, in addition to the log files by going to the Monitor tab—Reports pages of the web interface to select a type of report, capture data, schedule periodic e-mail delivery and archive reports.

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1: The TOE restricts the ability to modify System data collection, analysis and reaction to authorized System Administrator and authorized Administrators.
- FMT_MTD.1a: The TOE restricts the ability to query, modify, delete, clear and add System and audit data, and shall restrict the ability to query and modify all other TOE data (i.e., configuration settings and assign users to groups) to the System Administrator. The TOE maintains one System Administrator account, by default, that is a member of the Administrators group; however, this user has full control.
- FMT_MTD.1b: The TOE restricts the ability to query, modify, delete, clear and add all System configuration settings except the ability to issue the upgrade and upgradeconfigcommands and assign users to groups to the Administrators group. Users assigned to the Administrators group can perform all system functions with the exception of installing and checking for TOE updates.
- FMT_MTD.1c: The TOE restricts the ability to query, modify, delete, clear and add all System configuration settings except the ability to create, edit or remove user accounts and restricts the ability to issue the upgrade, upgradeconfig, resetconfig, systemsetup, and userconfig commands or running the System Setup Wizard to the Operators group. Users assigned to the Operators group can only perform a limited set of TOE security functions.
- FMT_MTD.1d: The TOE restricts the ability to query system status information to Guests group. Users assigned to the Guests group can only view system status information and cannot perform any security management functions. These authorized administrators are generally those users assigned to monitor system status where any actions required are reported to an authorized administrator with the appropriate permissions to take actions, as required.

- FMT_SMF.1: The TOE provides security management functions to manage functions related to system data collection, analysis and reaction, system configuration, audit data and user security attributes. The TOE provides a web-based GUI and terminal application CLI for use by authorized administrators to manage TOE Security Functions (TSFs).
- FMT_SMR.1: The TOE has three assigned group roles (i.e., Administrators, Operators, Guests) and all are considered administrators in order to access TOE security data; however, the Guests may only view system data. Note that the System Administrator is part of the administrators group but has additional capabilities, as well and there is only one System Administrator.

6.1.4 Protection of the TSF

The TOE restricts access to its interfaces by requiring authorized Administrators to logon via a web browser to access the GUI or via a terminal application to access the CLI. The TOE maintains a security domain using the appliance hardware running the AsyncOS. The TOE is protected from external physical interference or tampering by virtue of it being installed in a controlled access facility where it is protected from unauthorized physical access. Additionally, the TOE provides separate physical network interfaces to separate network traffic via either the L4 Traffic Monitor or Web Proxy server configuration generated by web users on one network to another, and vice-versa. The TOE appliance is placed inside the firewall on the network being monitored. The TOE provides reliable timestamps for its own use.

Authorized administrators are only allowed to connect to the CLI via a dedicated management network. The dedicated management network must also be used to connect to the TOE GUI via which users must logon using a secure HTTPS browser interface.

The TOE downloads signature updates in an encrypted form over HTTP. These signature updates are then decrypted and verified using either a SHA1 (160 bit) or MD5 (128 bit) hash algorithm in order to ensure their integrity. The decryption and verification of the signature updates is performed by the TOE's Dynamic Vectoring and Streaming (DVS) engine which is an anti-malware scanning engine.

In the evaluated configuration, no additional software is authorized for installation onto the TOE appliances and the appliance devices are locked down such that it is configured only to support IronPort WSA functionality.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_ITI.1: The TOE detects modifications of all TSF data during transmission between a remote trusted IT product (an update server) and the TSF and will ignore and request the originating trusted product to send the TSF data again if modifications are detected.
- FPT_RVM.1: The TOE ensures that TSP enforcement functions are invoked and succeed before each function is allowed to proceed. Authorized administrators must successfully log on with valid user identity and password in order to access TSF.
- FPT_SEP.1: The TOE provides a security domain for its own use within the appliance device.
- FPT_STM.1: The TOE correlates collected network traffic event data using time stamps provided by its appliance hardware component running AsyncOS.

6.1.5 Intrusion Detection System

The TOE provides signature analysis of web traffic with the help of an internal database of Webroot signatures. Webroot signatures identify web-based spyware and malware. These signatures are updated periodically via a secure connection to IronPort Systems update servers. The TOE also maintains and performs real-time statistical and integrity analysis on data within the network and provides the following type of monitoring/reporting information where an authorized Administrator can manage:

- System Overview—client transactions, bandwidth, response time (in milliseconds) and total number of connections.
- Security Services Summary—Web Proxy transactions and L4 Traffic Monitor connections.

- Top Sites by Malware—monitored and blocked.
- Malware Categories Detected—monitored and blocked.
- WSA Status—system uptime and system resource utilization.
- Proxy Traffic Characteristics—transactions per second, bandwidth, response time (in milliseconds), cache hits and connections.
- Current Configuration—Web Proxy, L4 Traffic Monitor and WSA version information.
- L4 Traffic Monitor—top malware ports and sites detected.
- Client Activity—Web Proxy: top clients by malware detected; and L4 Traffic Monitor: Top clients by malware detected.
- Anti-Malware—malware categories detected and top malware threats detected.
- Web Reputation Filters—web reputation actions and web reputation scores and actions.

Alerts are generated for the attacks listed above on the System Reports page of the console. These are available for view by all authorized users of the TOE. An authorized Administrator can configure the TOE to automatically generate e-mail alerts to signal that the TOE is experiencing abnormal conditions that provides severity levels (i.e., Info, Warning, Critical) for Web Proxy; Web Reputation Filter; DVS and Anti-Malware; L4 Traffic Monitor; System; Hardware and/or Updater. E-mail alerts can be configured to be sent to one or more authorized Administrators.

Web Reputation Filtering

The TOE provides default Web Reputation Filtering scores as shown in the following table:

Table 7 – Default Reputation Filtering Scores

Score	Action	Description	Example
-10 to -5.0	Block	Bad site; request is blocked and no further scanning occurs.	• URL downloads information without user permission • Sudden spike in URL volume • URL is a typo of a popular domain
-4.9 to 4.9	Scan	Gray site; request is passed to the DVS engine for further scanning. The DVS engine scans request and server response content.	• Recently created URL that has a dynamic IP address and contains downloadable content. • Network owner IP address that has a positive SenderBase Reputation Score (SBRS).
5.0 to 10.0	Allow	Good site; request is allowed, no scanning required.	• URL contains no downloadable content. • Reputable, high-volume domain with long history. • Domain present on several allow lists. • No links to URLs with poor reputations

Threshold settings for web reputation scoring are flexible and can be modified by an authorized Administrator to other than the aforementioned default by accessing Security Services Web—Web Reputation Filters—Edit Web Reputation Filters Settings.

L4 Traffic Monitor

By default, the L4 Traffic Monitor is set to monitor traffic on all ports during initial TOE setup and an authorized Administrator can use the Security Services tab—L4 Traffic Monitor page to enable L4 Traffic Monitor after initial configuration or to modify existing settings: The following table provides setting options:

Table 8 – L4 Traffic Monitor Options

Options	L4 Traffic Monitor Configurations
Monitor ports	• Monitor all ports for rogue activity (this is the default setting). • Monitor non-proxy ports only (effectively stops malware attempts to bypass Port 80).
Action	• Monitor only—scans all traffic for domains and IP addresses that match entries in the L4 Traffic Monitor database. Monitor only does not block suspicious traffic. This setting is usefully for identifying infected clients without affecting the user experience. • Monitor and block—scans all traffic for domains and IP addresses that match entries in the appliance administrative lists, and block list database. This setting is useful for identifying infected clients, and stopping malware attempts through non-standard ports, meaning ports other than proxy ports.
L4 Traffic Monitor Block List (optional)	L4 Traffic Monitor administrative block list where an authorized Administrator enters known IP addresses for the L4 Traffic Monitor to block or monitor using the L4 Traffic Monitor Block List field

Note— the L4 Traffic Monitor is configured to monitor and block, the L4 Traffic Monitor and the Web Proxy must be configured on the same network to confirm that all clients are accessible on routes that are configured for data traffic.

As the TOE sits on the network behind the firewall, all traffic entering and leaving the protected network pass through the TOE for monitoring and/or action(s), as configured.

The Intrusion Detection System function is designed to satisfy the following security functional requirements:

- IDS_ANL.1 (EXP): The TOE performs signature and integrity analysis, detection of malware, application of content filters on collected and real-time web network traffic and records corresponding event data. The TOE records within the analytical results the data and time of the result, type of result and identity of the malware/spyware.
- IDS_RCT.1 (EXP): The TOE provides the ability to generate alarms at the console when a malware intrusion is detected within the network and notify administers via e-mail alerts at an Authorized administrator-configurable recurrence. The TOE also provides the ability to automatically block or allow web access based on rule configuration when a malware intrusion is detected.
- IDS_RDR.1 (EXP): The TOE provides the ability to review results from malware IDS scanning, sensing and analyzing tasks (e.g., System data) using a web-based interface provided by the TOE that can produce eXtensible Markup Language (XML)-formatted reports by restricting access to administrator interfaces (i.e., web-based GUI and optionally, via command line). The only users that may read system data must be assigned to one of the roles/groups as identified in Section 6.1.3 and all such users are authorized by the TOE. The TOE does not allow anyone else to access system data.
- IDS_SDC.1 (EXP): The TOE collects network traffic data for use in scanning, sensing and analyzing functions, acting as an IDS scanner for malware/spyware attempting to enter or exit the network. The TOE collects data and time of the event, type of the event, subject identity and the outcome (success or failure) of the event; and network traffic information including protocol, source address and destination address.
- IDS_STG.1(EXP): The TOE ensures the most recent of at least 10 MB per log file of system data events are always able to be recorded by overwriting the oldest events stored in the database tables when system data storage space is exhausted. The default log size is 10MB before the log is rolled over. The TOE supports up to 100MB of space for the log files. Therefore, it is possible to have the current log file and nine rolled over (saved) log files before any rolled over log is overwritten.
- IDS_STG.2 (EXP): The TOE prevents loss in new/current event data by overwriting the oldest events stored in the logs when the system data storage capacity is exhausted. When this occurs, an alarm is generated and sent to an authorized Administrator using a configured notification mechanism (e.g., e-mail alert).

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by IronPort ensure that configuration items are uniquely identified, and that documented procedures are used to control and track changes that are made to the TOE. IronPort performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, and the CM documentation.

These activities are documented in:

- IronPort Configuration Management Plan

The Configuration management assurance measure satisfies the following EAL 2 assurance requirements:

- ACM_CAP.2

6.2.2 Delivery and operation

IronPort provides delivery documentation and procedures to identify the TOE, secure the TOE during delivery, and provide necessary installation and generation instructions. IronPort's delivery procedures describe all applicable procedures to be used to prevent in appropriate access to the TOE. IronPort also provides documentation that describes the steps necessary to install WSA in accordance with the evaluated configuration.

These activities are documented in:

- IronPort Delivery Procedures
- Cisco IronPort S-Series Web Security Appliance running AsyncOS™ 5.6.1 COMMON CRITERIA GUIDE for IronPort Appliances
- IronPort AsyncOS™ 5.6.1 RELEASE NOTES for Web Security Appliances
- Networking Worksheet IronPort S-Series Web Security Appliance (Quick Start Guide)

The Delivery and operation assurance measure satisfies the following EAL 2 assurance requirements:

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

IronPort has documents describing all facets of the design of the TOE. These documents serve to describe the security functions of the TOE, its interfaces both external and between subsystems, the architecture of the TOE (in terms of subsystems), and correspondence between the available design abstractions (including the ST).

These activities are documented in:

- Cisco IronPort S-Series Web Security Appliance Design Document (HLD, FSP, and RCR)

The Development assurance measure satisfies the following EAL 2 assurance requirements:

- ADV_FSP.1
- ADV_HLD.1
- ADV_RCR.1

6.2.4 Guidance documents

IronPort provides administrator and user guidance on how to utilize the TOE security functions and warnings to administrators and users about actions that can compromise the security of the TOE.

These activities are documented in:

- ASYNCOS™ 5.6.1 USER GUIDE for Web Security Appliances

The Guidance documents assurance measure satisfies the following EAL 2 assurance requirements:

- AGD_ADM.1
- AGD_USR.1

6.2.5 Tests

The test documents describe the overall test plan, testing procedures, the tests themselves, including expected and actual results. In addition, these documents describe how the functional specification has been appropriately tested.

These activities are documented in:

- Cisco IronPort S Series Web Security Appliance Test Document (FUN and COV) EDCS-767742
- Test Case mapping Table

The Tests assurance measure satisfies the following EAL 2 assurance requirements:

- ATE_COV.1
- ATE_FUN.1
- ATE_IND.2

6.2.6 Vulnerability assessment

IronPort has conducted a Strength of Function (SOF) analysis wherein all permutational or probabilistic security mechanisms have been identified and analyzed resulting in a demonstration that all of the relevant mechanisms fulfill the minimum strength of function claim, SOF-Basic).

IronPort performs regular vulnerability analyses of the entire TOE (including documentation) to identify weaknesses that can be exploited in the TOE.

These activities are documented in:

- IronPort Strength of Function Analysis
- IronPort Vulnerability Analysis

The Vulnerability assessment assurance measure satisfies the following EAL 2 assurance requirements:

- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

This ST conforms to the U.S. Government IDSSPP, Version 1.6 where all SFRs have been copied exactly as the Common Criteria (CC) Part 2 and IDSSPP in Section 5.1 with the following exceptions.

Table 9 – ST SFRs vice PP SFRs

Requirement Component	Modification of Security Functional and Security Assurance Requirements
FAU_GEN.1	• Selection – incorporated the IDSSPP selection of 'basic' • Assignment – incorporated the IDSSPP assignment of 'Access to the System and access to the TOE and System data' • Assignment – incorporated the IDSSPP assignment of 'the additional information specified in the Details column of Table 2 Auditable Events' • Refinement – refined the IDSSPP assignment by replacing 'Table 2 Auditable Events' with 'following table' as the table is not Table 2 within this ST • Moved Table 2 to after FAU_GEN.1.2 as the IDSSPP had it incorrectly reflected after FAU_GEN.1.1 • Added table caption as 'Table 4 – Auditable Events' • Added FMT_MTD.1 iterations (a-d) to Table 4 to address the STs iterations of this SFR
FAU_SAR.1	• Assignment – completed the IDSSPP assignment of authorized users as 'authorized Administrators' • Assignment – completed the IDSSPP assignment list of audit information as 'all audit information'
FAU_SAR.2	No change
FAU_SAR.3	• Selection – incorporated the IDSSPP selection 'sorting' • Assignment – incorporated the IDSSPP assignment of 'date and time, subject identity, type of event, and successor failure of related event'
FAU_SEL.1	• Selection – incorporated the IDSSPP selection 'event type' • Assignment – completed the IDSSPP assignment as 'no additional attributes'
FAU_STG.2	• Selection – incorporated the IDSSPP assignment 'detect' • Assignment – completed the IDSSPP selection as 'at least 10MB per log file' • Selection – completed the IDSSPP selection as 'audit storage exhaustion'
FAU_STG.4	• Selection – completed the IDSSPP selection as 'overwrite the oldest stored audit records' • Assignment – completed the CC assignment as 'send an alarm' where the IDSSPP incorrectly reflected this using the selection convention
FIA_AFL.1	Removed – TOE does not communicate with remote IT products (see note below regarding PD 0097)
FIA_ATD.1	Assignment - completed the CC assignments as: • User identity; • Authentication data; • Authorizations; and • Role Note: IDSSPP erroneously identified a) – c) as selections per the IDSSPP conventions; however, as the CC, Part 2, identifies all as an assignment, the ST has included all as one assignment and included the IDSSPP alphabetized listing Note: U.S. English used to reflect the IDSSPP 'authorisations' in ST, as authorized
FIA_UAU.2	Replaced – added higher level component that is hierarchical to IDSSPP specified and therefore fully satisfies
FIA_UID.2	Replaced – added higher level component that is hierarchical to IDSSPP specified and therefore fully satisfies

Requirement Component	Modification of Security Functional and Security Assurance Requirements
FMT_MOF.1	• Selection – incorporated the IDSSPP selection 'modify the behavior' [Note: the IDSSPP erroneously excluded 'of' at the end of the CC selection such that the ST reflects correctly as 'modify the behavior of'] • Assignment – incorporated the IDSSPP assignment of System data collection, analysis and reaction' • Assignment – incorporated the IDSSPP assignment 'authorized System Administrators' [Assignment refinement – refined System Administrators to 'System Administrator' as the TOE has one and added 'authorized Administrators' to reflect that the TOE only has one System Administrator and other authorized Administrators that can perform management of security functions behavior]
FMT_MTD.1a	• Iterated to address all TOE management restrictions based on authorizations and role assigned • Selection – incorporated the IDSSPP selection 'query' and added additional selections 'modify, delete, clear' to reflect all TOE TSF management abilities • Assignment – incorporated the IDSSPP additional assignment list of TSF data 'and add System and audit data, and shall restrict the ability to query and modify all other TOE data' [Assignment refinement – refined the IDSSPP assignment to further clarify (i.e., configuration settings and assign users to groups' as part of the assignment to completely reflect the role being conveyed] • Assignment – completed the IDSSPP assignment of the authorized identified roles as 'System Administrator'
FMT_MTD.1b	• Added iteration to address all TOE management restrictions based on role(s) • Selection – completed the CC selection as 'query, modify, delete, clear' • Assignment – completed the CC selection assignment as 'and add all System configuration settings except the ability to issue the upgrade and upgradeconfig commands and assign users to groups' • Assignment – completed the CC assignment as 'Administrators group'
FMT_MTD.1c	• Added iteration to address all TOE management restrictions based on role(s) • Selection – completed the CC selection as 'query, modify, delete, clear' • Assignment – completed the CC selection assignment as 'and add all System configuration settings except the ability to create, edit or remove user accounts and restricts the ability to issue the upgrade, upgradeconfig, resetconfig, systemset6up, and userconfig commands or running the System Setup Wizard' • Assignment – completed the CC assignment as 'Operators group'
FMT_MTD.1d	• Added iteration to address all TOE management restrictions based on role(s) • Selection – completed the CC selection as 'query' • Assignment – completed the CC selection assignment as 'system status information' • Assignment – completed the CC assignment as 'Guests group'
FMT_SMF.1	Added - this requirement was added in this ST to satisfy a dependency added to FMT_MOF.1 by CC V2.3. This requirement simply requires that security functions actually be present in addition to being protected if they are present and therefore does not impact PP conformance.
FMT_SMR.1	• Refinement – refined the CC SFR to match the IDSSPP refinement by adding "following" between 'the' and 'role' prior to assignment • Assignment - completed the assignment
FPT_ITA.1	Removed – TOE does not communicate with remote IT products (see note below regarding PD 0097)
FPT_ITC.1	Removed – TOE does not communicate with remote IT products (see note below regarding PD 0097)

Requirement Component	Modification of Security Functional and Security Assurance Requirements
FPT_ITI.1	This requirement as written in the PP was removed per PD 0097 (see note below). It was added back into the TOE to support the receipt of updates from the vendor via HTTPS. • Refinement – refined the IDSSPP requirement to reflect the communication between the external trusted IT product providing TSF system data.
FPT_RVM.1	No change
FPT_SEP.1	No change
FPT_STM.1	No change
IDS_ANL.1 (EXP)	• Selection – completed the IDSSPP selection of statistical, signature, integrity as 'signature, integrity' • Assignment – completed the IDSSPP assignment of other analytical functions as 'no additional analytical functions • Assignment – completed the IDSSPP assignment of other security relevant information about the result as 'identity of malware/spyware'
IDS_RCT.1 (EXP)	• Assignment - completed the IDSSPP assignment of alarm designation as 'authorized Administrators' • Assignment – completed the IDSSPP assignment of appropriate actions as 'determine an action to block or monitor the traffic based on configuration'
IDS_RDR.1 (EXP)	• Assignment - completed the IDSSPP assignment of authorized users as 'authorized Administrators and the authorized System Administrator' • Assignment – completed the IDSSPP assignment of list of System data as 'all data'
IDS_SDC.1 (EXP)	• Selection – completed the IDSSPP selection of startup and shutdown; identification and authentication events; data accesses; service requests; network traffic; security configuration changes; data introduction; start-up and shutdown of audit functions; detected malicious code; access control configuration; service configuration; authentication configuration; accountability policy configuration; detected known vulnerabilities to reflect all available selection options • Assignment - completed the IDSSPP assignment of other specifically defined events as 'no additional information' • Refinement – refined 'Table 3 System Events' to reflect 'the following Table' • Added table caption as 'Table 5 – System Events' to the IDSSPP table
IDS_STG.1 (EXP)	• Assignment – completed the IDSSPP assignment of metric for saving System data as 'at least 10 MB per log file' • Selection – completed the IDSSPP selection of System data storage exhaustion, failure, attack as 'System data storage exhaustion'
IDS_STG.2 (EXP)	Selection – completed the selection of ignore System data, prevent System data, except those taken by the authorized user with special rights, overwrite the oldest stored System data as 'overwrite the oldest stored System data'

TOE Security Objective: Removed O.EXPORT (see note below regarding PD 0097)

TOE Security Objective: Added O.IMPORT to support the TOEs ability to verify the integrity of TOE data imported by the TOE via a remote trusted IT product (ie. an update server)

Security Assurance Requirements: reflected the CC, Part 2 assurance components of ACM as the IDSSPP was not current/complete (i.e., IDSSPP does not include ACM_CAP.2.7c and therefore ACM_CAP.2.4c through ACM_CAP.2.6c were incorrect/incomplete) where the ST properly includes:

- **ACM_CAP.2.4c** The configuration list shall uniquely identify all configuration items that comprise the TOE.
- **ACM_CAP.2.5c** The configuration list shall describe the configuration items that comprise the TOE.
- **ACM_CAP.2.6c** The CM documentation shall describe the method used to uniquely identify the configuration items.
- **ACM_CAP.2.7c** The CM system shall uniquely identify all configuration items.

NOTE: Removal and/or not reflecting FIA_AFL.1, FPT_ITA.1, FPT_ITC.1and O.EXPORT are authorized per Precedent Decision (PD) 0097 as the PP author's intent for the concept of "remote IT product" was at the component level and an IDS does not communicate with other IDS components outside of the IDS system.

A separate instance of FPT_ITI.1 was added back in only to protect the communications between the TOE and the signature update server in the IT Environment of the TOE.

Rationale

This section provides the rationale for completeness and consistency of the ST. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Strength of Functions;
- Requirement Dependencies;
- TOE Summary Specification; and,
- PP Claims.

7.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat. Note that rationale has been taken directly from the IDSSPP and no changes have been made, other than to address IDSSPP deviations reflected in Section 7.

7.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of assumptions, threats and organizational policies by the security objectives.

Table 10 - Environment to Objective Correspondence

Assumptions, Threats and Organizational Security Policies	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP	O.IMPORT
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.NOTRUST													X	X			
T.COMINT	X						X	X			X						
T.COMDIS	X						X	X									
T.LOSSOF	X						X	X			X						
T.NOHALT		X	X	X			X	X									
T.PRIVIL	X						X	X									
T.IMPCON						X	X	X				X					X
T.INFLUX									X								
T.FACCNT										X							
T.SCNCFG		X															
T.SCNMLC		X															
T.SCNVUL		X															

Assumptions, Threats and Organizational Security Policies	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.INSTAL	O.PHYCAL	O.CREDEN	O.PERSON	O.INTROP	O.IMPORT
T.FALACT					X												
T.FALREC				X													
T.FALASC				X													
T.MISUSE			X														
T.INADVE			X														
T.MISACT			X														
P.DETECT		X	X							X							
P.ANALYZ				X													
P.MANAGE	X					X	X	X				X		X	X		
P.ACCESS	X						X	X									
P.ACCACT								X		X							
P.INTGTY											X						
P.PROTCT									X				X				

7.1.1.1 A.ACCESS

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

This Assumption is satisfied by ensuring that:

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

7.1.1.2 A.ASCOPE

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

This Assumption is satisfied by ensuring that:

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

7.1.1.3 A.DYNMIC

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

This Assumption is satisfied by ensuring that:

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

7.1.1.4 A.LOCATE

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

This Assumption is satisfied by ensuring that:

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

7.1.1.5 A.MANAGE

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

This Assumption is satisfied by ensuring that:

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

7.1.1.6 A.NOEVIL

The authorized Administrator are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

This Assumption is satisfied by ensuring that:

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

7.1.1.7 A.NOTRST

The TOE can only be accessed by authorized users.

This Assumption is satisfied by ensuring that:

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

7.1.1.8 A.PROTCT

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

This Assumption is satisfied by ensuring that:

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

7.1.1.9 T.COMDIS

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

This Threat is satisfied by ensuring that:

- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE data.
- O.IDAUTH: The O.IDAUTH objective provides for authentication of users prior to any TOE data access.
- O.PROTCT: The O.PROTCT objective addresses this threat by providing TOE self-protection.
- OE.PROTECT: The OE.PROTECT objective counters this policy by requiring the IT environment to protect itself and the TOE from interference and tampering.

7.1.1.10 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.

This Threat is satisfied by ensuring that:

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

7.1.1.11 T.FACCNT

Unauthorized attempts to access TOE data or security functions may go undetected.

This Threat is satisfied by ensuring that:

- O.AUDITS: The O.AUDITS objective counters this threat by requiring the TOE to audit attempts for data accesses and use of TOE functions.

7.1.1.12 T.FALACT

The TOE may fail to react to identified or suspected vulnerabilities or inappropriate activity.

This Threat is satisfied by ensuring that:

- O.RESPON: The O.RESPON objective ensures the TOE reacts to analytical conclusions about suspected vulnerabilities or inappropriate activity.

7.1.1.13 T.FALASC

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

This Threat is satisfied by ensuring that:

- O.IDANLZ: The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources.

7.1.1.14 T.FALREC

The TOE may fail to recognize vulnerabilities or inappropriate activity based on IDS data received from each data source.

This Threat is satisfied by ensuring that:

- O.IDANLZ: The O.IDANLZ objective provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source.

7.1.1.15 T.IMPCON

An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.

This Threat is satisfied by ensuring that:

- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
- O.EADMIN: The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product.
- O.IDAUTH: The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses.
- O.INSTAL: The O.INSTAL objective states the authorized Administrator will configure the TOE properly.
- O.IMPORT: The O.IMPORT objective ensures that updates to TOE system data are verified in transit between a remote trusted IT product and the TOE.

7.1.1.16 T.INADVE

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

This Threat is satisfied by ensuring that:

- O.AUDITS: The O.AUDITS objective addresses this threat by requiring a TOE to collect audit data.
- O.IDSENS: The O.IDSENS objective addresses this threat by requiring a TOE, that contains a Sensor, to collect Sensor data.

7.1.1.17 T.INFLUX

An unauthorized user may cause malfunction of the TOE by creating an influx of data that the TOE cannot handle.

This Threat is satisfied by ensuring that:

- O.OFLOWS: The O.OFLOWS objective counters this threat by requiring the TOE handle data storage overflows.

7.1.1.18 T.LOSSOF

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

This Threat is satisfied by ensuring that:

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

7.1.1.19 T.MISACT

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

This Threat is satisfied by ensuring that:

- O.AUDITS: The O.AUDITS objective addresses this threat by requiring a TOE to collect audit data.
- O.IDSENS: The O.IDSENS objective addresses this threat by requiring a TOE, that contains a Sensor, to collect Sensor data.

7.1.1.20 T.MISUSE

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

This Threat is satisfied by ensuring that:

- O.AUDITS: The O.AUDITS objective addresses this threat by requiring a TOE to collect audit data.
- O.IDSENS: The O.IDSENS objective addresses this threat by requiring a TOE, that contains a Sensor, to collect Sensor data.

7.1.1.21 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.

This Threat is satisfied by ensuring that:

- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
- O.IDANLZ: The O.IDANLZ objective addresses this threat by requiring the TOE to analyze System data, which includes attempts to halt the TOE.
- O.IDAUTH: The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses.
- O.IDSCAN: The O.IDSCAN objective addresses this threat by requiring the TOE to collect System data, which includes attempts to halt the TOE.
- O.IDSENS: The O.IDSENS objective addresses this threat by requiring the TOE to collect System data, which includes attempts to halt the TOE.

7.1.1.22 T.PRIVIL

An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

This Threat is satisfied by ensuring that:

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

7.1.1.23 T.SCNCFG

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

This Threat is satisfied by ensuring that:

- O.IDSCAN: The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a configuration setting change.

7.1.1.24 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.

This Threat is satisfied by ensuring that:

- O.IDSCAN: The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of malicious code. The ST will state whether this threat must be addressed by a Scanner.

7.1.1.25 T.SCNVUL

Vulnerabilities may exist in the IT System the TOE monitors.

This Threat is satisfied by ensuring that:

- O.IDSCAN: The O.IDSCAN objective counters this threat by requiring a TOE, that contains a Scanner, collect and store static configuration information that might be indicative of a vulnerability. The ST will state whether this threat must be addressed by a Scanner.

7.1.1.26 P.ACCACT

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

This Organizational Policy is satisfied by ensuring that:

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

7.1.1.27 P.ACCESS

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

This Organizational Policy is satisfied by ensuring that:

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

7.1.1.28 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.

This Organizational Policy is satisfied by ensuring that:

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

7.1.1.29 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.

This Organizational Policy is satisfied by ensuring that:

- O.AUDITS: The O.AUDITS objective addresses this policy by requiring collection of audit data.
- O.IDSCAN: The O.IDSCAN objective addresses this policy by requiring collection of Scanner data.
- O.IDSENS: The O.IDSENS objective addresses this policy by requiring collection of Sensor data.

7.1.1.30 P.INTGTY

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

This Organizational Policy is satisfied by ensuring that:

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

7.1.1.31 P.MANAGE

The TOE shall only be managed by authorized users.

This Organizational Policy is satisfied by ensuring that:

- O.ACCESS: The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions.
- O.EADMIN: The O.EADMIN objective ensures there is a set of functions for administrators to use.
- O.IDAUTH: The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses.
- O.PROTCT: The O.PROTCT objective addresses this policy by providing TOE self-protection.
- O.CREDEN: The O.CREDEN objective requires administrators to protect all authentication data.
- O.INSTAL: The O.INSTAL objective supports the O.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy.
- O.PERSON: The O.PERSON objective ensures competent administrators will manage the TOE.

7.1.1.32 P.PROTCT

The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

This Organizational Policy is satisfied by ensuring that:

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

7.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the ST. Note that the following table indicates the requirements that effectively satisfy the individual objectives. Note that the rationale contained herein has been copied from the IDSSPP.

7.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

Table 11 – SFR to Security Objective Mapping

SFR	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.IMPORT
FAU_GEN.1										X		
FAU_SAR.1						X						
FAU_SAR.2							X	X				
FAU_SAR.3						X						
FAU_SEL.1						X				X		
FAU_STG.2	X						X	X	X		X	
FAU_STG.4									X	X		
FIA_UAU.2							X	X				
FIA_ATD.1								X				
FIA_UID.2							X	X				
FMT_MOF.1	X						X	X				
FMT_MTD.1a-d	X						X	X			X	
FMT_SMF.1						X	X			X		
FMT_SMR.1								X				
FPT_RVM.1	X										X	
FPT_SEP.1	X					X		X		X	X	
FPT_STM.1										X		
IDS_SDC.1 (EXP)		X	X									
IDS_ANL.1 (EXP)				X								
IDS_RCT.1 (EXP)					X							
IDS_RDR.1 (EXP)						X	X	X				
IDS_STG.1 (EXP)	X						X	X	X		X	
IDS_STG.2 (EXP)									X			
FMT_SMF.1	X						X	X		X	X	
FPT_ITI.1												X

7.2.1.1 O.PROTCT

The TOE must protect itself from unauthorized modifications and access to its functions and data.

This TOE Security Objective is satisfied by ensuring that:

- FAU_STG.2: 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.
- FMT_MOF.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_MTD.1a-d: Only authorized Administrators of the System may query and add System and audit data, and authorized Administrators of the TOE may query and modify all other TOE data.
- FMT_SMF.1: The TOE is required to perform security management functions to manage functions related to system data collection, analysis and reaction, system configuration, audit data and users.
- IDS_STG.1(EXP): 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.

- FPT_RVM.1: The must ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
- FPT_SEP.1: The TSF must be protected from interference that would prevent it from performing its functions.

7.2.1.2 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.

This TOE Security Objective is satisfied by ensuring that:

- IDS_SDC.1(EXP): A System containing a Scanner is required to collect and store static configuration information of an IT System. The type of configuration information collected are defined in the ST.

7.2.1.3 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.

This TOE Security Objective is satisfied by ensuring that:

- IDS_SDC.1(EXP): 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. These events are defined in the ST.

7.2.1.4 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).

This TOE Security Objective is satisfied by ensuring that:

- IDS_ANL.1(EXP): The Analyzer is required to perform intrusion analysis and generate conclusions.

7.2.1.5 O.RESPON

The TOE must respond appropriately to analytical conclusions.

This TOE Security Objective is satisfied by ensuring that:

- IDS_RCT.1(EXP): The TOE is required to respond accordingly in the event an intrusion is detected.

7.2.1.6 O.EADMIN

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

This TOE Security Objective is satisfied by ensuring that:

- FAU_SAR.1: The TOE must provide the ability to review the audit trail of the System.
- FAU_SAR.3: The TOE must provide the ability to manage the audit trail of the System.
- FAU_SEL.1: The TOE must provide the ability to manage the audit trail of the System.
- FMT_SMF.1: The TOE is required to perform security management functions to manage functions related to system data collection, analysis and reaction, system configuration, audit data and users.
- IDS_RDR.1(EXP): The System must provide the ability for authorized Administrator to view all System data collected and produced.
- FPT_SEP.1: The TSF must be protected from interference that would prevent it form performing its functions.

7.2.1.7 O.ACCESS

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

This TOE Security Objective is satisfied by ensuring that:

- FAU_SAR.2: The TOE is required to restrict the review of audit data to those granted with explicit read-access.
- FAU_STG.2: 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.
- FIA_UAU.2: Users authorized to access the TOE are defined using an authentication process.
- FIA_UID.2: Users authorized to access the TOE are defined using an identification process.
- FMT_MOF.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_MTD.1a-d: Only authorized Administrator of the System may query and add System and audit data, and authorized Administrator of the TOE may query and modify all other TOE data.
- FMT_SMF.1: The TOE is required to perform security management functions to manage functions related to system data collection, analysis and reaction, system configuration, audit data and users.
- IDS_RDR.1(EXP): The System is required to restrict the review of System data to those granted with explicit read-access.
- IDS_STG.1(EXP): The System is required to protect the System data from any modification and unauthorized deletion.

7.2.1.8 O.IDAUTH

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

This TOE Security Objective is satisfied by ensuring that:

- FAU_SAR.2: The TOE is required to restrict the review of audit data to those granted with explicit read-access.
- FAU_STG.2: The TOE is required to protect the stored audit records from unauthorized deletion.
- FIA_ATD.1: Security attributes of subjects use to enforce the authentication policy of the TOE must be defined.
- FIA_UAU.2: Users authorized to access the TOE are defined using an authentication process.
- FIA_UID.2: Users authorized to access the TOE are defined using an identification process.
- FMT_MOF.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_MTD.1a-d: Only authorized Administrator of the System may query and add System and audit data, and authorized Administrator of the TOE may query and modify all other TOE data.
- FMT_SMR.1: The TOE must be able to recognize the different administrative and user roles that exist for the TOE.
- IDS_RDR.1(EXP): The System is required to restrict the review of System data to those granted with explicit read-access.
- IDS_STG.1(EXP): 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.
- FPT_SEP.1: The TSF must be protected from interference that would prevent it from performing its functions.

7.2.1.9 O.OFLOWS

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

This TOE Security Objective is satisfied by ensuring that:

- FAU_STG.2: 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.4: The TOE must prevent the loss of audit data in the event the its audit trail is full.
- IDS_STG.1(EXP): 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.2(EXP): The System must prevent the loss of audit data in the event the its audit trail is full.

7.2.1.10 O.AUDITS

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

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: Security-relevant events must be defined and auditable for the TOE.
- FAU_SEL.1: The TOE must provide the capability to select which security-relevant events to audit.
- FAU_STG.4: The TOE must prevent the loss of collected data in the event the its audit trail is full.
- FMT_SMF.1: The TOE is required to perform security management functions to manage functions related to system data collection, analysis and reaction, system configuration, audit data and users.
- FPT_STM.1: Time stamps associated with an audit record must be reliable.
- FPT_SEP.1: The TSF must be protected from interference that would prevent it from performing its functions.

7.2.1.11 O.INTEGR

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

This TOE Security Objective is satisfied by ensuring that:

- FAU_STG.2: 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.
- FMT_MTD.1a-d: Only authorized Administrator of the System may query or add audit and System data.
- FMT_SMF.1: The TOE is required to perform security management functions to manage functions related to system data collection, analysis and reaction, system configuration, audit data and users.
- IDS_STG.1(EXP): The System is required to protect the System data from any modification and unauthorized deletion.
- FPT_RVM.1: The must ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
- FPT_SEP.1: The TSF must be protected from interference that would prevent it from performing its functions.

7.2.1.12 O.IMPORT

When a remote trusted IT product makes TSF system data available to an IDS component, the TOE will ensure the integrity of the TSF system data.

This TOE Security Objective is satisfied by ensuring that:

- FPT_ITI.1: The TSF shall detect modifications and verify the integrity of all TSF data transmitted between a remote trusted IT product and the TSF.

7.3 Security Assurance Requirements Rationale

EAL2 was chosen as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. IronPort WSA is targeted at a relatively benign environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have little attack potential. The chosen assurance level is appropriate with the threats and assumptions defined for the environment. As such, EAL2 is appropriate to provide the assurance necessary to counter the limited potential for attack.

7.4 Strength of Functions Rationale

The TOE minimum Strength of Function (SOF) is Basic (SOF-Basic). The rationale for the SOF is based on the low attack potential and the need to protect against the relatively benign environment with good physical access security and competent administrators. SOF-Basic is therefore selected as the evaluated TOE is intended to operate in commercial and DoD environments processing unclassified but sensitive information. This security function is in

turn consistent with the security objectives described in Section 4. Further, SOF-Basic was chosen to address the password mechanism that implements the FIA_UAU.2 (User authentication before any action) requirement that contains the only permutational mechanism in the TOE. FIA_UAU.2 instantiated by the identification and authentication function is the only requirement in the TOE that necessitates a SOF claim.

7.5 Requirement Dependency Rationale

The following table reflects the CC-required dependencies being satisfied in this ST.

Table 12 – Requirement Dependencies Satisfied

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1 and FMT_MTD.1	FAU_GEN.1 and FMT_MTD.1
FAU_STG.2	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	*FAU_STG.2*
FIA_ATD.1	none	none
FIA_UAU.2	FIA_UID.1	*FIA_UID.2*
FIA_UID.2	none	none
FMT_MOF.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1a	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1b	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1c	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_MTD.1d	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	*FIA_UID.2*
IDS_ANL.1 (EXP)	none	none
IDS_RCT.1 (EXP)	none	none
IDS_RDR.1 (EXP)	none	none
IDS_SDC.1 (EXP)	none	none
IDS_STG.1 (EXP)	none	none
IDS_STG.2 (EXP)	none	none
FPT_RVM.1	none	none
FPT_SEP.1	none	none
FPT_STM.1	none	none
FPT_ITI.1	none	none
ACM_CAP.2	none	none
ADO_DEL.1	none	none
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.1	ADV_FSP.1 and ADV_RCR.1	ADV_FSP.1 and ADV_RCR.1
ADV_RCR.1	none	none
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1
ATE_COV.1	ADV_FSP.1 and ATE_FUN.1	ADV_FSP.1 and ATE_FUN.1
ATE_FUN.1	none	none
ATE_IND.2	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1	ADV_FSP.1 and AGD_ADM.1 and AGD_USR.1 and ATE_FUN.1
AVA_SOF.1	ADV_FSP.1 and ADV_HLD.1	ADV_FSP.1 and ADV_HLD.1
AVA_VLA.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1	ADV_FSP.1 and ADV_HLD.1 and AGD_ADM.1 and AGD_USR.1

7.6 Explicitly Stated Requirements Rationale

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.

7.7 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. The following table demonstrates the relationship between security requirements and security functions.

Table 13 – Security Functions vs. Requirements Mapping

	Security Audit	User data protection	Identification and Authentication	Security Management	Protection of the TSF	Intrusion Detection System
FAU_GEN.1	X					
FAU_SAR.1	X					
FAU_SAR.2	X					
FAU_SAR.3	X					
FAU_SEL.1	X					
FAU_STG.2	X					
FAU_STG.4	X					
FIA_ATD.1			X			
FIA_UAU.2			X			
FIA_UID.2			X			
FMT_MOF.1				X		
FMT_MTD.1a				X		
FMT_MTD.1b				X		
FMT_MTD.1c				X		
FMT_MTD.1d				X		
FMT_SMF.1				X		
FMT_SMR.1				X		
FPT_RVM.1					X	
FPT_SEP.1					X	
FPT_STM.1					X	
FPT_ITI.1					X	
IDS_ANL.1 (EXP)						X
IDS_RCT.1 (EXP)						X
IDS_RDR.1 (EXP)						X
IDS_SDC.1 (EXP)						X

	Security Audit	User data protection	Identification and Authentication	Security Management	Protection of the TSF	Intrusion Detection System
IDS_STG.1 (EXP)						X
IDS_STG.2 (EXP)						X

7.8 PP Claims Rationale

See Section 7, Protection Profile Claims.