IronPort Messaging Gateway Version 5.1.2
Security Target

Version 1.0

06/20/08

Prepared for:
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

Table of Contents

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is IronPort Systems Messaging Gateway Version 5.1.2 provided by IronPort Systems. The TOE monitors network traffic sent and received on port 25 containing SMTP email messages.

The Security Target contains the following additional sections:

- Section 2 – Target of Evaluation (TOE) Description
  This section gives an overview of the TOE, describes the TOE in terms of its physical and logical boundaries, and states the scope of the TOE.
- Section 3 – TOE Security Environment
  This section details the expectations of the environment, the threats that are countered by the TOE and IT environment, and the organizational policy that the TOE must fulfill.
- Section 4 – TOE Security Objectives
  This section details the security objectives of the TOE and IT environment.
- Section 5 – IT Security Requirements
  The section presents the security functional requirements (SFR) for the TOE and IT Environment that supports the TOE, and details the assurance requirements for EAL2.
- Section 6 – TOE Summary Specification
  The section describes the security functions represented in the TOE that satisfy the security requirements.
- Section 7 – Protection Profile Claims
  This section presents any protection profile claims.
- Section 8 – Rationale
  This section closes the ST with the justifications of the security objectives, requirements and TOE summary specifications as to their consistency, completeness, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – IronPort Messaging Gateway Version 5.1.2 Security Target

ST Version – Version 1.0

ST Date – 06/20/08

TOE Identification – IronPort Messaging Gateway system, consisting of the IronPort Systems AsyncOS version 5.1.2, IronPort Systems appliance versions C150, C350, C600, C650, X1000 and X1050.

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 Common Criteria (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 Claim: basic

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements (SFRs) – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - 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**]).
    - 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 …").
- Explicitly stated SFRs (i.e., those not found in Part 2 of the CC) are identified with "(EXP)" following the identification of the new functional class/name (i.e., Intrusion Detection System (IDS)) and the associated family descriptor. Example: Analyzer analysis (EXP) (IDS_ANL.1)
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

2. TOE Description

The TOE is IronPort Systems Messaging Gateway Version 5.1.2 running on IronPort Systems hardware appliance versions C150, C350, C600, C650, X1000 and X1050. The TOE includes server applications running on the appliance hardware that is supported in the evaluated configuration as well as the appliance hardware itself. The TOE monitors SMTP email network traffic.

The remainder of this section summarizes the TOE architecture.

2.1 TOE Overview

The TOE monitors Simple Mail Transfer Protocol (SMTP) email network traffic. The TOE monitors email network traffic in the IT environment between an external and an internal network, such that network traffic sent and received on port 25 must pass thru the TOE. The TOE provides separate physical interfaces that can be used to separate internal and external networks. The location of the TOE in the network in the IT environment in the evaluated configuration requires email network traffic pass thru the TOE. For example, an internal network will be connected to one Ethernet network interface, and an external network will be connected to another separate Ethernet network interface.

The TOE can be configured to monitor email network traffic sent from the internal network to the external network, or vice versa. The TOE limits the amount of email that suspicious senders can send; specifically, the more hostile a sender appears, the slower the rate at which they may send messages will be. The TOE implements email message filters that calculate values called *reputation scores* that the TOE uses to determine if a sender should be throttled or blocked entirely.

2.2 TOE Architecture

The TOE monitors network traffic sent and received on port 25 containing SMTP email messages by performing the following traffic analysis techniques:

- Signature analysis
- Detection of spam
- Application of content filters
- Application of virus outbreak filters

The TOE can take one or more of the following actions in order to enforce an email message policy (i.e. to enforce the implicit IDS security policy):

- Generate an email to an administrator containing an alarm
- Generate an alarm that is written to a log file that can be examined using the administrator console
- Drop the email message
- Bounce the email message
- Archive the email message
- Add a blind-carbon copied recipient to the email message
- Modify the email message

The TOE is controlled by rule sets that are specific to each analysis technique; there are administratively-configurable rule sets as follows:

- Anti-spam rules
- Content filter rules
- Virus outbreak filter rules

Anti-spam, content filter, and virus outbreak rules are each implemented as collections of TOE configuration settings that can be specified using administrator console interfaces. Rules are configured such that they are applied

to specific groups of users based on email message attributes (Envelope Recipients, Envelope Sender, From: header, or Reply-To: header) in order to perform each type of analysis as described above.

See the IDS and security management sections in the TSS for more detailed information for each of the above traffic analysis techniques, actions that can be taken to enforce email message policy, and administration of TOE security functions.

The TOE in its intended environment can be described in terms of the following components:

- **IronPort appliance hardware** – Provides runtime environment for modified BSD operating system. Includes getty administrator console interface (via the appliance serial port).
- **IronPort modified BSD operating system component** – Provides runtime environment for AsyncOS application software component. Consists of modified BSD kernel process, file system, communication facilities, and start-up facilities. Modifications limited to tuning parameters, bug fixes, optimization, removing startup commands.
- **IronPort AsyncOS application software component** – Monitors SMTP protocol email network traffic sent and received on port 25 and takes action based on administratively-configurable rules. Provides web and terminal administrator console interfaces.
- **SMTP email server application** – Used by email senders and receivers to send and receive email. Also used by the TOE to send alerts to administrators.
- **Web browser application** – Provides an environment for presenting GUI TSFI that are made accessible via the HTTP protocol.
- **Terminal application** – Provides console interfaces that are accessible using a serial connected terminal.

2.2.1 Physical Boundaries

The components that make up the TOE are:

- IronPort appliance hardware
- IronPort modified BSD operating system component
- IronPort AsyncOS application software component

The TOE relies on services provided by the following:

- SMTP email servers that are compliant with RFC 2821
- Web browser Microsoft Internet Explorer 6.02

The TOE is depicted in the diagram below in its network environment behind a firewall where it filters out everything except SMTP packets. The diagram includes box A and B which are used to represent listeners. Listeners are email processing services that are configured on a particular IP interface. The TOE uses listeners to specify criteria that messages must meet in order to be accepted and relayed to recipient hosts. Listeners only apply to email entering the IronPort appliance either from internal systems within the network (as shown via Listener B from groupware server and message generation system in the diagram below) or from the Internet (as shown via Listener A). Listener B represents the optional private listener that can be configured.

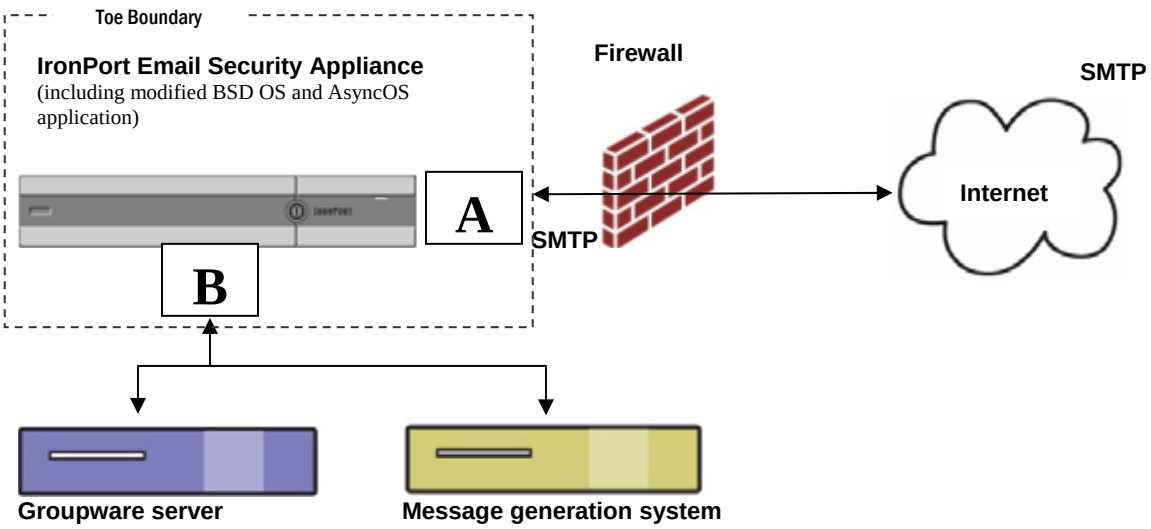

Figure 1: TOE boundary

2.2.2 Logical Boundaries

This section identifies the security functions that the TSF provides**.**

- Audit
- Identification and authentication
- Security management
- TSF protection
- Intrusion detection (EXP)

2.2.2.1 Security audit

The TOE generates audit events for the start up and shutdown of audit functions, access to the TOE and system data, all use of the authentication and identification mechanism and all modifications made to the security function configuration, to the values of TSF data and to the group of users that are part of a role. Authorized administrators and authorized system administrators can read all audit information via the TOE's GUI interface. Note that the IDS_SDC and IDS_ANL requirements address the recording of results from System data collecting and analyzing tasks.

See the corresponding section in the TSS for more detailed information.

2.2.2.2 Identification and authentication

The TOE maintains user identities, authentication data, and role information. The administrative console provides the single TOE logon mechanism for administrators to manage security functions.

See the corresponding section in the TSS for more detailed information.

2.2.2.3 Security management

The TOE restricts the ability to administer functions related to collecting and analyzing tasks. The TOE restricts the ability to manage collecting and analyzing System data) to authorized administrators.

See the corresponding section in the TSS for more detailed information.

2.2.2.4 TSF protection

The TOE prevents users from bypassing identification and authentication, roles, and audit access policies by controlling access to the administrator console and by controlling access to administrator console interfaces using username/password.

See the corresponding section in the TSS for more detailed information.

2.2.2.5 Intrusion detection (EXP)

The TOE monitors network traffic sent and received on port 25 containing SMTP email messages. The TOE performs signature analysis, detection of spam, and application of content filters on collected email network traffic and records corresponding event data.

See the corresponding section in the TSS for more detailed information.

2.3 TOE Documentation

IronPort Systems offers a series of documents that describe the installation process for the TOE, as well as guidance for subsequent use and administration of the 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 Assumptions

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

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

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

3.1.2 Physical Assumptions

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

A.LOCATE The processing resources of the TOE will be located within controlled access facilities, which 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 administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

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

3.2 Threats

The following are threats identified for 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 network traffic data received from each data source.

T.FALASC The TOE may fail to identify vulnerabilities or inappropriate activity based on association of network traffic 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 Intrusion Detection System System Protection Profile.

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

P.ANALYZ Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to system 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 system.

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 Information Technology (IT) Security Objectives

The following are the TOE security objectives:

O.EXPORT When a remote trusted IT product makes TSF system data available to the TOE, the TOE will provide a means to ensure the integrity of the TSF system data.

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

O.IDSCAN The TOE 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 TOE 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 TOE.

O.IDANLZ The TOE must accept network traffic data from targeted IT system resources and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

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

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

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

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

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

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

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

4.2 Security Objectives for the Environment

The TOE's operating environment must satisfy the following objectives. These objectives do not levy any IT requirements but are satisfied by procedural or administrative measures.

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 administrators 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

5.1 TOE Security Functional Requirements

The following table describes the SFRs from CC Part 2 as well as the explicitly stated requirements (identified with "(EXP)") that are satisfied by the TOE.

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

Table 1 TOE Security Functional Components

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 [***not specified***] level of audit; and c) [**Access to the System and access to the TOE and System data**].

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to System	
FAU_GEN.1	Access to the TOE and System data	
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.1	All modifications to the values of TSF data	

Component	Event	Details
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity

Table 2: Auditable Events

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST**, [the additional information specified in the Details column of Table 2 Auditable Events].**

5.1.1.2 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [***authorized administrators and authorized system 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 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***] modifications to the audit records.

FAU_STG.2.3 The TSF shall ensure that [**the most recent, limited by available storage space**] audit records will be maintained when the following conditions occur: [***audit storage exhaustion***]**.**

5.1.1.4 Prevention of Audit Data Loss (FAU_STG.4)

FAU_STG.4.1 The TSF shall [***overwrite the oldest stored audit records***] and [**send an email alert to an authorized administrator or system administrator**] if the audit trail is full.

5.1.2 Identification and Authentication (FIA)

5.1.2.1 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) Role; and
d) no other security attributes].

5.1.2.2 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.

5.1.2.3 User identification before any action (FIA_UID.2)

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

5.1.3 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 behaviour of***] the functions [**of System data collection, analysis and reaction**] to [**authorized System administrators**].

5.1.3.2 Management of TSF Data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [***query*** [**and add System data**]]**, and shall restrict** the [**ability to query and modify all other TOE data**] to [**authorized administrators**].

5.1.3.3 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [
a.) **Manage functions related to system data collection and analysis**
b.) **Manage users**
c.) **View audit data**]

5.1.3.4 Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the **following** roles **[authorized administrator, authorized System administrator]**.

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

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 IDS Component requirements (EXP)

5.1.5.1 Analyzer analysis (EXP) (IDS_ANL.1)

IDS_ANL.1.1 The System shall perform the following analysis function(s) on all system data received:
a) signature; and
b) the following additional traffic analysis techniques:
- Detection of spam
- Application of content filters

- Application of virus outbreak filters. (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,
b) type of result,; and
c) identification of data source. (EXP)

5.1.5.2 Analyzer react (EXP) (IDS_RCT.1)

IDS_RCT.1.1 The System shall send an email to an administrator containing an alarm and take the following actions:
a) Drop the email message
b) Bounce the email message
c) Archive the email message
d) Add a blind-carbon copied recipient to the email message
e) Modify the email message

when an intrusion is detected. (EXP)

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

IDS_RDR.1.1 The System shall provide authorized administrators with the capability to read all System 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)

5.1.5.4 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) System data; and
b) no other defined events (EXP)

IDS_SDC.1.2 At a minimum, the System shall collect and record the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) Network traffic protocol, source address and destination address.. (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 the most recent, limited by available storage space, 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.

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.

Requirement Class	Requirement Component
ACM: Configuration management	ACM_CAP.2: Configuration items

Requirement Class	Requirement Component
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

Table 3 EAL 2 Assurance Components

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 labelled 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 minimal level of audit that are stored in files in its operating system component. Authorized administrators and authorized system administrators can access and view all audit information via the TOE's web browser based GUI interface.

Each audit record includes date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. The auditable events include:

- Start-up and shutdown of the audit function
- Access to System
- Access to the TOE and System data
- 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's default installation configures the audit log files to maintain 10 files of no more than 10M for each log subscription. The user does not need to configure this. However, this value is user customizable. The user can configure each log subscription to allow 1-1000 maximum log files, and each log file can be configurable to a maximum of between 100KB and 100MB. There is no limit to the number of log subscriptions that the user can create.

With a typical configuration the log space should not grow beyond a reasonable limit. If through user customization of the log limits, the log files grow too much, alerts will be sent to the administrator when the log partition grows beyond 90% usage. Based on the model, the log partition sizes various for the different models as indicated below

Model	**Space**
C150	54GB
C350	79GB
C600	182GB
C650	181GB
X1050	181GB

6.1.1.1 Security function summary

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

- FAU_GEN.1: The TOE generates audit events for the minimal level of audit. Note that the IDS_SDC and IDS_ANL requirements address the recording of results from System data collecting and analyzing tasks.
- FAU_SAR.1: The TOE provides authorized administrators and authorized system administrators with the capability to read all audit information which is presented in a manner suitable for users to interpret and read.
- FAU_STG.2: The TOE does not provide interfaces to modify individual records. The ability to detect unauthorized modifications to audit records in the audit trail is therefore trivially met since records cannot

be modified in the first place. When the audit trail becomes full, the TOE ensures that the most recent audit records will be maintained, limited only by the available storage space.

- FAU_STG.4: The TOE generates an email alert to the authorized administrator or system administrator and begins overwriting the oldest stored audit records when the audit trail becomes full. (Note that the TOE does not stop collecting or producing System data). The alert is generated to an authorized administrator or system administrator who has been configured via the command line interface (*alertconfig* command) to receive email alerts for this event.

6.1.2 Identification and Authentication

The TOE defines users in terms of:

- user identity,
- authentication data, and
- roles.

Only authorized Administrators and the System Administrator may access TOE functions and system data and they are required to log on with a unique user ID and password in order to proceed to TOE administrative interfaces provided via the web browser and the command line interface. The TOE defines users in terms of user identity, authentication data and role and provides its own username/password authentication mechanism via a system-defined role assignment.

Users are required to enter a unique identifier and password prior to logging on either via the GUI or on the CLI. The password mechanism requires passwords to be a minimum of six (6) characters. To login to the TOE, the user provides the login name and password to the administrator console. If either the login name or the password is incorrect, the login request will fail and no administrator console functions will be made available. As result of a successful login, an administrator console session is established. As result of a successful login, commands can then be sent to the component to perform the following:

- Manage functions related to system data collection, analysis, and reaction
- Manage users, including creating user accounts

The administrator console component requires passwords to be at least six characters from the printable character set.

6.1.2.1 Security function summary

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

- FIA_ATD.1: The TOE maintains user identities, authentication data, and role information locally as part of system information (ie. in files in the operating system component). Identification and authentication information cannot be linked to or imported from other naming or authentication services on the network.
- FIA_UAU.2: The TOE offers no TSF-mediated functions until the user is authenticated. Note that the password mechanism can meet or exceed SOF-basic when passwords of the minimum length of six characters are used.
- FIA_UID.2: The TOE offers no TSF-mediated functions until the user is identified.

6.1.3 Security Management

The TOE provides both a Graphical User Interface (GUI)-based and command-line administrator console interface that are accessible using a web browser and a terminal application, respectively. These interfaces can be used by authorized Administrators to access and view all audit information, manage functions related to system data collection, analysis and reaction; log reports; manage users; as well as manage network connections. The TOE restricts access to its interfaces by requiring users to logon before allowing access to administrative interfaces.

The command line interface (CLI) is the primary interface used to administer the TOE. All administrators in the evaluated configuration are required to use the CLI to perform all TOE security management functions defined in this ST with the exception of audit review. The ability to access and view the audit records is provided by the GUI. Administrators may also monitor the TOE via the GUI. The CLI is used to perform all other security functions including configuring the IronPort appliance and managing users and intrusion detection functions. Some examples of commands that are available via the command line are as follows:

The CLI provides the authorized administrator with commands such as those shown below:

- **antispamstatus** Display Anti-Spam status
- **antispamupdate** Manually update spam definitions
- **clearchanges *or* clear** Clear changes
- **commit** Commit changes
- **deleterecipients** Delete messages from the queue
- **hostrate** Monitor activity for a particular host
- **hoststatus** Get the status of the given hostname
- **last** Display who has recently logged into the system
- **netstat** Displays network connections, routing tables, and a number of network interface statistics.
- **settime** Manually set the system clock
- **showconfig** Display all configuration values
- **who** List who is logged in
- **whoami** Display your current user id
- **alertconfig** Configure email alerts
- **aliasconfig** Configure email aliases
- **deliveryconfig** Configure mail delivery
- **dictionaryconfig** Configure content dictionaries
- **ntpconfig** Configure NTP time server
- **password or passwd** Change your password
- **userconfig** Add, edit, and remove users

Managing the membership of system roles is accomplished via the System Administration tab on the User Management page. The IronPort TOE defines three (3) groups of users: Administrators, Operators and Guests where the following pertains:

- Administrators have full access to all system configuration settings;
- Operators are restricted from creating, editing or removing user accounts and cannot use the following commands: resetconfig, upgradecheck, upgradeinstall, systemsetup or running the System Setup Wizard; and
- Guests can only view system status information.

The TOE defines two security roles: authorized administrator and authorized System administrator.. These security roles correspond with the groups defined above. The System Administrator is a member of the Administrators group but has additional privileges above all other administrative users. The TOE has one System Administrator account, by default, which cannot be deleted. All members of the Administrator's group (including the System Administrator account) are members of the "Authorized System Administrator" security role defined in this ST. All

members of the Operators group are considered members of the "Authorized Administrator" security role, as they have access to TOE data. The Guest group can only view status information and has no management capabilities.

All TOE system data is managed by administrators including email messages that have been quarantined for violating email message policy. Notifications of these quarantined messages are not to be configured to be sent to end users. Users who are assigned to the guest role must NOT be given permission to manage quarantined messages.

6.1.3.1 Security function summary

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

- FMT_MOF.1: The TOE restricts the ability to modify the behavior of the functions of System data collection, analysis and reaction by restricting access to administrator console interfaces.
- FMT_MTD.1: The TOE restricts the ability to query and add System data to authorized administrators. Note that only authorized administrators can query or modify any other types of TOE data, as well.
- FMT_SMF.1: The TOE provides authorized administrators with the ability to access and view audit information, manage functions and data related to collecting and analyzing tasks, as well as the ability to manage users.
- FMT_SMR.1:
  - Users that are members of the "administrators" group are considered part of the authorized system administrator role.
  - Users that are members of the "operators" group are considered part of the authorized administrator role.

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. The TOE appliance is placed inside the firewall on the network being monitored. The TOE provides reliable timestamps for its own use.

Administrators are only allowed to connect to the GUI interface via a dedicated management network and must logon via an HTTP browser interface to access the TOE GUI. The CLI interface is accessed via a terminal connected to the serial port of the device.

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 Context Adaptive Scanning Engine (CASE) engine which is an anti-spam 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 TOE functionality.

6.1.4.1 Security function summary

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 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: Email network traffic cannot bypass TOE IDS functions because of the appliance's physical location in the network in the IT environment. Email traffic must pass through the TOE thru its Ethernet network interface card interfaces to travel between internal and external networks. Management interfaces

cannot be bypassed in general because users are required to log in before the requested operation is allowed.

- FPT_SEP.1: The TOE maintains a security domain using appliance hardware. The TOE relies on process separation mechanisms provided by the hardware to segregate each process and to ensure protection of memory and processor context for TOE processes. Additionally, the design of the appliance prevents non-TOE software from executing on the device. The use of a hardware appliance protects the TOE from external physical interference or tampering, including providing separate physical interfaces to separate network traffic generated by SMTP email senders on one network from SMTP email receivers on another network.
- FPT_STM.1: The TOE correlates collected network traffic event data using time stamps provided by its appliance hardware component.

6.1.5 Intrusion detection (EXP)

6.1.5.1 Analyzing email messages

The TOE monitors network traffic sent and received on port 25 containing SMTP email messages based by performing the following traffic analysis techniques:

- Signature analysis
- Detection of spam
- Application of content filters
- Application of virus outbreak filters

Signature analysis consists of identifying deviations from normal patterns of behavior by examining email message attributes, e.g. comparing message content against a database of known attacks or disallowed email message features. Note that automatic network traffic signature updates are disabled in the evaluated configuration, manual administrator console interfaces must instead be used in the evaluated configuration. Also note that signature analysis is the basis for each of the above-listed analysis techniques. Each of the above-listed analysis techniques performs analysis that builds on the results of signature analysis in order to target types of known attacks or disallowed email message features.

Detection of spam consists of classifying email senders based on senders' trustworthiness, along with analyzing four types of email message attributes:

- **Email reputation** – who is sending the message
- **Message content** – what content is included in the message
- **Message structure** – how was the message constructed
- **Web reputation** – where does the call to action (within the content of an email message body) take the recipient

Application of content filters consists of using rules describing how to handle messages and attachments as they are received. Filter rules identify messages based on message or attachment content, information about the network, message envelope, message headers, or message body.

The SenderBase Reputation Service allows enterprises to identify known spam based on the connecting IP address. Messages from unknown or less reputable senders can be subjected to anti-spam scanning, and the number of messages accepted from each sender can be throttled. Email senders with the worst reputation can have their connections entirely rejected or their messages bounced. Messages are filtered using the sender's SenderBase Reputation Score (SBRS) which is returned from the SenderBase Reputation Service. The SBRS score is a numeric value assigned to an IP address based on information from the SenderBase Repuation Service which aggregates data from over 25 public blacklists and open proxy lists, and combines this data with global data from SenderBase to assign a score from -10.0 to +10.0 as follows:

-10.0 – Most likely to be a source of spam
0 – Neutral, or not enough information to make a recommendation

+10.0 – Most likely to be a trustworthy sender

The Reputation Score rule checks the SenderBase Reputation Score against the specified value. If the message does not have a SenderBase Reputation Score at all (because one was never checked for it, or because the system failed to get a response from the SenderBase Reputation Service query server), any comparison against a reputation fails (the number will not be greater than, less than, equal to, or not equal to any value).

Application of virus outbreak filters consists of using mechanisms to protect against email viruses that otherwise would be handled by the IT environment, before signatures in the IT environment have been updated in order to identify and handle a previously unseen type of virus. The TOE provides administratively-configurable rule sets that can be used to detect viruses not otherwise defined using a signature.

6.1.5.2 Enforcing email message policy

The TOE can take one or more of the following actions in order to enforce an email message policy:

- Generate an email to an administrator containing an alarm
- Drop the email message
- Bounce the email message
- Archive the email message
- Add a blind-carbon copied recipient to the email message
- Modify the email message

6.1.5.3 Managing email message policy

The TOE is controlled by rule sets that are specific to each analysis technique; there are administratively-configurable rule sets as follows:

- Anti-spam rules
- Content filter rules
- Virus outbreak filter rules

Anti-spam, content filter, and virus outbreak rules are each implemented as collections of TOE configuration settings that can be specified using administrator console interfaces. Rules are configured such that they are applied to specific groups of users based on email message attributes (Envelope Recipients, Envelope Sender, From: header, or Reply-To: header) in order to perform each type of analysis as described above. Note that the TOE provides interfaces to define anti-virus rules for use by the anti-virus scanning services performed by the IT environment.

Rules can be applied to email network traffic as follows:

- **Monitor incoming email** – by accepting connections from many external hosts and directing messages to a limited number of internal network servers.
- **Monitor outgoing email** – by accepting connections from a limited number of internal network servers and directing messages to many external mail hosts.

Note that combinations of separate appliance hardware interfaces provided by the hardware appliance are used to support the above configurations.

6.1.5.4 Security function summary

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

- IDS_SDC.1: The TOE collects and analyzes system event data. The TOE collects date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and network traffic information including protocol, source address, and destination address.
- IDS_ANL.1: The TOE performs signature analysis, detection of spam, application of content filters, and application of content filters on collected email network traffic and records corresponding event data. The

TOE records within analytical results the date and time of the result, type of result, and identification of data source.

- IDS_RCT.1: The TOE provides the ability to generate alarms and notify an authorized administrator using email when an intrusion is detected. The TOE also provides the ability to automatically pass, reject, or modify email messages based on rule configuration when an intrusion is detected.
- IDS_RDR.1: The TOE provides the ability to review results from System data collecting and analyzing tasks using text-based command-line interfaces provided by the administrator console that can produce CSV-formatted reports by restricting access to administrator console interfaces.
- IDS_STG.1: The TOE ensures that the most recent system data is always able to be recorded, when the system data storage space is exhausted, the oldest events stored in the system data store will be overwritten.
- IDS_STG.2: The TOE prevents loss in new/current event data by overwriting the oldest events stored in the log when the system data storage capacity is exhausted. When this occurs and alarm is generated and sent to the authorized administrator using a configured notification mechanism.

6.2 TOE Security Assurance Measures

6.2.1 Configuration management

The configuration management measures applied by IronPort Systems 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 Systems ensures changes to the implementation representation are controlled with the support of automated tools and that TOE associated configuration item modifications are properly controlled. IronPort Systems performs configuration management on the TOE implementation representation, design documentation, tests and test documentation, user and administrator guidance, delivery and operation documentation, vulnerability analysis documentation, configuration management documentation, and security flaws.

These activities are documented in:

- IronPort Systems 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 Systems provides delivery documentation and procedures to identify the TOE, allow detection of unauthorized modifications of the TOE and installation and generation instructions at start-up. IronPort Systems' delivery procedures describe all applicable procedures to be used to detect modification to the TOE. IronPort Systems also provides documentation that describes the steps necessary to install the TOE.

These activities are documented in:

- IronPort Systems Delivery, Installation, Generation and Start-up Procedures

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

- ADO_DEL.1
- ADO_IGS.1

6.2.3 Development

IronPort Systems has numerous documents describing all facets of the design of the TOE. In particular, they have a functional specification that describes the accessible TOE interfaces; a high-level design that decomposes the TOE architecture into subsystems and describes each subsystem and their interfaces; and, correspondence documentation

that explains how each of the design abstractions correspond from the TOE summary specification in the Security Target to the actual implementation of the TOE.

These activities are documented in:

- IronPort Systems Functional Specification
- IronPort Systems High-Level Design
- IronPort Systems Correspondence

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 Systems 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:

- IronPort Systems Administrator Guide
- IronPort Systems User Guide

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

- AGD_ADM.1
- AGD_USR.1

6.2.5 Tests

IronPort Systems has a test plan that describes how each of the necessary security functions is tested, along with the expected test results. IronPort Systems has documented each test as well as an analysis of test coverage and depth demonstrating that the security aspects of the design evident from the functional specification and high-level design are appropriately tested.

These activities are documented in:

- IronPort Systems Test Plan
- IronPort Systems Actual Test Results

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

The TOE administrator and user guidance documents describe the operation of the TOE and how to maintain a secure state. These guides also describe all necessary operating assumptions and security requirements outside the scope of control of the TOE. They have been developed to serve as complete, clear, consistent, and reasonable administrator and user references. Furthermore, IronPort Systems has conducted a misuse analysis demonstrating that the provided guidance is complete.

IronPort Systems has conducted a 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 SOF claim: SOF-Basic.

IronPort Systems 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 Systems Vulnerability Analysis

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

- AVA_SOF.1
- AVA_VLA.1

7. Protection Profile Claims

The TOE does not claim conformance to any protection profile.

8. 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.

8.1 Rationale for IT Security Objectives

This section provides a rationale for the existence of each assumption, threat, and policy statement that compose this security target. Table 5, Security Environment vs. Objectives, demonstrates the mapping between the assumptions, threats, and polices to the security objectives is complete. The following discussion provides detailed evidence of coverage for each assumption, threat, and policy.

Table 4 – Security Environment vs. Objectives

	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.EXPORT
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															
T.FALACT					X												
T.FALREC				X													
T.FALASC				X													
T.MISUSE			X														

	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.EXPORT
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				

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The O.INSTAL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDAUTH objective by only permitting authorized users to access TOE functions. The O.EXPORT objective ensures that the TOE will provide a means by which the TOE can verify the integrity of TSF data (e.g. attack signatures) being imported by the TOE.

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

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

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

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

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

The O.IDSCAN objective counters this threat by requiring the TOEr, collect and store static configuration information that might be indicative of a configuration setting change.

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

The O.IDSCAN objective counters this threat by requiring the TOE to collect and store static configuration information that might be indicative of malicious code.

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

The O.IDSCAN objective counters this threat by requiring the TOE to collect and store static configuration information that might be indicative of a vulnerability.

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

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

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

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

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

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

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

The O.AUDITS and O.IDSENS objectives address this threat by requiring the TOE to collect audit and system event data.

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

The O.AUDITS and O.IDSENS objectives address this threat by requiring the TOE to collect audit and system event data.

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

The O.AUDITS and O.IDSENS objectives address this threat by requiring the TOE to collect audit and system event data.

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

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

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

The O.IDANLZ objective requires analytical processes be applied to data collected from the system.

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

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

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

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

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

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

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

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

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

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

8.2 Rationale for Security Objectives for the Environment

The purpose for the environmental objectives is to provide protection for the TOE through procedural and administrative measures. The defined objectives provide for physical protection of the TOE, proper management of the TOE, and interoperability requirements on the TOE. Together with the TOE security objectives, these environmental objectives provide a complete description of the responsibilities of the TOE in meeting security needs.

8.3 Security Requirements Rationale

This section demonstrates that the functional components provide complete coverage of the defined security objectives. The mapping of components to security objectives is depicted in the following table.

Table 5 - Security Requirements Mapping

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT
FAU_GEN.1										X		
FAU_SAR.1						X						
FAU_STG.2	X						X	X	X		X	
FAU_STG.4									X	X		

	O.PROTCT	O.IDSCAN	O.IDSENS	O.IDANLZ	O.RESPON	O.EADMIN	O.ACCESS	O.IDAUTH	O.OFLOWS	O.AUDITS	O.INTEGR	O.EXPORT
FIA_ATD.1								X				
FIA_UAU.2							X	X				
FIA_UID.2							X	X				
FMT_MOF.1	X						X	X				
FMT_MTD.1	X						X	X			X	
FMT_SMF.1						X						
FMT_SMR.1								X				
FPT_ITI.1												X
FPT_RVM.1	X					X		X		X	X	
FPT_SEP.1	X					X		X		X	X	
FPT_STM.1										X		
IDS_SDC.1		X	X									
IDS_ANL.1				X								
IDS_RCT.1					X							
IDS_RDR.1						X	X	X				
IDS_STG.1	X						X	X	X		X	
IDS_STG.2									X			

The following discussion provides detailed evidence of coverage for each security objective.

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

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

The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].

O.IDSCAN The TOE 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.

The System is required to collect and store static configuration information of an IT System. [IDS_SDC.1].

O.IDSENS The TOE 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 TOE.

A System is required to collect events indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets of an IT System. [IDS_SDC.1].

O.IDANLZ The TOE must accept network traffic data from targeted IT system resources and then apply analytical processes and information to derive conclusions about intrusions (past, present, or future).

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

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

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

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

The TOE must provide authorized administrators and authorized system administrators with the ability to view and interpret all audit information from the audit records [FAU_SAR.1]. The TOE is required to provide authorized administrators with the ability to manage functions and data related to collecting and analyzing tasks, as well as the ability to manage users [FMT_SMF.1]. The System must provide the ability for authorized administrators to view all System data collected and produced [IDS_RDR.1]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected from interference that would prevent it from performing its functions [FPT_SEP.1].

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

The System is required to restrict the review of System data to those granted with explicit read-access [IDS_RDR.1]. The TOE is required to protect the audit data from deletion as well as guarantee the availability of the audit data in the event of storage exhaustion, failure or attack [FAU_STG.2]. The System is required to protect the System data from any modification and unauthorized deletion [IDS_STG.1]. Users authorized to access the TOE are defined using an identification and authentication process [FIA_UID.2, FIA_UAU.2]. The TOE is required to provide the ability to restrict managing the behavior of functions of the TOE to authorized users of the TOE [FMT_MOF.1]. Only authorized administrators of the System may query and add System data, and authorized administrators of the TOE may query and modify all other TOE data [FMT_MTD.1].

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

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

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

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

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

Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1].. The TOE must prevent the loss of collected data in the event the audit trail is full [FAU_STG.4]. The TOE must ensure that all functions are invoked and succeed before each function may proceed [FPT_RVM.1]. The TSF must be protected form interference that would prevent it from performing its functions [FPT_SEP.1]. Time stamps associated with an audit record must be reliable [FPT_STM.1].

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

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

O.EXPORT When a remote trusted IT product makes TSF system data available to the TOE, the TOE will provide a means to ensure the integrity of the TSF system data.

The TOE must provide a means for the TOE to ensure the integrity of TSF data destined for the TOE [FPT_ITI.1].

8.4 Security Assurance Requirements Rationale

EAL2 was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment.

8.5 Strength of Functions Rationale

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

The relevant security functional requirement is FIA_UAU.2. The intent is that the password mechanism meets or exceeds SOF-basic and the evidence can be found in the strength of function analysis.

8.6 Requirement Dependency Rationale

This Security Target does satisfy all the requirement dependencies of the Common Criteria. The following table lists each requirement with a dependency and indicates whether the dependent requirement was included. As the table and accompanying rationale indicates, all dependencies have been met.

Table 6 - Requirement Dependencies

Functional Component	Dependency	Included
FAU_GEN.1	FPT_STM.1	Yes
FAU_SAR.1	FAU_GEN.1	Yes
FAU_STG.2	FAU_GEN.1	Yes
FAU_STG.4	FAU_STG.1	NO
FIA_UAU.2	FIA_UID.1	NO
FMT_MOF.1	FMT_SMR.1 & FMT_SMF.1	Yes
FMT_MTD.1	FMT_SMR.1 & FMT_SMF.1	Yes
FMT_SMR.1	FIA_UID.1	NO

For requirements FIA_UAU.2 and FMT_SMR.1, a dependency on FIA_UID.1 is indicated in the table above. While this ST does not include FIA_UID.1, it does include FIA_UID.2, which is hierarchical to FIA_UID.1. Therefore, the dependency on FIA_UID.1 has been satisfied. For requirement FAU_STG.4, a dependency on FAU_STG.1 is indicated in the table above. While this ST does not include FAU_STG.1, it does include FAU_STG.2, which is hierarchical to FAU_STG.1. Therefore, the dependency on FAU_STG.1 has been satisfied.

8.7 Explicitly Stated Requirements Rationale

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

8.8 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. Table 7 - Requirements Mapped To Security Function demonstrates the relationship between security requirements and security functions.

Table 7 - Requirements Mapped To Security Function

	Security Audit	Identification and Authentication	Security Management	Protection of the TOE Security Functions	IDS Component Requirements (IDS)

	Security Audit	Identification and Authentication	Security Management	Protection of the TOE Security Functions	IDS Component Requirements (IDS)
FAU_GEN.1	X				
FAU_SAR.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.1			X		
FMT_SMF.1			X		
FMT_SMR.1			X		
FPT_ITI,1				X	
FPT_RVM.1				X	
FPT_SEP.1				X	
FPT_STM.1				X	
IDS_ANL.1					X
IDS_RCT.1					X
IDS_RDR.1					X
IDS_SDC.1					X
IDS_STG.1					X
IDS_STG.2					X

8.9 PP Claims Rationale

See Section 7, Protection Profile Claims.