IronPort Email Security Appliances Security Target

Version 1.0
November 29, 2010

Prepared for:
Cisco IronPort Systems LLC
950 Elm Avenue
San Bruno, CA 94066

Prepared By:
Science Applications International Corporation
Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive
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 Email Security Appliances (ESA), comprising the C160, C370, X1060, and X1070 appliance models, running IronPort AsyncOS software, version 7.1, and the C670 appliance model running IronPort AsyncOS version 7.3, from Cisco IronPort Systems LLC. The TOE is an IDS System-type product that monitors Simple Mail Transfer Protocol (SMTP) network traffic, analyzes the monitored network traffic using various techniques, and reacts to identified threats associated with email messages (such as spam and inappropriate or malicious content). Note that version 7.3 of AsyncOS has been specifically created to support use of a FIPS 140-2 validated Hardware Security Module (HSM), which is included only in the C670 appliance model. The vendor asserts the correct implementation of cryptographic algorithms in the appliance models running AsyncOS Version 7.1, which have not been FIPS validated. Otherwise, in terms of the security functionality claimed within this ST, there is no difference between versions 7.1 and 7.3 of AsyncOS.

This Security Target contains the following additional sections:

- TOE Description (Section 2)—provides an overview of the TOE and describes the physical and logical boundaries of the TOE
- Security Problem Definition (Section 3)—describes the assumptions, policies and threats that define the security problem to be addressed by the TOE and its environment
- Security Objectives (Section 4)—describes the security objectives for the TOE and its operational environment intended to counter the threats, address the policies, and satisfy the assumptions in the Security Problem Definition
- IT Security Requirements (Section 5)—provides a set of security functional requirements to be met by the TOE. The IT security requirements also provide a set of security assurance requirements that are to be satisfied by the TOE
- TOE Summary Specification (Section 6)—describes the security functions of the TOE and how they satisfy the security functional requirements
- Protection Profile Claims (Section 7)—provides rationale that the TOE conforms to the Protection Profile for which conformance has been claimed
- Rationale (Section 8)—provides mappings and rationale for the security objectives, security requirements, and security functions to justify their completeness, consistency, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – IronPort Email Security Appliances Security Target

ST Version – Version 1.0

ST Date – November 29, 2010

TOE Identification – IronPort Email Security Appliances, comprising the C160, C370, X1060, and X1070 appliance models, running IronPort AsyncOS software, version 7.1, and the C670 appliance model running IronPort AsyncOS version 7.3.

TOE Developer – Cisco IronPort Systems LLC

Evaluation Sponsor – Cisco IronPort Systems LLC

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 3, July 2009.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 3, July 2009.
    - Part 3 Conformant

This ST and the TOE it describes are conformant to the following package:

- EAL 2 Augmented with ALC_FLR.2

This ST and the TOE it describes are conformant to the following protection profile:

- U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007.

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 …").
- Extended requirements (i.e., those not found in Part 2 or Part 3 of the CC) are identified with "(EXT)" following the identification of the new functional class/name (i.e., Intrusion Detection System (IDS)) and the associated family descriptor. For example, "IDS_ANL.1: Analyzer analysis (EXT)".
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.4 Glossary

The following terms are used throughout this Security Target.

AES Advanced Encryption Standard—a block-based symmetric-key encryption standard, defined in FIPS PUB 197

BSD Berkeley Software Distribution—a derivative of the UNIX operating system developed and distributed by the Computer Systems research Group of the University of California, Berkeley, from 1977 to 1995

DER Distinguished Encoding Rules—a message transfer syntax, widely used for encoding public key certificates

DNS	Domain Name System—the hierarchical naming system for resources (such as computers and services) connected to the Internet or a private network. It translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide
FIPS	Federal Information Processing Standards—publicly announced standards developed by the United States federal government for use by all non-military government agencies and by government contractors
FTP	File Transfer Protocol—a network protocol used to copy a file from one computer to another over a TCP/IP-based network
HSM	Hardware Security Module—a hardware device implementing cryptographic algorithms and protocols
HTTP	Hypertext Transfer Protocol—a request-response protocol standard for client-server computing. HTTP is not secure
HTTPS	Hypertext Transfer Protocol Secure—a combination of the Hypertext Transfer Protocol with the /TLS protocol to provide encryption and secure identification of the server
IMAP	Internet Message Access Protocol—an application layer Internet protocol that allows an e-mail client to access e-mail on a remote mail server
LDAP	Lightweight Directory Access Protocol—an application protocol for querying and modifying data using directory services running over TCP/IP
MD5	Message Digest algorithm 5—a widely used cryptographic hash function with a 128-bit hash value
MTA	Mail Transfer Agent—in Internet message handling services, the process that transfers email from one computer to another, implementing both the client and server portions of SMTP
MX	Mail eXchanger—in the context of the Domain Name System, formally refers to an IP address assigned to a device hosting a mail server
NTP	Network Time Protocol—a means of synchronizing clocks over a computer network
POP	Post Office Protocol—an application-layer Internet standard protocol used by local email clients to retrieve email from a remote server over a TCP/IP connection
RADIUS	Remote Authentication Dial in User Service—a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service
RFC	Request For Comments—a memorandum published by the Internet Engineering Task Force (IETF) describing methods, behaviors, research, or innovations applicable to the working of the Internet and Internet-connected systems. The IETF adopts some of the proposals published as RFCs as Internet standards.
RPC	Remote Procedure Call—a network protocol that allows a computer program running on one host to cause code to be executed on another host
RSA	Rivest-Shamir-Adleman—an algorithm for public-key cryptography
SCP	Secure Copy—a means of securely transferring computer files between hosts. It is based on the SSH protocol
SHA1	Secure Hash Algorithm 1—a cryptographic hash function that takes arbitrary data as its input and produces a fixed-length bit string, such that any change to the input data produces a different output string. SHA1 is defined by FIPS 180-2 and produces output strings of 160 bits
SMTP	Simple Mail Transfer Protocol—an Internet standard for email transmission across Internet Protocol (IP) networks

SSH Secure Shell—a network protocol that allows data to be exchanged using a secure channel between two networked devices. It is typically used to login securely to a remote machine and execute commands at its Command Line Interface

TLS Transport Layer Security—a cryptographic protocol that provides security for communications over networks. It is used in conjunction with HTTP to provide HTTPS

Triple DES Triple Data Encryption Standard—a block-based symmetric-key encryption standard, defined in FIPS PUB 46-3. It is a precursor to AES

2. TOE Description

The TOE is IronPort Email Security Appliances (ESA), comprising Cisco IronPort Systems' IronPort hardware appliance models C160, C370, X1060, and X1070, running IronPort AsyncOS software, version 7.1, and the C670 appliance model running IronPort AsyncOS version 7.3. Note that version 7.3 of AsyncOS has been specifically created to support use of a FIPS 140-2 validated Hardware Security Module (HSM), which is included only in the C670 appliance model. Otherwise, all appliance models comprising the TOE provide the same security functionality. They differ only in the number and speed of their network connections and their processing capacity (in terms of memory and processor speeds).

2.1 TOE Overview

The TOE is an IDS System-type product that monitors Simple Mail Transfer Protocol (SMTP) network traffic, analyzes the monitored network traffic using various techniques, and reacts to identified threats associated with email messages (such as spam and inappropriate or malicious content). The TOE handles any traffic it receives on its network interfaces as if it were SMTP—any non-SMTP traffic will produce SMTP command errors. There is a limit to the number of bad commands that can be executed before the TOE drops the connection.

The TOE is designed to serve as the SMTP gateway or Mail Exchanger (MX), providing the Message Transfer Agent (MTA) role in the customer's network infrastructure. As such, the TOE is intended to be installed to enable it to monitor email between an external and an internal network, such that network traffic sent and received on TCP port 25[1] must pass through the TOE. The TOE provides separate physical interfaces allowing it to be connected to separate internal and external networks.

The TOE can be configured to monitor email network traffic sent from the internal network to the external network, and vice versa.

The TOE provides capabilities to manage its monitoring, analysis and reaction functions, and controls access to those capabilities through the use of administrative roles with varying security management authorizations. All administrative users of the TOE are required to be identified and authenticated before accessing the TOE's management capabilities, and administrative actions are audited.

2.2 TOE Architecture

2.2.1 TOE Capabilities

The TOE monitors SMTP network traffic and applies the following traffic analysis mechanisms:

- Signature analysis—the administrator can configure message filters, comprising 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 headers, or message body
- Detection of spam—the TOE implements a layered mechanism to detecting and handling spam. The first layer of spam control is called reputation filtering, which allows for classifying email senders and restricting access to email infrastructures based on a sender's trustworthiness as determined by the TOE. The second layer comprises scanning of messages by the TOE's Anti-Spam engine. In addition, the administrator can create policies to deliver messages from known or highly reputable senders directly to the end user without any anti-spam scanning, while messages from less reputable or unknown senders are subjected to anti-spam scanning. The TOE can also be configured to throttle the number of messages it will accept from suspicious senders, reject connections or bounce messages
- Anti-virus scanning—the TOE incorporates v4.58 of the Sophos Anti-Virus virus scanning engine, which can be configured to scan messages and attachments for viruses on a per-mail policy basis and take the following actions based on the scan results: attempt to repair the attachment; drop the attachment; modify

[1] SMTP traffic typically is communicated on TCP port 25, but the TOE can be configured to monitor other ports for SMTP traffic.

the subject header; add an additional header; send the message to a different address or mail host; archive the message; or delete the message

- Application of content filters—the administrator can create content filters to be applied to messages on a per-recipient or per-sender basis. Content filters are similar to the message filters described above under "Signature analysis", except that they are applied later in the email processing pipeline, after a message has been split into a number of separate messages for each matching policy
- Application of virus outbreak filters—the TOE has the ability to compare incoming messages with administrator-configured Virus Outbreak Rules. Messages that match such rules are assigned a threat level and that threat level is compared to the threat level threshold set by the administrator. Messages meeting or exceeding the threshold are quarantined.

The TOE can then take one or more of the following actions in response to detected potential intrusions as identified by the traffic analysis mechanisms:

- 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 various administrator-configurable rule sets that control the behavior of spam detection, anti-virus scanning, content filtering and virus outbreak filtering 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.

2.2.2 Physical Boundaries

The TOE is IronPort Email Security Appliances (ESA), comprising Cisco IronPort Systems' IronPort hardware appliance models C160, C370, X1060, and X1070, running IronPort AsyncOS software, version 7.1, and the C670 appliance model running AsyncOS version 7.3. The TOE comprises the following components:

- **IronPort appliance hardware**—provides Ethernet connectors for connections to internal and external networks to support monitoring of SMTP network traffic, as well as a management network connection, a separate serial port for a console connection, and the runtime environment for a modified BSD operating system
- **IronPort modified BSD operating system component**—provides the runtime environment for the AsyncOS application software component. It consists of a modified BSD kernel process, file system, communications facilities and start-up facilities. Modifications have been limited to tuning parameters, bug fixes, optimizations, and removing startup commands
- **IronPort AsyncOS application software component**—monitors SMTP network traffic sent and received on TCP port 25 and takes action based on administratively-configurable rules. Provides a command line interface (CLI) for administrator access to the TOE.

The TOE components and their relationships to each other are depicted in the figure below:

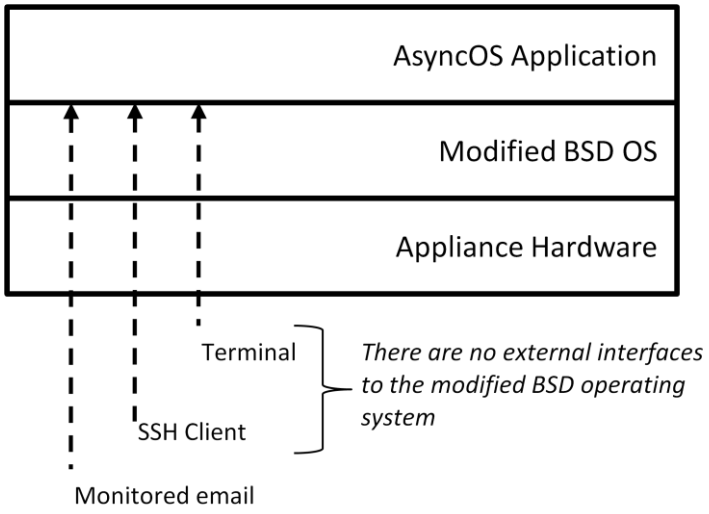

Figure 1: High-level TOE Architecture

The intended purpose and method of use of the TOE assumes the following are in its operational environment:

- SMTP email servers that are compliant with RFC 2821
- Any one or more of the following means of accessing the administrative interfaces of the TOE:
    - Telnet/SSH client, to access the TOE's CLI via the management network
    - Terminal or terminal application to access the console interface via the serial port

  Note: If Telnet is used to connect to the TOE for management purposes, the terminal or workstation used to administer the TOE appliance must be directly connected to the TOE appliance in the evaluated configuration.

Depending on the requirements of the customer, any of the following optional components may also exist in the operational environment of the TOE:

- RADIUS or LDAP server to support authentication of administrators
- NTP server to support synchronization of the appliance's system clock with other computers
- Syslog server for storing log files pushed to it by the TOE (note that the TOE has capacity for storing log files)
- SCP client for uploading and downloading configuration files and downloading log files
- SCP server for storing log files pushed to it by the TOE.

Figure 2 below depicts the TOE in a typical configuration, illustrating the following connections:

- Through the corporate firewall to the Internet to receive and send SMTP traffic
- To the corporate SMTP servers, to which it sends monitored SMTP traffic that has successfully passed through all its IDS filtering, and from which it receives SMTP traffic to be dispatched to the Internet
- To the directly connected management console
- To the internal management network, containing the various optional servers listed above.

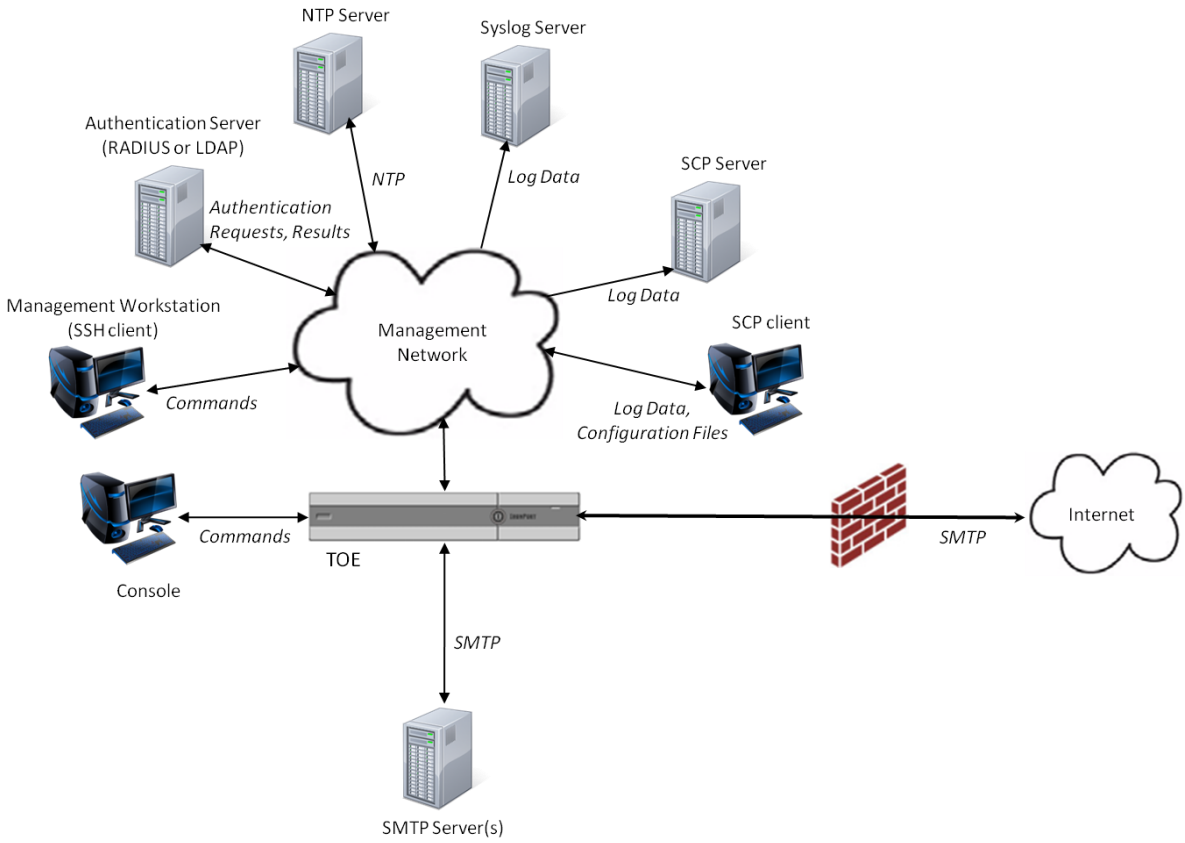

Figure 2: TOE Deployment Scenario

Figure 3 depicts the TOE in a typical configuration, where it is installed behind the enterprise firewall, between the firewall and the enterprise's email generation systems (e.g., groupware servers such as Exchange or Domino, and POP/IMAP servers). The TOE implements the concept of a "listener", which is an email processing service configured on a particular IP interface. Listeners apply only to email entering the TOE—either from the Internet (Listener A in Figure 3) or from internal systems (Listener B in Figure 3). The TOE uses listeners to specify criteria that messages must meet in order to be accepted and relayed to recipient hosts.

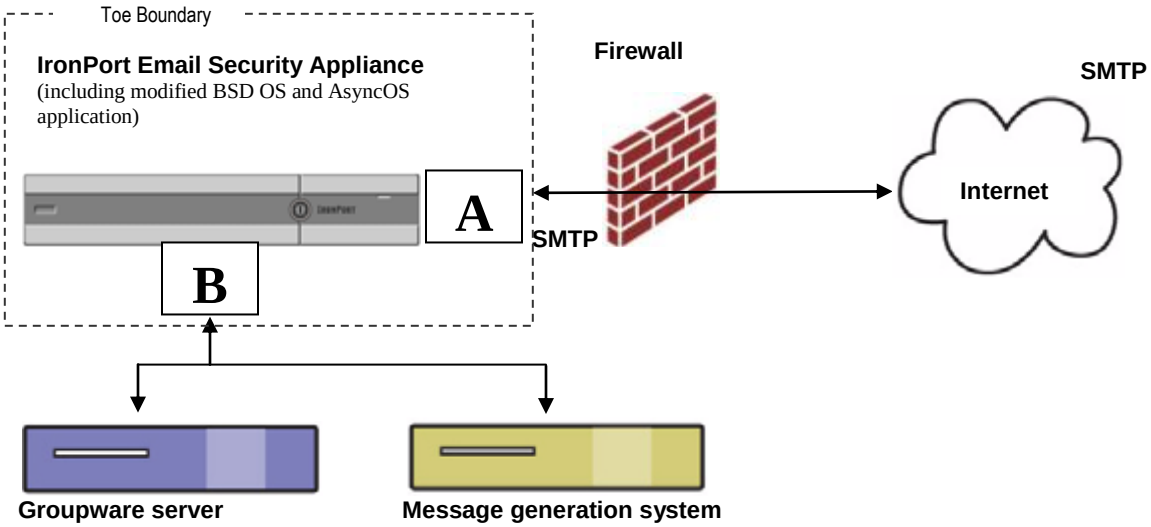

Figure 3: Typical TOE Deployment Configuration

Depending on the network configuration into which the TOE is installed, the firewall may need to be configured to allow access on various ports. At a minimum, both SMTP (port 25) and DNS (port 53) services must have access to the Internet. The TOE guidance documentation provides advice on other services that may need to be allowed through the firewall.

2.2.3 Logical Boundaries

This section identifies the security functions that the TSF provides, as follows:

- Audit
- Cryptographic support
- Identification and authentication
- Security management
- TSF protection
- Intrusion detection.

2.2.3.1 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 users can read all audit information via the TOE's CLI. The TOE provides capabilities to sort audit data for review. In the event the space available for storing audit records is exhausted, the TOE alerts the administrator and commences overwriting the oldest stored audit records.

2.2.3.2 Cryptographic support

The TOE provides the cryptographic algorithms and key management capabilities necessary to support Secure Shell (SSH), allowing secure remote administration of the TOE at its CLI. In the C670 appliance model, the cryptographic capabilities are provided by a Cavium HSM, the FIPS 140-2 validated Nitrox XL CN15xx-NFBE FIPS Cryptographic Module (FIPS 140-2 certificate # 1360). In the other appliance models, the cryptographic capabilities are provided by OpenSSL, version 0.9.8k 25 Mar 2009.

2.2.3.3 Identification and authentication

The TOE maintains user identities, authentication data, and role information. The TOE implements a local authentication mechanism for administrators, based on the attributes stored in its own internal database. Additionally, the TOE can be configured to support authentication using an external RADIUS or LDAP server.

2.2.3.4 Security management

The TOE provides capabilities to manage its security functions, and controls access to those capabilities through the use of administrative roles with varying security management authorizations. In the evaluated configuration, all security management functions specified in this ST must be performed via the CLI.

2.2.3.5 TSF protection

The TOE is able to download updates for Sophos Anti-Virus definitions, IronPort Anti-Spam rules, and Virus Outbreak Filter rules from IronPort update servers over HTTPS. These signature updates are verified using an MD5 (128 bit) hash algorithm, in order to ensure their integrity.

The TOE provides reliable time stamps for its own use, based on its own internal clock. The TOE can also be configured to synchronize its time with other computers via an NTP server.

2.2.3.6 Intrusion detection

The TOE monitors SMTP network traffic. The TOE performs signature analysis, detection of spam, anti-virus scanning, and application of content filters on collected email network traffic and records corresponding event data.

The TOE provides the administrators with capabilities to review the stored event data. In the event the space available for storing event data is exhausted, the TOE alerts the administrator and commences overwriting the oldest stored event data.

2.2.4 Features Excluded from Evaluation

The features described in this section have not been evaluated.

The IronPort Email Security Appliances can support the following additional capabilities, but these require separate licenses and are completely unavailable on an appliance without the proper feature keys and configurations:

- McAfee Anti-Virus—behaves identically to the Sophos Anti-Virus capability included in the evaluated configuration. It is a user-level process that accepts messages and returns verdicts via RPC
- Cloudmark Anti-Spam—behaves identically to the anti-spam capability included in the evaluated configuration. It is a user-level process that accepts messages and returns verdicts via RPC
- ImageAnalyzer Image Analysis—supports scanning for "inappropriate" images. This is a user-level process that accepts images and returns verdicts. The administrator is able to treat messages based on a range of values that specify the "appropriateness" of a given image
- RSA Data Loss Prevention—scans outbound email and returns verdicts in the form of descriptions of policy level violations. For example, an outgoing message may be quarantined based on the potential violation of a HIPPA policy
- IronPort Email Encryption—receives an email message and returns an encrypted message encapsulated in HTML. A new, secure message is constructed and delivered from the appliance to end users
- Centralized Management—allows configuration and management of multiple appliances at the same time in a cluster configuration.

Additionally, the following capabilities described in the TOE guidance documentation have not been included within the scope of the evaluation and are to remain disabled in the evaluated configuration:

- Support for SMTP Authentication
- DomainKeys and DomainKeys Identified Mail (DKIM) authentication
- Sender Policy Framework (SPF) and Sender ID Framework (SIDF) verification
- Support for SNMP, either for status monitoring or trap generation (SNMP is disabled by default)
- Use of the web-based graphical user interface
- FTP access to the TOE.

2.3 TOE Documentation

Cisco IronPort Systems supplies the following documents as part of the TOE, describing the installation process for the TOE and providing guidance for use and administration of the TOE security features:

- For the C160, C370, X1060, and X1070 appliance models:
  - *Cisco IronPort AsyncOS 7.1 for Email Configuration Guide*, April 27, 2010
  - *Cisco IronPort AsyncOS 7.1 for Email Advanced Configuration Guide*, April 27, 2010
  - *IronPort AsyncOS 7.1 CLI Reference Guide for IronPort Appliances*, April 5, 2010
  - *Cisco IronPort AsyncOS 7.1 for Email Daily Management Guide*, April 27, 2010
- For the C670 appliance model:
  - *Cisco IronPort AsyncOS 7.3 for Email Configuration Guide*, June 30, 2010
  - *Cisco IronPort AsyncOS 7.3 for Email Advanced Configuration Guide*, June 30, 2010

- *IronPort AsyncOS 7.3 CLI Reference Guide for Cisco IronPort Appliances*, August 12, 2010
- *Cisco IronPort AsyncOS 7.3 for Email Daily Management Guide*, April 27, 2010.

3. Security Problem Definition

The TOE security environment describes the security aspects of the intended environment in which the TOE is to be used and the manner in which it is expected to be employed. The statement of the TOE security environment defines the following:

- Organizational Policies that the TOE and the environment of the TOE satisfy
- Threats that the TOE and the environment of the TOE counter
- Assumptions made about the operational environment and the intended method of use for the TOE.

Furthermore, the TOE is intended to be used in environments where the relative assurance that its security functions are enforced is commensurate with EAL 2 augmented with ALC_FLR.2 as defined in the CC.

All security environment statements have been drawn from a validated Protection Profile (U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007 Protection Profile).

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.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 TOE.

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.PROTCT	The TOE must protect itself from unauthorized modifications and access to its functions and data.
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.
O.AUDIT_PROTECTION	The TOE will provide the capability to protect audit information.
O.AUDIT_SORT	The TOE will provide the capability to sort the audit information.
O.TIME	The TOE will provide reliable timestamps.

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.

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

OE.CERTIFICATES The operational environment shall provide a means by which public key certificates can be created and managed.

5. IT Security Requirements

Most of the security requirements for the TOE have been drawn from Parts 2 and 3 of the Common Criteria as well as from the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments. The security functional requirements have been selected to correspond to the actual security functions implemented by the TOE and as required by the Protection Profile, while the assurance requirements have been selected to offer assurance that those security functions are properly realized.

This Security Target utilizes extended requirements only as reproductions of requirements found in the Protection Profile to which it claims conformance. Therefore, all requirements for information related to the extended requirements are satisfied by this Security Target's conformance to a validated Protection Profile.

5.1 Extended Components Definition

The U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments (IDSSPP) defines extended security functional requirements, which are included in this ST. The extended requirements can be identified by the use of the keyword "EXT" in the title. The IDSSPP provides a rationale for the use of extended security requirements, identifying that the CC audit family (FAU) was used as a model.

5.2 TOE Security Functional Requirements

This section specifies the security functional requirements (SFRs) for the TOE. SFRs were drawn from the Protection Profile (PP) identified in the Conformance Claims section and from Part 2 of CC v3.1, Revision 3.

Note that the PP was written using CC v3.1, Revision 1, whereas this ST claims conformance to CC v3.1, Revision 3. Those SFRs that are drawn from CC Part 2 therefore reproduce the wording of CC Part 2 v3.1, Revision 3. Section 7 (Protection Profile Claims) identifies the SFRs whose wording, for this reason, differs from that used in the PP.

The following table describes the SFRs satisfied by the TOE.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
	FAU_SAR.1: Audit Review
	FAU_SAR.2: Restricted Audit Review
	FAU_SAR.3: Selectable Audit Review
	FAU_SEL.1: Selective Audit
	FAU_STG.2: Guarantees of Audit Data Availability
	FAU_STG.4: Prevention of Audit Data Loss
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation
	FCS_CKM.4: Cryptographic Key Destruction
	FCS_COP.1(1): Cryptographic Operation (Symmetric Encryption)
	FCS_COP.1(2): Cryptographic Operation (Signature Services)
	FCS_COP.1(3): Cryptographic Operation (Hashing Services)

Requirement Class	Requirement Component
FIA: Identification and Authentication	FIA_ATD.1: User Attribute Definition
	FIA_UAU.1: Timing of Authentication
	FIA_UAU.5: Multiple Authentication Mechanisms
	FIA_UID.1: Timing of Identification
FMT: Security Management	FMT_MOF.1: Management of Security Functions Behavior
	FMT_MTD.1(1): Management of TSF Data
	FMT_MTD.1(2): Management of TSF Data (User Accounts)
	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_STM.1: Reliable time stamps
IDS: IDS Component requirements	IDS_ANL.1: Analyzer analysis (EXT)
	IDS_RCT.1: Analyzer react (EXT)
	IDS_RDR.1: Restricted Data Review (EXT)
	IDS_SDC.1: System Data Collection (EXT)
	IDS_STG.1: Guarantee of System Data Availability (EXT)
	IDS_STG.2: Prevention of System data loss (EXT)

Table 1: TOE Security Functional Components

5.2.1 Security Audit (FAU)

5.2.1.1 Audit Data Generation (FAU_GEN.1)

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

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

b) All auditable events for the [***basic***] level of audit; and

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

Application Note: The auditable events for the basic level of auditing are included in Table 2: Auditable Events.

Component	Event	Details
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to System	
FAU_GEN.1	Access to the TOE and System data	Object IDS, Requested access
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	

Component	Event	Details
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	
FIA_UAU.1, FIA_UAU.5	All use of the configured authentication mechanism	User identity, location
FIA_UID.1	All use of the user identification mechanism	User identity, location
FMT_MOF.1	All modifications in the behavior of the functions of the TSF	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity
FPT_ITI.1	The action taken upon detection of modification of transmitted TSF data	

Table 2: Auditable Events

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

a) Date and time of the event, type of event, subject identity (if applicable), 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**].

5.2.1.2 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.

5.2.1.3 Restricted Audit Review (FAU_SAR.2)

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

5.2.1.4 Selectable Audit Review (FAU_SAR.3)

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

5.2.1.5 Selective Audit (FAU_SEL.1)

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

a) [***event type***]

b) [**no other attributes**].

5.2.1.6 Guarantees of Audit Data Availability (FAU_STG.2)

FAU_STG.2.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

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

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

5.2.1.7 Prevention of Audit Data Loss (FAU_STG.4)

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

5.2.2 Cryptographic Support (FCS)[2]

5.2.2.1 Cryptographic Key Generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**ANSI X9.31 Appendix A.2.4 PRNG**] and specified cryptographic key sizes [**128 bits, 256 bits (AES); 168 bits (TDES)**] that meet the following: [**ANSI X9.31**].

5.2.2.2 Cryptographic Key Destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**overwrite with zeroes**] that meets the following: [**none**].

5.2.2.3 Cryptographic Operation (Symmetric Encryption) (FCS_COP.1(1))

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

5.2.2.4 Cryptographic Operation (Signature Services) (FCS_COP.1(2))

FCS_COP.1.1(2) The TSF shall perform [**cryptographic signature services**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**1024 bits, 2048 bits**] that meet the following: [**FIPS PUB 186-3 with ANSI X9.31-1998**].

5.2.2.5 Cryptographic Operation (Hashing Services) (FCS_COP.1(3))

FCS_COP.1.1(3) The TSF shall perform [**cryptographic hashing services**] in accordance with a specified cryptographic algorithm [**SHA-1**] and cryptographic ~~key~~ **hash** sizes [**160 bits**] that meet the following: [**FIPS PUB 180-3**].

5.2.3 Identification and Authentication (FIA)

5.2.3.1 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) Authorisations; and

d) /no other security attributes/].

5.2.3.2 Timing of Authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [**attempts to send email**] on behalf of the user to be performed before the user is authenticated.

[2] The C670 appliance model, running AsyncOS Version 7.3, incorporates a FIPS 140-validated HSM. In all other appliance models of the TOE, running AsyncOS Version 7.1, the vendor asserts the correct implementation of the cryptographic capabilities specified for the TOE.

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

5.2.3.3 Multiple Authentication Mechanisms (FIA_UAU.5)

FIA_UAU.5.1 The TSF shall provide [**a local authentication mechanism and support for external authentication via RADIUS or LDAP**] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**following rules:**

- **The built in "admin" user (an authorized System administrator role) is always authenticated locally by the TSF**
- **If an external authentication server is configured, it is consulted by the TSF to authenticate the submitted user identity**
- **If a configured external authentication server cannot be reached, or no external authentication server is configured, the submitted user identity will be authenticated locally by the TSF**].

5.2.3.4 Timing of Identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow [**attempts to send email**] on behalf of the user to be performed before the user is identified.

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

5.2.4 Security Management (FMT)

5.2.4.1 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**].

5.2.4.2 Management of TSF Data (FMT_MTD.1(1))

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

5.2.4.3 Management of TSF Data (User Accounts) (FMT_MTD.1(2))

FMT_MTD.1.1(2) The TSF shall restrict the ability to [***modify, delete, create***] the [**user accounts**] to [**authorized System administrators**].

5.2.4.4 Specification of Management Functions (FMT_SMF.1)

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

a.) **Manage functions related to System data collection and analysis**

b.) **Manage user accounts**

c.) **Configure external authentication**

d.) **Set the System time**

e.) **View audit data**

f.) **Select the set of events to be audited from the set of all auditable events**].

5.2.4.5 Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [**authorized administrator, authorized System administrator, and *[no other security management roles]***].

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

Application Note: The PP defined roles, as specified in FMT_SMR.1.1, are instantiated by the TOE-defined roles as follows: "authorized administrator" is instantiated by the "Operators" role; "authorized System administrator" is instantiated by the "Administrators" role.

5.2.5 Protection of the TOE Security Functions (FPT)

5.2.5.1 Inter-TSF Detection of Modification (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 and a remote trusted IT product within the following metric [**the strength must be conformant to the strength offered by the MD5 (128 bit) hash algorithm**].

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

5.2.5.2 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.2.6 IDS Component Requirements (IDS)

5.2.6.1 Analyzer Analysis (EXT) (IDS_ANL.1)

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

a) [***signature***]; and

b) [**the following additional traffic analysis techniques:**

- **Detection of spam**
- **Anti-virus scanning**
- **Application of content filters**
- **Application of virus outbreak filters**]. (EXT)

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

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

b) [**no other security relevant information about the result**]. (EXT)

5.2.6.2 Analyzer React (EXT) (IDS_RCT.1)

IDS_RCT.1.1 The System shall send an alarm to [**an administrator, contained in an email**] and take [**the following actions, as configured by an authorized System administrator:**

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. (EXT)

5.2.6.3 Restricted Data Review (EXT) (IDS_RDR.1)

IDS_RDR.1.1 The System shall provide [**authorized administrators, authorized System administrators**] with the capability to read [**all System data**] from the System data. (EXT)

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

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. (EXT)

5.2.6.4 System Data Collection (EXT) (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) [***network traffic***]; and

b) [**no other defined events**]. (EXT)

IDS_SDC.1.2 At a minimum, the System shall collect and record the following information:

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

b) The additional information specified in the details column of Table 3 System Events. (EXT)

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

Table 3: System Events

5.2.6.5 Guarantee of System Data Availability (EXT) (IDS_STG.1)

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

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

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***]. (EXT)

5.2.6.6 Prevention of System Data Loss (EXT) (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. (EXT)

5.3 TOE Security Assurance Requirements

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

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.2: Security-enforcing functional specification
	ADV_TDS.1: Basic design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures

Requirement Class	Requirement Component
ALC: Life-cycle support	ALC_CMC.2: Use of a CM system
	ALC_CMS.2: Parts of the TOE CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_FLR.2: Flaw reporting procedures
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

Table 4: EAL 2 Assurance Components

5.3.1 Development (ADV)

5.3.1.1 Security Architecture Description (ADV_ARC.1)

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

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

5.3.1.2 Security-enforcing Functional Specification (ADV_FSP.2)

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For SFR-enforcing TSFIs, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For SFR-enforcing TSFIs, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

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

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.3.1.3 Basic Modular Design (ADV_TDS.1)

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behaviour of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarize the SFR-enforcing behaviour of the SFR-enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all behaviour described in the TOE design is mapped to the TSFIs that invoke it.

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

ADV_TDS.1.2E The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.3.2 Guidance Documents (AGD)

5.3.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

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

5.3.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

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

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.3.3 Life-cycle Support (ALC)

5.3.3.1 Use of a CM System (ALC_CMC.2)

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

ALC_CMC.2.2D The developer shall provide the CM documentation.

ALC_CMC.2.3D The developer shall use a CM system.

ALC_CMC.2.1C The TOE shall be labeled with its unique reference.

ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.

ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

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

5.3.3.2 Parts of the TOE CM Coverage (ALC_CMS.2)

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.

ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

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

5.3.3.3 Delivery Procedures (ALC_DEL.1)

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

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

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

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

5.3.3.4 Flaw Reporting Procedures (ALC_FLR.2)

ALC_FLR.2.1D The developer shall document flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.2.3D The developer shall provide flaw remediation guidance addressed to TOE users.

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.2.6C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

ALC_FLR.2.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.2.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

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

5.3.4 Tests (ATE)

5.3.4.1 Analysis 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 in the test documentation and the TSFIs 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.

5.3.4.2 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, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

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

5.3.4.3 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 execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.3.5 Vulnerability Assessment (AVA)

5.3.5.1 Vulnerability Analysis (AVA_VAN.2)

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

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

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

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the TOE security functions and how the TOE meets the security functional requirements.

6.1 TOE Security Functions

Note that the TOE defines five (5) user groups (or administrative roles):

- Administrators
- Operators
- Helpdesk
- Read-only
- Guests.

The Administrators group corresponds to the "authorized System administrator" role defined in the PP and the SFRs in this ST. The Operators group corresponds to the "authorized administrator" role defined in the PP and the SFRs in this ST. The remaining groups (Helpdesk, Read-only, and Guest) do not have any security management capabilities within the scope of the SFRs defined in this ST, and so are not considered to be security management roles. This is further discussed in Section 6.1.4 (Security Management).

6.1.1 Security Audit

The TOE provides its own audit mechanism that can generate audit records for the basic level of audit. Audit records are stored in files in the file system provided by the TOE's modified BSD operating system component. The TOE stores auditable events in separate log files containing related types of audited data. The following log files together comprise the TSF audit trail:

- IronPort Text Mail Logs—record information regarding the operations of the email system, such as message receipt, message delivery attempts, bounces, etc.
- Delivery Logs—record critical information about the TOE's email delivery operations
- Bounce Logs—record information about bounced recipients
- System Logs—record boot information and DNS status information
- CLI Audit Logs—record all CLI activity
- Anti-Virus Logs—record events related to the status of receiving updates of the latest anti-virus identity files
- Authentication Logs—record all successful user logins and failed user authentication attempts.

Note that the TOE generates various other log files that record information about the behavior of the TOE, but these do not contain logs that satisfy the TOE's auditing requirements.

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

- Start-up and shutdown of the audit function—recorded in System Logs
- Access to System—recorded in IronPort Text Mail Logs, Delivery Logs and Bounce Logs
- Access to the TOE and System data—recorded in: IronPort Text Mail Logs, Delivery Logs, and Bounce Logs (for email traffic); and CLI Audit Logs (for console interfaces)
- Reading of information from the audit records—recorded in CLI Audit Logs
- Unsuccessful attempts to read information from the audit records—recorded in CLI Audit Logs

- All modifications to the audit configuration that occur while the audit collection functions are operating—recorded in CLI Audit Logs
- All use of the authentication mechanism—recorded in Authentication Logs
- All use of the user identification mechanism—recorded in Authentication Logs
- All modifications in the behavior of the functions of the TSF—recorded in CLI Audit Logs
- All modifications to the values of TSF data—recorded in CLI Audit Logs
- Modifications to the group of users that are part of a role—recorded in CLI Audit Logs
- The action taken upon detection of modification of transmitted TSF data—recorded in Anti-Virus Logs.

Administrators and Operators can access and view all audit information via the CLI. The TOE restricts the capability to view the audit records to these roles. The CLI additionally provides the capability to sort audit records based on date and time, subject identity, type of event, and success or failure of the related event. Administrators and Operators can also include or exclude auditable events from the set of audited events based on the event type. This is done by configuring which audit logs are active.

In addition to using the CLI to view audit records, the TOE provides the following additional mechanisms for retrieving log files:

- SCP—a client that supports an `scp` command can copy log files from the TOE to the client host. The user of the `scp` command on the client must be the `admin` user on the TOE, as the TOE will prompt for the `admin` user password before processing the SCP request
- SCP Push—additionally, the TOE can be configured to periodically push log files to a SCP server on a remote computer
- Syslog Push—the TOE can be configured to push log files to a remote syslog server.

The TOE's default installation configures the audit log files to maintain 10 files of no more than 10M for each log subscription. The administrative user does not need to configure this. However, this value is customizable. The administrative 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 administrative user can create.

With a typical configuration, the log space should not grow beyond a reasonable limit. If through 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. If the space available for storing audit records is exhausted, the TOE will start to overwrite the oldest records in the audit trail, and generate an email alert to this effect and send it to an Administrator.

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 basic 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_SAR.2: The TOE ensures only authorized administrators and authorized System administrator are able to read the audit records in the various audit log files.
- FAU_SAR.3: The TOE provides capabilities to sort audit records based on date and time, subject identity, type of event, and success or failure of the related event.
- FAU_SEL.1: The TOE provides the capability to specify what auditable events are actually audited, based on the event type.

- FAU_STG.2: The TOE does not provide interfaces to modify individual records. 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 Cryptographic Support

The TOE implements the following cryptographic operations to support SSHv2 and TLS, which provide secure remote access to the CLI and secure downloads over HTTPS respectively:

- AES with 128 or 256 bit keys, to provide symmetric encryption and decryption of data
- Triple DES with 168 bit keys, also to provide symmetric encryption and decryption of data
- RSA with 1024 or 2048 bit keys, to provide digital signature services (generation and verification)
- SHA-1 (160 bit hash), to support message integrity.

The TOE generates its own AES and Triple DES keys and provides CLI commands for importing RSA certificates and keys in the form of Base64 encoded DER certificates, enclosed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----". The TOE destroys keys when they are no longer required by overwriting them with zeroes.

In the C160, C370, X1060, and X1070 appliance models, the cryptographic functions described above are provided by OpenSSL (version 0.9.8k, 25 March 2009). The C670FIPS appliance model includes a Cavium HSM, the FIPS 140-2 validated Nitrox XL CN1520-NFBE (FIPS 140-2 certificate #'s 1360 and 1361).

6.1.2.1 Security function summary

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

- FCS_CKM.1: The TOE generates symmetric keys to support AES (128 and 256 bit keys) and Triple DES (168 bit keys) cryptographic operations
- FCS_CKM.4: The TOE destroys cryptographic keys by overwriting them with zeroes
- FCS_COP.1(1): The TOE implements AES and Triple DES to provide symmetric encryption and decryption services
- FCS_COP.1(2): The TOE implements RSA (with 1024 or 2048 bit keys) to provide digital signature generation and verification services in support of SSH and TLS
- FCS_COP.1(3): The TOE implements SHA-1 to provide cryptographic hashing services.

6.1.3 Identification and Authentication

The TOE provides the capability to identify and authenticate the administrative users of the TOE. It prevents administrative user actions from being performed prior to identification and authentication of the user (all filtering of email occurs without identification or authentication of users).

The TOE defines a default user account, called `admin`. This account has all administrative privileges. The TOE allows additional administrative accounts to be created. Each account comprises a user name (which identifies the user), authentication data, in the form of a password or a public key certificate, and authorizations, in the form of a group assignment that grants certain administrative privileges. Assigning a group to a user account essentially confers a security management role on that user (see Section 6.1.4, Security Management, for details on the security management roles supported by the TOE).

Users are required to enter their user name and password in order to login to the TOE. Note, however, that users accessing the CLI via SSH can be authenticated using public key cryptography. This requires the user's public key to be entered into the TOE (using the `sshconfig` command) and associated with the user's account. If there is no public key configured for the user, the user will instead be prompted to enter a password to authenticate. The password mechanism requires passwords to be a minimum of six (6) characters from the printable character set.

In addition to its local authentication mechanism, the TOE can be configured to utilize an external authentication server to obtain authentication decisions and authorizations for a submitted user identity during the login process. The TOE can be configured to use an LDAP server or a RADIUS server (but not both). When configured, the external authentication service overrides local authentication, except in the following cases:

- Local authentication can be used in failover cases (such as when the external authentication server is down), but this requires shadow accounts to be created in the local account database.
- The builtin "admin" user is always authenticated locally.

Otherwise, if the submitted user identity is not successfully authenticated by the external authentication server, the user is not permitted to login.

6.1.3.1 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 authorizations locally as part of system information (i.e., in files in the operating system component).
- FIA_UAU.1: The TOE allows users to attempt to send email through the TOE without being authenticated.
- FIA_UAU.5: The TOE provides its own local authentication mechanism and can also be configured to use an external RADIUS or LDAP server to provide authentication decisions and user authorizations to the TOE.
- FIA_UID.1: The TOE allows users to attempt to send email through the TOE without being identified.

6.1.4 Security Management

The TOE provides administrative users with a command line interface (CLI) to interact with and manage the security functions of the TOE. The 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. The CLI is used to perform all 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 listed in the following table.

CLI Command	Description
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

CLI Command	Description
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
sshconfig	Configure SSH keys. Disable SSH1.

Table 5: Example CLI Commands

The TOE defines five (5) user groups (or administrative roles):

- 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
- Helpdesk—have access to system quarantines, end-user spam quarantines, and message tracking via the GUI. However, since in the evaluated configuration the GUI is excluded from use and the FTP service is disabled, a user in the Helpdesk group has no capability available to them
- Read-only—can view administrative interfaces, but do not have the ability to commit configuration changes or to access the file system or SCP, thus preventing them from accessing log files
- Guests—can only view system status information.

The Administrators group (including the default `admin` user) corresponds to the "authorized System administrator" role defined in the PP and the SFRs in this ST. The Operators group corresponds to the "authorized administrator" role defined in the PP and the SFRs in this ST. The remaining groups (Helpdesk, Read-only, and Guest) do not have any security management capabilities within the scope of the SFRs defined in this ST, and so are not considered to be security management roles.

6.1.4.1 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(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 (excluding user accounts), as well.
- FMT_MTD.1(2): The TOE restricts the ability to manage user accounts to users in the Administrator role (equivalent to the PP's "authorized System administrator").
- 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 to be in the "authorized System administrator" role. Users that are members of the Operators group are considered to be in the "authorized administrator" role.

6.1.5 Protection of the TSF

The TOE is able to download updates for Sophos Anti-Virus definitions, IronPort Anti-Spam rules, and Virus Outbreak Filter rules from IronPort update servers over HTTPS. These signature updates are verified using the MD5 (128 bit) hash algorithm, in order to ensure their integrity. The MD5 hashes for downloaded signature updates are downloaded in a file that is maintained on a separate server, via HTTPS.

The TOE provides reliable time stamps for its own use, based on its own internal clock. The TOE can also be configured to synchronize its time with other computers via an NTP server.

More generally, the TOE protects itself by supporting the use of secure protocols to access its CLI (SSHv2) and for uploading and downloading configuration files and log files (SCP). The TOE implements its own cryptographic mechanisms to support these protocols (see Section 6.1.2). The TOE requires all administrative users to be identified and authenticated prior to accessing any of the security management capabilities of the TOE, including uploading and downloading configuration and log files via SCP. The TOE provides separate physical interfaces for connecting to the management network and to the networks on which SMTP network traffic will be received and transmitted. All network traffic that is subject to the TOE's intrusion detection function is treated as if it is SMTP traffic. Any non-SMTP traffic will produce SMTP command errors and be discarded.

6.1.5.1 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_STM.1: The TOE correlates collected network traffic event data using time stamps provided by its appliance hardware component.

6.1.6 Intrusion Detection

6.1.6.1 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
- Anti-virus scanning
- Application of content filters
- Application of virus outbreak filters.

Signature analysis involves the use of patterns corresponding to known attacks or misuse, 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

The TOE incorporates Sophos Anti-Virus, which can be configured to scan messages and attachments for viruses on a per-mail policy basis and take the following actions based on the scan results: attempt to repair the attachment; drop the attachment; modify the subject header; add an additional header; send the message to a different address or mail host; archive the message; or delete the message.

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.

6.1.6.2 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
- 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

6.1.6.3 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
- Anti-virus rules
- Content filter rules

- Virus outbreak filter rules.

Each of these rule sets are 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.

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.

6.1.6.4 Storing collected System data

System data is recorded in log files that are stored on the appliance. System data logs are physically protected from unauthorized access and modification by storing them on the appliance. System data logs are logically protected from unauthorized access and modification by restricting access to administrator console interfaces used to manage the log files. When an SMTP protocol command and/or email data causes System data to be generated, if the log file reaches an administrator-configured maximum size, the log will be rolled over. Rolling over a log consists of creating a new log file with the timestamp of the rollover and designating the file as current with the letter "c" extension and renaming the current log file to have a letter "s" extension, signifying saved. When an SMTP protocol command and/or email data causes System data to be generated, if System data storage space has been exhausted in general, the oldest log file where the record type will be stored will be deleted in order to create storage space. After the oldest log file has been deleted, the current log file is rolled over as described above.

If System data storage space is exhausted, an alarm (in the form of an email) is generated and sent to the administrator.

The following log files together comprise the stored System data:

- IronPort Text Mail Logs—record information regarding the operations of the email system, such as message receipt, message delivery attempts, bounces, etc.
- Delivery Logs—record critical information about the TOE's email delivery operations
- Bounce Logs—record information about bounced recipients
- Domain Debug Logs—record the client and server communication during an SMTP conversation between the TOE and a specified recipient host
- Injection Debug Logs—record the SMTP conversation between the TOE and a specified host connecting to the system
- Anti-Spam Logs—record results of the anti-spamming capability of the TOE, as well as logs associated with the Context Adaptive Scanning Engine
- Anti-Virus Logs—record results of the anti-virus scanning capability of the TOE
- Spam Quarantine Logs—record actions associated with the TOE's spam quarantine processing
- SMTP Conversation Logs—record all parts of incoming and outgoing SMTP conversations
- Safe/Block Lists Logs—record data about the safelist/blocklist settings and database.

6.1.6.5 Security function summary

The Intrusion Detection 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 protects stored System data from unauthorized deletion and modification. 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, an alarm (in the form of an email) is generated and sent to the administrator.

7. Protection Profile Claims

The TOE conforms to the U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007 (the IDSSPP). Section 1.3 of the PP states "…STs that claim conformance to this PP shall meet a minimum standard of demonstrable-PP conformance…". This Security Target is a suitable solution to the generic security problem described in the PP. The following sections provide the rationale supporting this conformance claim.

7.1 TOE Type

The TOE provides the capabilities to monitor SMTP traffic sent and received on TCP port 25, analyze the monitored network traffic using various signature-based analysis techniques, and react to identified threats (such as spam and inappropriate or malicious content). As such, it provides the Sensor and Analyzer functions of an IDS System and is consistent with the TOE type specified in the IDSSPP. The IDSSPP clearly indicates an IDS System must include at least one Sensor or one Scanner, but is not required to include both.

7.2 Security Problem Definition

This Security Target includes all the assumptions and organizational security policies specified in the IDSSPP. It does not include the threats T.SCNCFG, T.SCNMLC, or T. SCNVUL, as these are threats that would be addressed by the Scanner function of an IDS System, and the TOE does not implement a Scanner function.

7.3 Security Objectives

This Security Target includes all IT security objectives and all security objectives for the environment as specified in the IDSSPP, except as follows:

- O.EXPORT—omitted in conformance with CCEVS precedent PD-0097
- O.IDSCAN—omitted, as it specifies a security objective for the Scanner function of an IDS System, and the TOE does not implement a Scanner function
- O.IDANLZ—made the following changes to the wording of this objective:
    - Replaced 'Analyzer' with 'TOE': the TOE is a complete IDS system, not a combination of separate Sensors and Analyzers
    - Added 'network traffic' as a qualifier of 'data': clarifies the scope of the TOE
    - Replaced 'IDS Sensors or IDS Scanners' with 'targeted IT system resources': the TOE is a complete IDS system, not a combination of separate Sensors and Analyzers. The TOE does not accept data from an IDS Scanner or IDS Sensor, but rather applies its own Sensor function directly to the targeted IT system resource (the network)
- OE.AUDIT_PROTECTION, OE.AUDIT_SORT, OE.TIME—these three objectives are specified as objectives for the operational environment in the IDSSPP (even though the PP specifies SFRs that meet these objectives). This Security Target specifies these as IT security objectives (and rewords them accordingly), since it also specifies the SFRs that meet these objectives.

In addition, this Security Target defines an additional objective for the operational environment, OE.CERTIFICATES.

7.4 Security Requirements

This Security Target includes the Security Functional Requirements from the IDSSPP, except as follows:

- Three requirements identified in the PP were omitted because they do not pertain to the TOE. See Table 6 below for details

- The IDSSPP was written to conform to CC v3.1, Revision 1, but this Security Target claims conformance to CC v3.1, Revision 3. Where Revision 3 specifies different wording to the SFRs drawn from the PP, the Security Target uses the Revision 3 wording. Cases where this applies are identified in Table 6 below.

This Security Target completes all selection and assignment operations left uncompleted in the IDSSPP. The following table identifies the SFRs to which this applies. This Security Target also adds SFRs not specified in the IDSSPP. Details are provided in the following table.

SFR	ST Tailoring of PP SFRs
FAU_GEN.1	Changed the PP wording to be compliant with CC v3.1, Revision 3. In addition, auditable events associated with some of the SFRs added to the ST but not specified in the PP have been included in Table 2. Note that, in accordance with CCEVS precedent PD-0024, it is not necessary for the TOE to generate audit records for the basic level of audit (as required by FAU_GEN.1 as specified in the IDSSPP) for any of the added SFRs, since the PP does not include a security objective that articulates this intent—O.AUDITS specifies the TOE must audit data accesses and use of the System functions, which are covered by the audit requirements specified in the PP.
FAU_SAR.1	*Assignment*—completed the assignment.
FAU_SAR.2	No changes
FAU_SAR.3	Changed the PP wording to be compliant with CC v3.1, Revision 3.
FAU_SEL.1	Changed the PP wording to be compliant with CC v3.1, Revision 3.
FAU_STG.2	Changed the PP wording to be compliant with CC v3.1, Revision 3. *Selection*—completed the selection. *Assignment*—completed the assignment. In addition, replaced the PP selection of "detect" with "prevent". This is stricter than the requirement in the PP.
FAU_STG.4	*Selection*—completed the selection. *Refinement*—refined the assignment completed by the PP to better characterize the behavior of the TOE. In addition, the PP indicates this operation as a selection, when in fact the operation is an assignment. The ST author has indicated the correct operation performed.
FCS_CKM.1, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3)	*Added*—specify the cryptographic algorithms and key management capabilities necessary to support Secure Shell (SSH) and HTTPS (TLS over HTTP), allowing secure remote administration of the TOE at its CLI, and secure downloads of signature updates.
FIA_AFL.1	*Removed*—the TOE does not provide a capability for external IT products to connect to it, therefore this requirement has been removed from the PP. Reference PD-0097.
FIA_UAU.1	*Assignment*—completed the assignment.
FIA_UAU.5	*Added*—specifies the TOE's support for both a local authentication mechanism and external authentication servers (RADIUS and LDAP). This augments the authentication capability specified by FIA_UAU.1. As such, it is associated with the Identification and Authentication security function and does not affect PP conformance. Further rationale is provided in Section 8.2.
FIA_ATD.1	*Assignment*—completed the assignment.
FIA_UID.1	*Assignment*—completed the assignment.

SFR	ST Tailoring of PP SFRs
FMT_MOF.1	No changes.
FMT_MTD.1(1)	Corresponds to FMT_MTD.1 in the PP. *Assignment*—completed the assignment.
FMT_MTD.1(2)	Added—this requirement was added to the Security Target to specify the management restriction on which roles can manage user accounts. This is more restrictive than the PP requirement (which would allow Operators to also manage user accounts), so satisfies the demonstrable conformance requirement to the PP.
FMT_SMF.1	*Added*—this requirement was added to the Security Target to satisfy dependencies of FMT_MOF.1 and FMT_MTD.1. This requirement was originally included by International Interpretation RI#65 that was adopted in CC Part 2, v2.3 and is included in CC v3.1. This requirement specifies that security functions actually be present in addition to being protected if they are present, and therefore does not impact PP conformance. Further rationale is provided in Section 8.2.
FMT_SMR.1	*Assignment*—completed the assignment.
FPT_ITA.1, FPT_ITC.1	*Removed*—the TOE does not communicate with IDS System components outside the TOE, and therefore these requirements have been removed from the PP. Reference PD-0097. Since the TOE is not a distributed system, it is also not necessary to include FPT_ITT.1, as discussed in PD-0097.
FPT_ITI.1	*Added*—the PP specifies this requirement to address protection of information communicated to other IDS components. It was removed from the PP since the IDS System TOE does not communicate with IDS System components outside the TOE (see PD-0097). However, the TOE specified in this Security Target does satisfy the requirement. The TOE can download signature updates from a remote trusted IT product. As such, it is associated with the TSF Protection security function and does not affect PP conformance. Further rationale is provided in Section 8.2.
FPT_STM.1	Changed the PP wording to be compliant with CC v3.1, Revision 3.
IDS_ANL.1	*Selection*—completed the selection. *Assignment*—completed the assignment.
IDS_RCT.1	*Assignment*—completed the assignment.
IDS_RDR.1	*Assignment*—completed the assignment.
IDS_STG.1	*Selection*—completed the selection *Assignment*—completed the assignment.
IDS_STG.2	*Selection*—completed the selection.
IDS_SDC.1	*Selection*—completed the selection. *Assignment*—completed the assignment.

Table 6: PP Conformance Rationale

The security assurance requirements specified in the IDSSPP are those in the EAL2 assurance requirement package, augmented with ALC_FLR.2 (Flaw Remediation). This Security Target has not made any changes to the security assurance requirements specified in the IDSSPP.

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
- Requirement Dependencies
- TOE Summary Specification
- PP Claims.

8.1 Security Objectives Rationale

The U.S. Government Protection Profile Intrusion Detection System System For Basic Robustness Environments (IDSSPP) provides rationale for the security objectives demonstrating the security objectives it defines are suitable to cover the intended environment. For the PP objectives reproduced in this ST, the PP rationale (provided in Sections 6.1 and 6.2 of the IDSSPP) is valid and is not further discussed. For O.IDANLZ (modified from the PP wording) and OE.CERTIFICATES (introduced by the ST), the following rationale applies:

	T.NOHALT	T.FALREC	T.FALASC	P.ANALYZ	P.PROTCT
O.IDANLZ	**X**	**X**	**X**	**X**	
OE.CERTIFICATES					**X**

Table 7: Security Problem Definition to Objectives Correspondence

8.1.1.1 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.

According to the IDSSPP, T.NOHALT is addressed primarily by O.IDAUTH and O.ACCESS, which provide for authentication of users prior to accessing any TOE function, and permit only authorized users to access TOE functions. The IDSSPP states the O.IDSCAN (not included in this ST, as explained in Section 7.3), O.IDSENS, and O.IDANLZ objectives contribute to addressing this threat by requiring the TOE to collect and analyze System data, which includes attempts to halt the TOE. This would be accurate where the ST selected "Start-up and shutdown" in IDS_SDC.1.1a), and where the TOE was collecting System data related to itself. In this ST, the TOE collects only "network traffic", so the O.IDSENS and O.IDANLZ objectives have no supporting contribution to make to countering T.NOHALT.

8.1.1.2 T.FALREC

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

According to the IDSSPP, T.FALREC is addressed by O.IDANLZ, which provides the function that the TOE will recognize vulnerabilities or inappropriate activity from a data source. The modifications made to O.IDANLZ in this ST do not affect its ability to address this threat—the TOE has the objective to accept network traffic data from targeted IT system resources and to apply analytical processes to the collected data to derive conclusions about intrusions.

8.1.1.3 T.FALASC

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

According to the IDSSPP, T.FALASC is addressed by O.IDANLZ, which provides the function that the TOE will recognize vulnerabilities or inappropriate activity from multiple data sources. The modifications made to O.IDANLZ in this ST do not affect its ability to address this threat—the TOE has the objective to accept network traffic data from targeted IT system resources (the email infrastructure) and to apply analytical processes to the collected data to derive conclusions about intrusions.

8.1.1.4 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.

According to the IDSSPP, P.ANALYZ is addressed by O.IDANLZ, which requires analytical processes to be applied to data collected from Sensors and Scanners. The modifications made to O.IDANLZ in this ST do not affect its ability to address this threat—the TOE is an IDS System that combines the function of a Sensor and Analyzer and has the objective to accept network traffic data from targeted IT system resources (the Sensor capability) and to apply analytical processes to the collected data to derive conclusions about intrusions (the Analyzer capability).

8.1.1.5 P.PROTCT

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

The ST defines OE.CERTIFICATES to assist in satisfying this policy. The TOE supports SSH and TLS to provide for secure remote administration of the TOE and relies on the operational environment to provide the means by which the public key certificates that support SSH and TLS operations can be created and managed.

8.2 Security Functional Requirements Rationale

Section 6.3 of the IDSSPP provides rationale for the security functional requirements it specifies, demonstrating that the security functional requirements are suitable to address the defined security objectives. This rationale is valid for the PP requirements reproduced in the ST and is not further discussed.

This ST includes the following security functional requirements not included in the IDSSPP: FIA_UAU.5; FMT_SMF.1; and FPT_ITI.1. The following table maps these requirements to applicable TOE security objectives described in Section 4. Supporting rationale for these mappings is provided following the table.

	O.EADMIN	O.PROTCT	O.IDAUTH
FCS_CKM.1		X	
FCS_CKM.4		X	
FCS_COP.1(1)		X	
FCS_COP.1(2)		X	
FCS_COP.1(3)		X	
FIA_UAU.5			X
FMT_MTD.1(2)	X		
FMT_SMF.1	X		
FPT_ITI.1		X	

Table 8: Objectives to Requirement Correspondence

8.2.1.1 O.EADMIN

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

The following security functional requirements contribute to satisfying this security objective:

- FMT_SMF.1—the ST includes FMT_SMF.1 to specify the security management functions that are required to provide the capabilities for effective management of the TOE's functions and data
- FMT_MTD.1(2)—the ST includes an iteration of FMT_MITD.1 to specify the TOE's restriction on the security roles that can manage user accounts. This contributes to effective security management by reducing the scope for privilege escalation.

8.2.1.2 O.PROTCT

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

The following security functional requirement contributes to satisfying this security objective:

- FPT_ITI.1—the ST includes FPT_ITI.1 to specify that the TOE will protect the integrity of TSF data (i.e., signature updates) it downloads from a remote trusted IT product. If it detects the TSF data has been modified, it will ignore the data and request retransmission
- FCS_COP.1(3)—the ST includes FCS_COP.1(3) to specify the cryptographic hashing service used to support integrity protection for SSH and TLS, used to protect remote administrator communications
- FCS_COP.1(1), FCS_COP.1(2)—the ST includes FCS_COP.1(1) and FCS_COP.1(2) to specify the encryption and signature services that support SSH and TLS, used to protect remote administrator communications
- FCS_CKM.1, FCS_CKM.4—the ST includes FCS_CKM.1 and FCS_CKM.4 to specify the capabilities to generate symmetric encryption keys that support SSH and TLS, and to destroy keys that are no longer required (e.g., when an SSH or TLS session ends). These are supporting requirements for protecting remote administrator communications.

8.2.1.3 O.IDAUTH

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

The following security functional requirement contributes to satisfying this security objective:

- FIA_UAU.5—the ST includes FIA_UAU.5 to specify that the TOE can provide its own local authentication mechanism, or can be configured to authenticate user identities using a remote RADIUS or LDAP authentication server.

8.3 Security Assurance Requirements Rationale

The IDSSPP provides rationale for the security assurance requirements, demonstrating that they are sufficient given the statement of security environment and security objectives. The rationale is provided in Section 6.4 of the IDSSPP and is valid for this ST, as it does not define any new security environment statements or objectives.

EAL2 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate level of independently assured security. The TOE is targeted at an environment with good physical access security where it is assumed that attackers will have low attack potential. Augmentation was chosen to provide the added assurance that is provided by defining flaw remediation procedures. Therefore, the target assurance level of EAL 2 augmented with ALC_FLR.2 is appropriate for such an environment.

8.4 Requirement Dependency Rationale

The dependency requirements rationale is presented in Section 6.7 of the IDSSPP. The IDSSPP requirements have been evaluated and it has been determined that all dependencies have been satisfactorily addressed in the IDSSPP.

This ST includes security functional requirements not included in the IDSSPP. The following table identifies the dependencies of these security functional requirements in this ST.

ST Requirement	CC Dependencies	ST Dependencies
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1), FCS_CKM.4	FCS_COP.1(1), FCS_CKM.4
FCS_CKM.4	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FCS_CKM.1
FCS_COP.1(1)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1), FCS_CKM.4	FCS_CKM.1, FCS_CKM.4
FCS_COP.1(2)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1), FCS_CKM.4	**See rationale**
FCS_COP.1(3)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1), FCS_CKM.4	**See rationale**
FIA_UAU.5	none	none
FMT_MTD.1(2)	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	none	none
FPT_ITI.1	none	none

Table 9: Requirement Dependencies

The following rationale justifies the CC-defined dependencies that are not satisfied by the ST requirements:

- FCS_COP.1(2) dependency on (FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1), FCS_CKM.4: The TOE obtains the keys necessary to support RSA cryptography from the operational environment, and leaves all aspects of key and certificate management (including generation and destruction) up to the operational environment. This is covered by OE.CERTIFICATES
- FCS_COP.1(3) dependency on (FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1), FCS_CKM.4: FCS_COP.1(3) specifies a cryptographic hash mechanism (SHA-1). This is not a keyed mechanism, so the dependencies of FCS_COP.1 on requirements for generating or importing keys and destroying keys are not relevant.

8.5 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 functional 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.

8.6 PP Claims Rationale

See Section 7, Protection Profile Claims.