National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

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

IronPort Email Security Appliances

Report Number: CCEVS-VR-VID10438-2010
Dated: 1 December 2010
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

John Akins
Aerospace Corporation
Columbia, MD

Jandria Alexander
Aerospace Corporation
Columbia, MD

Jean Hung
Mitre Corporation
Bedford, MA

Common Criteria Testing Laboratory

Tammy Compton
Gary Grainger
Quang Trinh
Science Applications International Corporation
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of IronPort Email Security Appliances (ESA), (henceforth referred to as IronPort ESA). It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in November 2010. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 2 augmented with ALC_FLR.2.

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. In terms of the security functionality claimed within this ST, there is no difference between versions 7.1 and 7.3 of AsyncOS.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 3) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 2). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 2 augmented with ALC_FLR.2) have been met.

The technical information included in this report was obtained from the IronPort Email Security Appliances Security Target and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	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
Protection Profile	U.S. Government Protection Profile Intrusion Detection System System for Basic Robustness Environments, Version 1.7, July 25, 2007
ST:	IronPort Email Security Appliances Security Target, Version 1.0, November 29, 2010
Evaluation Technical Report	Evaluation Technical Report For the IronPort Email Security Appliances (Proprietary), Version 2.0, November 8, 2010

Item	Identifier
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 2
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco IronPort Systems LLC
Developer	Cisco IronPort Systems LLC
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validators	John Akins, Aerospace Corporation, McLean, VA
	Jandria Alexander, Aerospace Corporation, McLean, VA
	Jean Hung, Mitre Corporation, Bedford, MA

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1 TOE Introduction

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. 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.

They differ only in the number and speed of their network connections and their processing capacity (in terms of memory and processor speeds).

3.1.1 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.

3.2 TOE Architecture

3.2.1 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 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

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

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.

3.2.2 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.

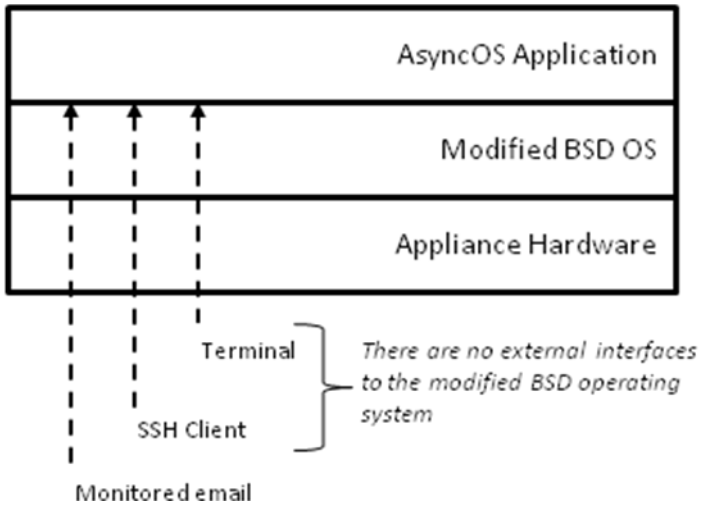

Figure 1: High-level TOE Architecture

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.

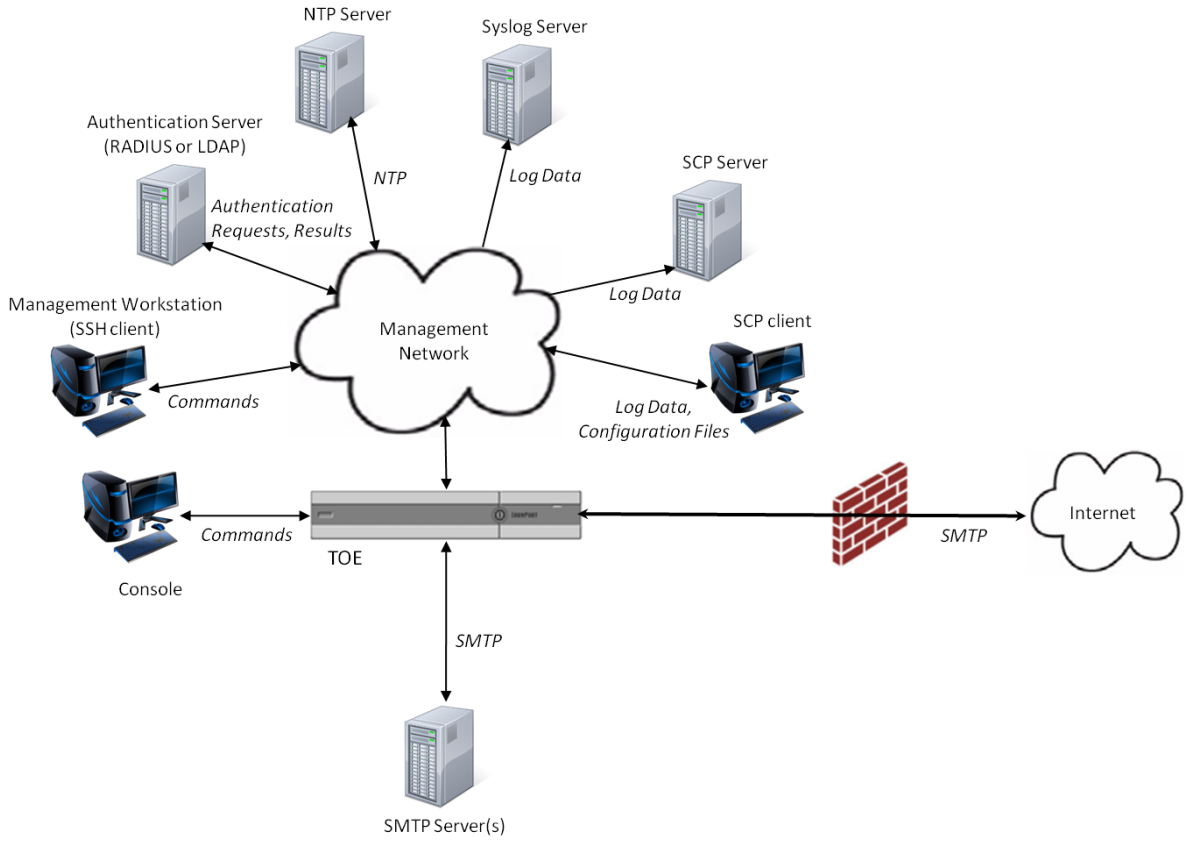

Figure 2: TOE Deployment Scenario

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.

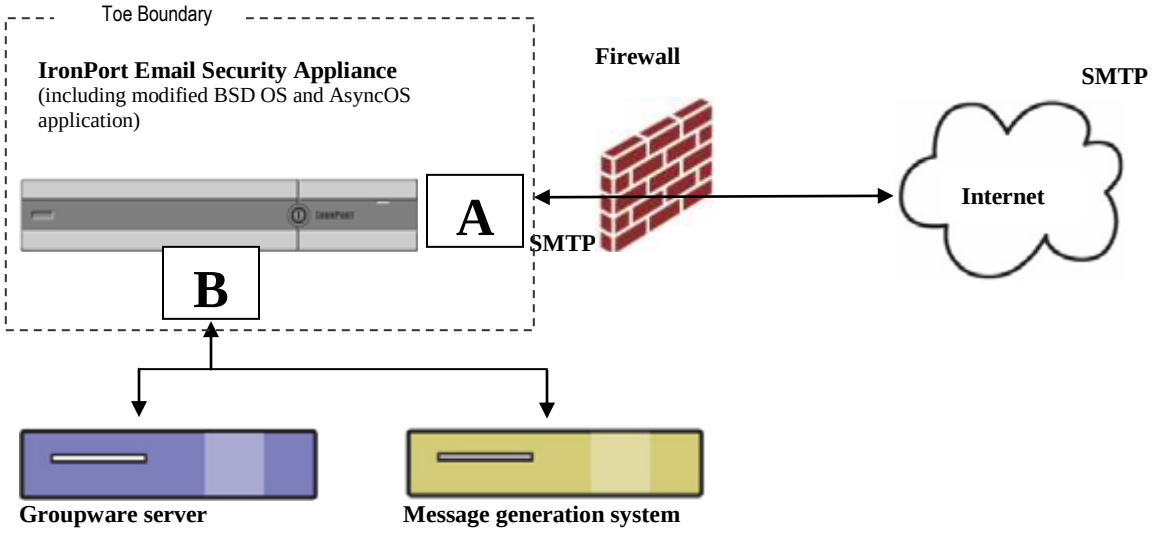

Figure 3: Typical TOE Deployment Configuration

Depending on the network configuration into which the TOE is installed, the firewall may need to be configured to allow access on various ports. The TOE Guidance documents outline the specific configuration settings that must be applied in the evaluated configuration. This includes required internet connectivity and port settings.

4 Security Policy

This section summaries the security functionality of the TOE:

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

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

5 Assumptions

The following assumptions were made during the evaluation of IronPort ESA:

- The TOE has access to all the IT System data it needs to perform its functions.
- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
- The TOE is appropriately scalable to the IT System the TOE monitors.
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- The TOE can only be accessed by authorized users.

6 Documentation

The following documentation was used as evidence for the evaluation of the IronPort ESA:

6.1 Design Documentation

1. Ironport Email Security Appliances TOE Design, Version 0.3, November 1, 2010
2. Ironport Email Security Appliances Functional Specification, Version 0.4, November 1, 2010
3. Ironport Email Security Appliances Security Architecture Specification, Version 0.3, November 1, 2010

6.2 Guidance Documentation

1. IronPort AsyncOS Common Criteria Guide for IronPort Appliances, Version 1.0, October 2010
2. 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
3. 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*

6.3 Life Cycle

1. Configuration Management, Lifecycle and Delivery Procedures for C160, C370, X1060, and X1070 appliance models, all running IronPort AsyncOS software, version 7.1 C670 appliance, running IronPort AsyncOS software, version 7.3, Version 3, EDCS-899942

6.4 Testing

1. Ironport Messaging Gateway Test Document (COV and FUN), 2010-09-01
2. IronPort_Test_Mappings.xls (090710)
3. Actual test Results

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the Cisco IronPort Email Security Appliances (ESA), Version 2.0, November 5, 2010.

7.1 Developer Testing

At EAL2, testing must demonstrate correspondence between the tests and the functional specification. The vendor testing addressed each of the security functions identified in the ST and interfaces in the design. These security functions include:

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

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the Common Criteria Guide, ran all of the developer tests and verified the results, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

The TSF uses MD5 to verify integrity of antivirus and antispam signature files. The TSF retrieves a manifest (file list with MD5 hash of each file) via HTTPS. It retrieves 3DES-encrypted signature files, decrypts them, and uses the MD5 hashes to verify the integrity of each decrypted file. During testing, the evaluation team focused on ensuring that the hash on the signature file was handled properly. During testing, the tester added characters to the end of the signature file. Then the server URL on the test ESA was set to the correct location for the test server.

On the test ESA, the IronPort tester (QA engineer) ran antivirusupdate. The test ESA successfully connected to the test signature server. It downloaded the identified signature file, computed the hash, and reported a checksum mismatch error in the antivirus log. The log message shows both the computed hash and the expected hash. The test ESA rejected the signature file.

While all TOE hardware models are functionally tested, only the C610 and C670 were included in the Common Criteria test configuration with test results/output recorded by Cisco. Since the code and hence security functionality is the same among the platforms, the evaluation team accepted this platform selection.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is IronPort Email Security Appliances solution including:

- C160, C370, X1060, and X1070 appliance models, running IronPort AsyncOS software, version 7.1
- C670 appliance model running IronPort AsyncOS version 7.3

To use the product in the evaluated configuration, the product must be configured as specified in the **IronPort AsyncOS Common Criteria Guide for IronPort Appliances, Version 1.0, October 2010** document.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL2 augmented with ALC_FLR.2 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1R2 and CEM version 3.1R2. The evaluation determined the IronPort ESA TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 2) augmented with ALC_FLR.2 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the IronPort ESA product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 2 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The ALC evaluation also ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation.

In addition to the EAL 2 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was

conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team performed a sample of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each EAL 2 VAN CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the entire vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

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.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *IronPort Email Security Appliances Security Target, Version 1.0, November 29, 2010*.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Science Applications International Corporation. *Evaluation Technical Report for the IronPort Email Security Appliances Part 2 (Proprietary)*, Version 2.0, November 8, 2010.

[7] Science Applications International Corporation. *Evaluation Team Test Report for the Cisco IronPort Email Security Appliances (ESA) Version 7.1 and 7.3, ETR Part 2 Supplement (SAIC and Cisco Proprietary)*, Version 2.0, November 5, 2010.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] IronPort Email Security Appliances Security Target, Version 1.0, November 29, 2010.