National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Cisco Email Security Appliance (ESA)

Report Number: CCEVS-VR-VID10581-2014
Version 1.0
November 13, 2014

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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Michael Allen, Senior Validator
The Aerospace Corporation

Jerome Myers, Senior Validator
The Aerospace Corporation

Kenneth Stutterheim, Lead Validator
The Aerospace Corporation

Common Criteria Testing Laboratory

Chris Gugel, CC Technical Director
Joshua Jones
Chris Rakaczky

Booz Allen Hamilton (BAH)
Linthicum Heights, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Email Security Appliance (ESA), provided by Cisco Systems, Inc. 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 Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Linthicum Heights, Maryland, United States of America, and was completed in October 2014. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements set forth in the Network Device Protection Profile (NDPP).

The Target of Evaluation (TOE) is the Cisco Email Security Appliance (ESA), with software version AsyncOS 8.0.2 build 63. The Cisco ESA TOE email protection product functionality was not evaluated as part of this evaluation.

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 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the NDPP. 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 is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes, and reviewed the individual work units of the ETR for the NDPP Assurance Activities. 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 technical information included in this report was obtained from the Cisco Email Security Appliance Security Target, Version 1.0, October 2014 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

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 Product Compliance 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	Cisco Email Security Appliance (ESA), with software version AsyncOS 8.0.2 build 63 *Refer to Table 2 for Models and Specifications
Protection Profile	Security Requirements for Network Devices, Version 1.1, 08 June 2012 (including the optional TLS, HTTPS, and SSH requirements) and Errata #2
Security Target	Cisco Email Security Appliance Security Target, Version 1.0, October 2014
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Cisco Email Security Appliance" Evaluation Technical Report v3.0 dated September 12, 2014
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Linthicum, Maryland
CCEVS Validators	Michael Allen, The Aerospace Corporation Jerome Myers, The Aerospace Corporation Kenneth Stutterheim, The Aerospace Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

3.2 Threats

The following lists the threats addressed by the TOE. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

- **T.ADMIN_ERROR** — An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- **T.TSF_FAILURE** — Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- **T.UNDETECTED_ACTIONS** — Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
- **T.UNAUTHORIZED_ACCESS** — A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- **T.UNAUTHORIZED_UPDATE** — A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- **T.USER_DATA_REUSE** — User data may be inadvertently sent to a destination not intended by the original sender.

3.3 Objectives

The following identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified.

- **O.PROTECTED_COMMUNICATIONS —** The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.

- **O.VERIFIABLE_UPDATES —** The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
- **O.SYSTEM_MONITORING —** The TOE will provide the capability to generate audit data and send those data to an external IT entity.
- **O.DISPLAY_BANNER —** The TOE will display an advisory warning regarding use of the TOE.
- **O.TOE_ADMINISTRATION —** The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
- **O.RESIDUAL_INFORMATION_CLEARING —** The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
- **O.SESSION_LOCK —** The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
- **O.TSF_SELF_TEST —** The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly**.**

3.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Security Requirements for Network Devices, Version 1.1, 08 June 2012 (including the optional TLS, HTTPS, and SSH requirements) with Errata #2 to which this evaluation claimed exact compliance.

- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

The evaluated configuration of the TOE includes the Cisco Email Security Appliance (ESA), with software version AsyncOS 8.0.2 build 63 product that is comprised of one or more of the product models. The TOE includes all the code that enforces the policies identified (see Section 5). The mail protection functionality was not evaluated as part of this evaluation.

The Non-FIPS 140-2 mode of operation is excluded from the evaluation. This mode will be disabled by configuration. The exclusion of this functionality does not affect compliance to the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1.

4 Architectural Information

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

4.1 TOE Introduction

The Target of Evaluation (TOE) is the Email Security Appliance (ESA). The TOE consists of one or more models as specified in Section 4.2 below and includes the software version AsyncOS 8.0.2 build 63.

4.2 Physical Boundaries

The TOE is comprised of both software and hardware. The hardware is comprised of the following: C170, C370, C670, X1070, C380, C680, and C000v, C100v, C300v, C600v running on Cisco UCS servers (blade or rack-mounted).

Table 2 – Hardware Models and Specifications

Model	X1070	C680	C670	C380	C370	C170	C000v	C100v	C300v	C600v
Processor	2x4 (2 quad cores)	2x6 (2 hexa cores)	2x4 (2 quad cores)	1x6 (1 hexa core)	1x4 (1 quad core)	1x2 (1 Dual Core)	UCS B-Series[1] or UCS C-Series[2] running ESXi 5.1 or 5.5	UCS B-Series[1] or UCS C-Series[2] running ESXi 5.1 or 5.5	UCS B-Series[1] or UCS C-Series[2] running ESXi 5.1 or 5.5	UCS B-Series[1] or UCS C-Series[2] running ESXi 5.1 or 5.5
Memory	4 GB	32 GB	4 GB	16 GB	4 GB	4 GB				
Hard disk	1.8 TB (300 x 6), RAID 10	1.8 TB (600 x 3), RAID 10	1.2 TB (300 x 4), RAID 10	1.2 TB (600 x 2), RAID 10	600 GB (300 x 2), RAID 1	250 GB, RAID 1				

[1] See the UCS B-Series data sheets for details on the interfaces
[2] See the UCS C-Series data sheets for details on the interfaces

Model	X1070	C680	C670	C380	C370	C170	C000v	C100v	C300v	C600v
Interfaces/UCS Server	(1) USB Console Port (1) Serial Console Port (1) Management Port (3) 10/100/1000 Port	(2) USB Console Port (1) Console Port (RJ-45 connector) (1) Management Port (4) 10/100/1000 Port (2) Power Supply (1) Remote Power Management Port	(1) USB Console Port (1) Serial Console Port (1) Management Port (3) 10/100/1000 Port (2) Power Supply	(2) USB Console Port (1) Console Port (1) Management Port (4) 10/100/1000 Port (2) Power Supply (1) Remote Power Management Port	(1) USB Console Port (1) Serial Console Port (1) Management Port (4) 10/100/1000 Port (2) Power Supply	(2) USB Console Port (1) Console Port (1) Management Port (2) 10/100/1000 Port (1) Power Supply				

The TOE resides on a network and supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 3 – IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Management Workstation using web browser for HTTPS	Yes	This includes any IT Environment Management workstation with a web browser installed that is used by the TOE administrator to support TOE administration through HTTPS protected channels. Any web browser that supports TLSv1.0 with the supported ciphersuites may be used.
Local Console	No	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
NTP Server	No	The TOE supports communications with an NTP server in order to synchronize the date and time on the TOE with the NTP server's date and time. A solution must be used that supports secure communications with up to a 32 character key.
SMTP Server	Yes	This includes the IT environment SMTP servers that the TOE receives and sends email.
Syslog Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages.
Update Server	No	This includes the Cisco IT environment update servers that are used to download the latest software updates for the TOE.

5 Security Policy

5.1 Security Audit

The Cisco Email Security Appliance provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco Email Security Appliance generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE provides the administrator with a circular audit trail or a configurable audit trail threshold to track the storage capacity of the audit trail. Audit logs are backed up over an encrypted channel to an external audit server.

5.2 Cryptographic Support

The TOE provides cryptography in support of other Cisco ESA security functionality. This cryptography has been validated for conformance to the requirements of FIPS 140-2 Level 2 (see Table 4 for certificate references).

Table 4 FIPS References

Algorithm	Cert. #
AES	1759
DSA	550
ECDSA	234
HMAC	1031
RNG	937
RSA	876
SHS (SHA-1)	1544

The TOE provides cryptography in support of remote administrative management via SSHv2. The cryptographic services provided by the TOE are described in Table 5 below.

Table 5 TOE Provided Cryptography

Cryptographic Method	Use within the TOE
Secure Shell Establishment (SSH)	Used to establish initial SSH session.
Transport Layer Security (TLS)	Used in TLS session establishment.
AES	Used to encrypt TLS session traffic. Used to encrypt SSH session traffic.
RSA Signature Services	Used in TLS session establishment. Used in SSH session establishment. X.509 certificate signing
HMAC	Used for keyed hash, integrity services in TLS an SSH session establishment.

Cryptographic Method	Use within the TOE
RNG	Used for random number generation Used in TLS session establishment. Used in SSH session establishment.
SHS (SHA-1)	Used to provide TLS traffic integrity verification Used to provide SSH traffic integrity verification

5.3 User Data Protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Packets are padded with zeros. Residual data is never transmitted from the TOE.

5.4 Identification and Authentication

The TOE performs two types of authentication: device-level authentication of remote Message Transfer Agents (MTA) and user authentication for the Authorized Administrator of the TOE. Device-level authentication allows the TOE to establish a secure channel with another MTA over TLS. The secure channel is established only after each device authenticates the other with an X.509v3 certificate.

The TOE provides authentication services for administrative users wishing to connect to the TOE's secure CLI and GUI administrative interfaces. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality.

The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules that includes special characters. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or remote interfaces. The SSHv2 interface also supports authentication using SSH keys. The remote GUI is protected using TLS.

5.5 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection. The TOE provides the ability to securely manage:

- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE;
- Update to the TOE; and
- TOE configuration file storage and retrieval.

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.

Administrators can create configurable login banners to be displayed at time of login, and can also define an inactivity timeout for each admin interface to terminate sessions after a set period of inactivity.

5.6 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually, or can configure the TOE to use NTP to synchronize the TOE's clock with an external time source. Finally, the TOE performs testing to verify correct operation of the appliance itself and that of the cryptographic module.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

5.7 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display an Authorized Administrator specified banner on the CLI and GUI management interfaces prior to allowing any administrative access to the TOE.

5.8 Trusted Path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 for remote CLI access and HTTPS for remote GUI access. The TOE can push log files to an external syslog server using SCP over SSH.

6 Documentation

The vendor provides guidance documentation on their support website, http://www.cisco.com/web/strategy/government/security_certification/net_business_benefit_seccert_common_criteria.html. The following documentation located on their support website was used as evidence for the evaluation of the Cisco Email Security Appliance (ESA):

- *Cisco IronPort Email Security Appliance, CC Configuration Guide, Version 1.0*

There are many documents available on the support website, but the above mentioned document is the only one that is to be trusted as having been part of the evaluation.
This guidance document contains the security-related guidance material for this evaluation and must be referenced to place the product within the Common Criteria evaluated configuration. The guidance document is applicable for all models of the ESA product claimed by this evaluation. Additionally, the guidance document contains references and pointers to other TOE guidance documentation for additional detail regarding the security-related functionality. These references were also examined during the evaluation.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is one or more Cisco Cisco Email Security Appliance (ESA), with software version AsyncOS 8.0.2 build 63.

To use the product in the evaluated configuration, the product must be configured as specified in the *Cisco IronPort Email Security Appliance, CC Configuration Guide, Version 1.0* document. Refer to Section 6 for information on where to retrieve the document from Cisco's support website and how to use this document to configure the TOE into the evaluated configuration.

8 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 Technical Report for a Target of Evaluation "Cisco Email Security Appliance" Evaluation Technical Report v3.0 dated September 12, 2014*, which is not publically available. The *Assurance Activities Report for a Target of Evaluation Cisco Email Security Appliance Security Target (Version 1.0) dated September 12, 2014* provides an overview of testing and the prescribed assurance activities.

8.1 Test Configuration

The evaluation team configured each tested model of the TOE according the *Cisco IronPort Email Security Appliance, CC Configuration Guide, Version 1.0* document for testing. The following TOE models were tested:

- C370
- C100v on a UCS C-Series C240M3 running ESXi 5.5

The following environment components and test tools* were utilized during the testing:

- Syslog Server: rsyslog 5.8.6-1ubuntu8.1 (note: this is an extension to sysklogd 1.5-6ubuntu1) was used for testing
- NTP Server: ntp_4.2.6.p3+dfsg-1ubuntu3.1_i386
- WireShark: version 1.12.1
- Bitvise SSH Client: version 4.60

*Only the test tools utilized for functional testing have been listed.

8.2 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the Cisco Email Security Appliance (ESA) by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the NDPP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or

observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.4 Evaluation Team Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The evaluation team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Eavesdropping on Communications
  In this test, the evaluators manually inspected network traffic to and from the TOE in order to ensure that no useful or confidential information could be obtained by a malicious user on the network.
- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.
- Web Interface Vulnerability Identification (Burp Suite)
  Burp Suite is a web application vulnerability assessment tool suite. Burp looks for major vulnerabilities including cross-site scripting, SQL injection, directory traversal, unchecked file uploads, etc. as well as less critical vulnerabilities such as unnecessary information disclosure.
- SSH Timing Attack (User Enumeration)
  This attack attempts to enumerate validate usernames for the SSH interface, by observing the difference in server response times to valid username login attempts.

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 documents, the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that all Assurance Activities and 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 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Cisco Email Security Appliance (ESA) TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

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 Cisco Email Security Appliance (ESA) product that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Assurance Activities specified in the Security Requirements for Network Devices Protection Profile (NDPP).

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 1 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 contained in the Security Target's TOE Summary Specification as well as a separately developed Functional Specification document. Additionally the evaluator performed the Assurance Activities specified in the NDPP related to the examination of the information contained in the TOE Summary Specification.

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 Assurance Activities, 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 1 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. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities specified in the NDPP related to the examination of the information contained in the operational guidance documents.

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 Assurance Activities, 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 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

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 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDPP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with 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 addressed the vulnerability analysis Assurance Activities in the NDPP, 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 test activities 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 performed the Assurance Activities in the NDPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the ESA TOE being configured for FIPS operation.

The evaluated software version of the TOE is AsyncOS 8.0.2 build 63. If a prior version of AsyncOS 8.0.2 is loaded on the TOE, the administrator should patch the TOE to build 63 or later. User installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; and with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration, thus, an IAR is not required.

The validation team cautions that administrators should always check the current version of software that is installed on the TOE after performing patch updates. When performing the software update process during the evaluation, it was determined that the TOE would indicate that the update process had completed but the provided audit records were ambiguous as to when the software was installed correctly or the software was not installed because it did not pass the hash checksum verification.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *Cisco Email Security Appliance Security Target, Version 1.0, October 2014*.

13 List of Acronyms

Acronym	Definition
ACL	Access Control Lists
AES	Advanced Encryption Standard
BRI	Basic Rate Interface
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CSU	Channel Service Unit
DHCP	Dynamic Host Configuration Protocol
DSU	Data Service Unit
EAL	Evaluation Assurance Level
EHWIC	Ethernet High-Speed WIC
ESP	Encapsulating Security Payload
GE	Gigabit Ethernet port
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	*Internet Control Message Protocol*
ISDN	*Integrated Services Digital Network*
ESA	Email Security Appliance
IT	Information Technology
MTA	Mail Transfer Agent
NDPP	Network Device Protection Profile
OS	Operating System
PBKDF2	Password-Based Key Derivation Function version 2
PoE	Power over Ethernet
POP3	Post Office Protocol
PP	Protection Profile
SA	Security Association
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
SIO	Cisco Security Intelligence
SIP	Session Initiation Protocol
SSHv2	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
WAN	Wide Area Network
WIC	WAN Interface Card

14 Terminology

Terminology	Definition
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.
Role	An assigned role gives a user varying access to the management of the TOE.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Vty	vty is a term used by Cisco to describe a single terminal (whereas Terminal is more of a verb or general action term).

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Cisco Email Security Appliance Security Target, Version 1.0, October 2014.
6. Evaluation Technical Report for a Target of Evaluation "Cisco Email Security Appliance" Evaluation Technical Report v3.0 dated September 12, 2014.
7. Cisco IronPort Email Security Appliance, CC Configuration Guide, Version 1.0.
8. Assurance Activities Report for a Target of Evaluation, Cisco Email Security Appliance, Security Target (Version 1.0) Assurance Activities Report, Version 1.0, dated September 12, 2014