Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Cisco Adaptive Security Appliances

Certification Report
2015/93

21 July 2015
Version 1.0

Amendment Record

Version	Date	Description
0.1	15 July 2015	Internal
1.0	21 July 2015	Public release

Executive Summary

This report describes the findings of the IT security evaluation of Cisco Adaptive Security Appliances (ASA) version 9.4(1) against Common Criteria and Protection Profiles.

The Target of Evaluation (TOE) is the Cisco Adaptive Security Appliances which is a purpose-built firewall platform with VPN capabilities.

For firewall services, the ASA 5500-X (low to mid-range), 5585-X (high-end) and ASA-SM Series all provide application-aware stateful packet filtering firewalls. A stateful packet filtering firewall controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connection-less IP packets against a set of rules specified by the authorised administrator for firewalls.

The Cisco ASA also provides IPsec connection capabilities. All references within the ST and this document to "VPN" connectivity refer to the use of IPsec tunnels to secure connectivity to and/or from the TOE, for example, gateway-to-gateway VPN or remote access VPN.
Other uses refer to the use of IPsec connections to tunnel traffic that originates from or terminates at the ASA itself, such as for transmissions from the ASA to remote audit/syslog servers, or AAA servers, or for an additional layer of security for remote administration connections to the ASA, such as SSH or TLS connections tunnelled in IPsec.

For management purposes, the ASDM is included. ASDM allows the ASA to be managed from a graphical user interface.

The report concludes that the product has complied with the Security Requirements for Network Devices, version 1.1 (NDPP) (with Errata#3), Network Device Protection Profile Extended Package Stateful Traffic Filter Firewall version 1.0 (FWEP) and Network Device Protection Profile Extended Package VPN Gateway version 1.1 (VPNGWEP) and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP).

The evaluation was performed by CSC and was completed on 23 June 2015.

With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled.
b) Configure and Operate the TOE according to the vendor's product administrator guidance.
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved.
d) The ASDM, the management software, terminates the connection with the TOE after the defined connection timeout period. However, it continues to

e) When updating the TOE's image, ensure that the administrator verify the hash of the downloaded software as present on the vendor website.

This report includes information about the underlying security policies and architecture of the TOE and information regarding the conduct of the evaluation.
It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 – Introduction

1.1 Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

The purpose of this Certification Report is to:

a) Report the certification of results of the IT security evaluation of the Cisco Adaptive Security Appliances against the requirements of the Common Criteria (CC), the NDPP v1.1 (with Errata#3), the FWEP v1.0 and the VPNGWEP v 1.1.

b) Provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target (Ref 9) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

The TOE is the Cisco Adaptive Security Appliances with the version information specified below.

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	Cisco Adaptive Security Appliances
Software Version	ASA 9.4(1) and ASDM 7.4
Hardware Platforms	ASA 5500-X Series (5512-X, 5515-X, 5525-X, 5545-X, 5555-X), ASA 5585-X Series (5585-X SSP-10, 5585-X SSP-20, 5585-X SSP-40, 5585-X SSP-60) ASA Services Module (ASA-SM) on Catalyst 6500 series switches including 6503-E, 6504-E, 6509-E and 6513-E

Security Target	Security Target for Cisco Adaptive Security Appliances, Version 3.0, 7 July 2015
Evaluation Technical Report	Evaluation Technical Report Cisco Adaptive Security Appliances, Version 1.0, dated 8 July 2015 Document reference: CSC-EFC-T0083-ETR
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, September 2012, Version 3.1, Revision 4
Methodology	Common Methodology for Information Technology Security, dated September 2012, Version 3.1, Revision 4
Conformance	U.S Government Protection Profile for Security Requirements for Network Devices (NDPP) Version 1.1, 08 June 2012 US Government Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall (TFFWEP) Version 1.0, 19 Dec 19 2011 US Government Network Device Protection Profile (NDPP) Extended Package VPN Gateway (VPNGW), Version 1.1, 12 April 2013 Security Requirements for Network Devices Errata #3, 3 November 2014
Vendor	Cisco Systems, Inc 170 West Tasman Drive, San Jose, California, United States
Evaluation Facility	CSC AUSTRALIA PTY LIMITED 217 Northbourne Ave Turner ACT 2612 Australia

Chapter 2 – Target of Evaluation

2.1 Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, security policies and its secure usage.

2.2 Description of the TOE

This section provides an overview of the Cisco Adaptive Security Appliances Target of Evaluation (TOE). The TOE is comprised of both software and hardware. The TOE is comprised of the following: ASA 5500-X Series (5512-X, 5515-X, 5525-X, 5545-X, 5555-X), ASA 5585-X Series (5585-X SSP-10, 5585-X SSP-20, 5585-X SSP-40, 5585-X SSP-60) and ASA Services Module (ASA-SM). The software is comprised of the Adaptive Security Appliance software image Release 9.4(1), with ASDM 7.4.

The Cisco Adaptive Security Appliances that comprise the TOE have common hardware characteristics. These differing characteristics affect only non-TSF relevant functionality (such as throughput, processing speed, number and type of network connections supported, number of concurrent connections supported and amount of storage) and therefore support security equivalency of the ASAs in terms of hardware.

2.3 TOE Functionality

The TOE provides the following security functionality:

A. Security Audit

The TOE can generate can audit events and create records related to cryptographic functionality, identification and authentication and administrative actions. The administrator can configure events, performs back-up operations and manages audit data storage.

B. Cryptographic support

The TOE provides cryptography in support of VPN connections using TLS and IPsec and remote administrative management via SSHv2 and TLS/HTTPS. The cryptographic random bit generators (RBGs) are seeded by an entropy noise source.

C. Full Residual Information 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.

D. Identification and authentication

The TOE performs two types of authentication: device-level authentication of the remote device (VPN peers) and user authentication for the authorised administrator of the TOE.

The TOE requires authorised 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. Password-based authentication can be performed on the serial console or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys. The TOE optionally supports use of a RADIUS or TACACS+ AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE's CLI.

E. 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 or TLS 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; and TOE configuration file storage and retrieval.

F. 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 authorised administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally Cisco ASA is not a general-purpose operating system and access to Cisco ASA memory space is restricted to only Cisco ASA functions.
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.

G. Trusted path/Channels

The TOE supports establishing trusted paths between itself and remote administrators using SSHv2 for CLI access and TLS for GUI/ASDM access. The TOE supports use of TLS and/or IPsec for connections with remote syslog servers. The TOE can use IPsec to encrypt connections with remote authentication servers (e.g. RADIUS or TACACS+). The TOE can establish trusted paths of peer-to-peer VPN tunnels using IPsec and VPN client tunnels using IPsec or TLS.

H. Firewall

The TOE provides stateful traffic firewall functionality including IP address-based filtering (for IPv4 and IPv6) to address the issues associated with unauthorised disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services and network-based reconnaissance. Address filtering can be configured to restrict the flow of network traffic between protected networks and other attached networks based on source and/or destination IP addresses. Port filtering can be configured to restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) and/or receiving (destination) port (service). Stateful packet inspection is used to aid in the performance of packet flow through the TOE and to ensure that only packets are only forwarded when they are part of a properly established session. The TOE supports protocols that can spawn additional sessions in accordance with the protocol RFCs where a new connection will be implicitly permitted when properly initiated by an explicitly permitted session. The File Transfer Protocol is an example of such a protocol, where a data connection is created as needed in response to an explicitly allowed command connection. System monitoring functionality includes the ability to generate audit messages for any explicitly defined (permitted or denied) traffic flow. TOE administrators have the ability to configure permitted and denied traffic flows, including adjusting the sequence in which flow control rules will be applied and to apply rules to any network interface of the TOE.

I. VPN

The TOE also provides packet filtering and secure IPsec tunnelling. The tunnels can be established between two trusted VPN peers as well as between remote VPN clients and the TOE. More accurately, these tunnels are sets of security associations (SAs). The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per the ESP security protocol. An authorised administrator can define the traffic that needs to be protected via IPsec by configuring access lists.

2.4 TOE Architecture

Refer to the Security Target (Ref 9) for an architectural description of the TOE and the TOE environment.

2.5 Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per the Cisco Adaptive Security Appliance (ASA) 9.4 (1) Preparative Procedures and Operational User Guide for the Common Criteria Certified Configuration, Version 3.1, 7 July 2015 (Ref 10).

The scope of the evaluation was limited to those claims made in the Security Target (Ref 9).

2.5.1 Evaluated Functionality

The TOE is comprised of several security features including stateful traffic firewall and VPN gateway. Each of the security features identified above consists of several security functionalities as identified below:

- Security Audit
- Cryptographic Support
- Full Residual Information Protection
- Identification and Authentication
- Security Management
- TOE Access
- Trusted Path/Channels
- Filtering

These evaluated security functionalities are described in more detail in section 1.6 of the Security Target (Ref 9).

2.5.2 Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration. Australian Government users should refer to Australian Government Information Security Manual (ISM) (Ref 8) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

Excluded Functionality

The following functionality is excluded from the evaluation.

Table 2 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Secure Policy Manager is excluded from the evaluated configuration	Use of Security Policy Manager is beyond the scope of this Common Criteria evaluation.

Filtering of non-IP traffic provided by the EtherType option when configuring information flow policies is excluded from the evaluated configuration	Use of non-IP traffic filtering is beyond the scope of this Common Criteria evaluation.
Smart Call Home. The Smart Call Home feature provides personalised, e-mail-based and web-based notification to customers about critical events involving their individual systems.	Use of Smart Call Home is beyond the scope of this Common Criteria evaluation.

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the selected Protection Profiles.

2.6 Security

2.6.1 Security Policy

The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected.

This evaluation was performed against U.S Government Protection Profile for Security Requirements for Network Devices (NDPP) Version 1.1, Errata #3, 3 Nov 2014, the US Government Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall (TFFWEP) Version 1.0, 19 Dec 2011 and the US Government Network Device Protection Profile (NDPP) Extended Package VPN Gateway (VPNGW), Version 1.1, 12 April 2013, therefore no Security Policy Model was provided for the TOE.

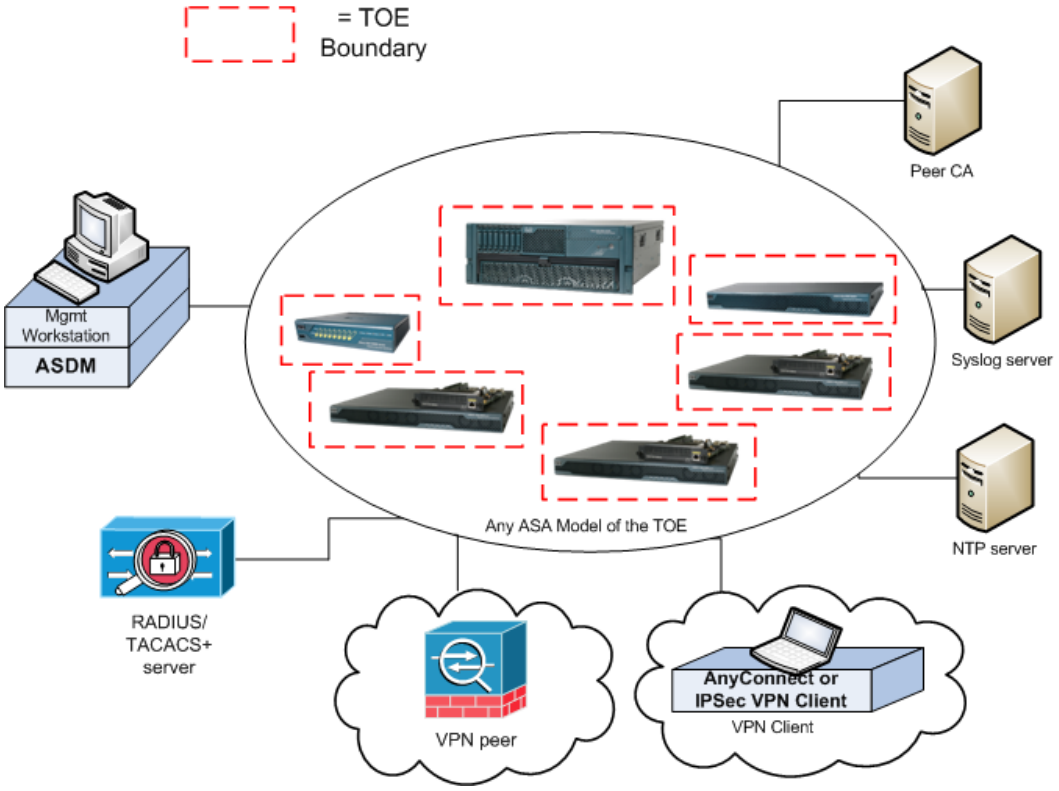
2.7 Usage

2.7.1 Evaluated Configuration

The TOE consists of one or more physical devices as specified in the figure below and includes the Cisco ASA software, which in turn includes the ASDM software. Each instantiation of the TOE has two or more network interfaces and is able to filter IP traffic to and through those interfaces.
The TOE can optionally connect to an NTP server for clock updates. If the TOE is to be remotely administered, the management station must connect using SSHv2. When ASDM is used a remote workstation with a TLS-enabled browser must be available. A syslog server can also be used to store audit records and the syslog server must support syslog over TLS or IPsec. The TOE is able to filter connections to/from these external using its IP traffic filtering and can encrypt traffic where necessary using TLS, SSH and/or IPsec.

More information about the hardware and software components that comprise the TOE as well as the environmental components that supported the evaluated configuration of the TOE are described in the section one of the Security Target (Ref 9).

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a hashed red line.



2.7.2 Secure Delivery

To ensure that the software received is the evaluated product the customer must check the version details received against the list specified in the TOE. The customer should perform the following checks to ensure that they have received the correct version of the TOE.

Shipment of units from Cisco Distributors to the user is via a commercial courier company who will pick up the unit from the Distribution Site and deliver it directly to the user.

For hardware components; using the packing slip and information on the stickers, the customer must check that the product number and serial numbers on the received hardware match what was ordered. Any discrepancies must be immediately reported to Cisco using the contact information on the packing slip.

For Software, the customer will access CCO (Cisco Connection Online) to download images. Customers will be prompted for their login and password. To create an account on CCO a user must have a valid support contract with Cisco and access to the contract number. Access control on the CCO site controls what software images a user account is allowed to download.

Encryption using SSL protects the software images as they are being downloaded from the Cisco web server to the user's computer.

2.7.3 Installation of the TOE

Installation and start up of the TOE such that it is in evaluated configuration is detailed for the consumer in the document, Cisco Adaptive Security Appliance (ASA) 9.4 (1) Preparative Procedures and Operational User Guide for the Common Criteria Certified Configuration, Version 3.1, 7 July 2015 (Ref 10).

2.8 Version Verification

To ensure the hardware received is the evaluated product the customer must check the models received against the list of TOE component hardware models at the beginning of the PRE wrapper document. This document is made available on the Cisco website for download.

In addition to verifying model numbers for hardware components, the software versions must also be verified by the customer recipient. Software versions can be checked by following the “Identifying the Evaluated Hardware and Software” instruction included in the user guidance.

When updates are made available by Cisco, an administrator can obtain and install those updates. Digital signatures are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to update the applicable TOE components. Instructions for how to do this verification are provided in the administrator guidance for this evaluation.

2.9 Documentation and Guidance

The following documents are available to the consumer when the TOE is purchased. Cisco does not ship hard copies of guidance documents with the product rather all guidance material is available for download online at www.cisco.com.

The guidance document: *Cisco Adaptive Security Appliance (ASA) 9.4(1) Preparative Procedures & Operational User Guide for the Common Criteria Certified configuration, dated 7 July 2015, Version 3.1* (Ref 10) provides information regarding the key configuration requirements for the TOE components.

All common criteria guidance material is available at **www.commoncriteriaportal.org**. The Information Security Manual (ISM) is available at **www.asd.gov.au**.

2.10 Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

The specific conditions listed in the following table are assumed to exist in the TOE’s environment. These assumptions include both practical realities in the development of

the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 3 Assumptions

Assumption	Assumption Definition
Reproduced from the NDPP	
A.NO_GENERAL_PURPOSE	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.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
Reproduced from the TFFWEP and VPNGWEP	
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

Chapter 3 – Evaluation

3.1 Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

3.2 Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the NDPP (Ref 5), FWEP (Ref 6), VPNGWEP (Ref 7), Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 3, Parts 2 and 3 (Refs 2 and 3).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4 (Ref 4).

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP).

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security were also upheld.

The evaluation was based on the default installation and configuration of the TOE with additional configuration taken from the Preparative Procedures & Operational User Guide for the Common Criteria Certified configuration (Ref 10).

3.3 Testing

3.3.1 Testing Coverage

All tests performed by the evaluators were taken from the NDPP, FWEP and VPNGWEP. These tests are designed in such a way as to provide a full coverage of testing for all security functions claimed by the TOE. All SFRs listed in the Security Target and the Protection Profile packages were exercised during testing.

3.3.2 Testing method used

Testing is determined by the Assurance activities outlined in the Protection Profile and Extended Packages.

Sampling

In terms of selecting the hardware and software sample to undergo independent testing the evaluators considered the various components comprising the TOE can run on multiple hardware platforms, however in all cases there is only a single version of software available the ASA hardware components.

In addition to this, the variation in choice of hardware platforms is in relation to only non-TSF relevant functionality (such as throughput, processing speed, number and

type of network connections supported, number of concurrent connections supported and amount of storage). There are no differences in the SFR enforcing subsystems of the TOE.

3.4 Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report (Ref 13).

3.5 Penetration Testing

The developer performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly-available information.

The evaluators researched the relevant protocols and technologies in their search for vulnerabilities. Additionally the evaluators explored security sites for public domain exploits and vulnerabilities.

The evaluators performed penetration testing taking into account the following factors:

a) Time taken to identify and exploit (elapsed time)

b) Specialist technical expertise required (specialist expertise)

c) Knowledge of the TOE design and operation (knowledge of the TOE)

d) Window of opportunity

e) IT hardware/software or other equipment required for the exploitation.

Chapter 4 – Certification

4.1 Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

4.2 Assurance

This certification is focused on the evaluation of product compliance with a Protection Profile that covers the technology area of network devices. Agencies can have confidence that the scope of an evaluation against an ASD approved Protection Profile covers the necessary security functionality expected of the evaluated product and known security threats will have been addressed.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with Protection Profiles (PPs). PPs provide assurance by a full security target and an analysis of the SFR in that ST, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by testing as outlined in the NDPP, FWEP and VPNGWEP assurance activities and a vulnerability analysis (based upon TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

Compliance also provides assurance through evidence of secure delivery procedures.

4.3 Certification Result

After due consideration of the conduct of the evaluation as reported to the certifiers and of the Evaluation Technical Report (Ref 11), the Australasian Certification Authority **certifies** the evaluation of the Cisco ASA product performed by the Australasian Information Security Evaluation Facility, CSC.

CSC **has determined** that the Cisco ASA uphold the claims made in the Security Target (Ref 9) and **has met** the requirements of the NDPP, FWEP and VPNGWEP.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with Protection Profiles.

The analysis is supported by testing as outlined in the NDPP, FWEP and VPNGWEP assurance activities and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures. Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref 8) and New Zealand Government users should consult the GCSB.

In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed, the ACA also recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled.
b) Configure and operate the TOE according to the vendor's product administrator guidance.
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved.
d) The ASDM, the management software, terminates the connection with the TOE after the defined connection timeout period. However, it continues to allow viewing of the running configuration, although the administrator is not able to make any changes to the TOE. We recommend that the administrator close the management session window by logging out when not in use.
e) When updating the TOE's image, ensure that the administrator verify the hash of the downloaded software as present on the vendor website.

Annex A – References and Abbreviations

A.1 References

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4

2. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, dated September 2012, Version 3.1 Revision 4

3. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, dated September 2012, Version 3.1 Revision 4

4. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, dated September 2012, Version 3.1, Revision 4.

5. US Government approved Protection Profile – Protection Profile for Network Devices (NDPP) version 1.1 June 8, 2012

6. US Government approved Network Devices Protection Profile – Protection Profile Stateful Traffic Filter Firewall Extended Package (FWEP) Version 1.0 December 2011

7. US Government Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, 12 April 2013 (VPNGWEP)

8. 2015 Australian Government Information Security Manual (ISM), Australian Signals Directorate

9. Security Target for Cisco Adaptive Security Appliances (ASA) 9.4(1), dated 7 July 2015, Version 3.1

10. Cisco Adaptive Security Appliance (ASA) 9.4(1) Preparative Procedures & Operational User Guide for the Common Criteria Certified configuration, dated 7 July 2015, Version 3.1

11. Evaluation Technical Report for Cisco Adaptive Security Appliances (ASA) 9.4(1), CSC-EFC-T0083-ETR, dated 8 July 2015, Version 1.0

12. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014.

13. Cisco ASA Entropy information, dated May 2015, Version 1.0

14. NIST publication SP800-90A Recommendations for Random Number Generation Using Deterministic Random Bit Generation, January 2012.

A.2 Abbreviations

ASDM	Adaptive Security Device Manager
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CA	Certification Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GCSB	Government Communications Security Bureau
ISM	Information Security Manual
NTP	Network Time Protocol
NDPP	US Government approved Protection Profile for Network Devices
PP	Protection Profile
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
VPN	Virtual Private Network