Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Cisco ASA 9.4(1.13), ASAv 9.4(1.240) and ASDM 7.4

Certification Report
2016/102

10-11-2016
Version 1.0

Amendment Record

Version	Date	Description
1.0	10-11-2016	Final

Executive Summary

This report describes the findings of the IT security evaluation of Cisco Adaptive Security Appliances (ASA) 9.4(1.13), Cisco Adaptive Security Appliances Virtual (ASAv) 9.4(1.240) and ASDM 7.4 against Common Criteria and Protection Profiles.

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

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Security Audit –**The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. 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.

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

- **Full residual information protection –** The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic.

- **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. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec X509v3 certificate based authentication or pre-shared key methods. The TOE provides authentication services for administrative users wishing to connect to the TOEs secure CLI and GUI administrator interfaces. 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. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH and HTTPS interfaces. The SSHv2 interface also supports authentication using SSH keys. The TOE optionally supports use of any RADIUS AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE.

- **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/HTTPS 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; TOE configuration file storage and retrieval, and the information flow control policies enforced by the TOE including encryption/decryption of information flows for VPNs. The TOE supports an "authorised administrator" role, which equates to any account authenticated to an administrative interface (CLI or GUI, but not VPN), and possessing sufficient privileges to perform security-relevant administrative actions. When an administrative session is initially established, the TOE displays an administrator- configurable warning banner. After a configurable period of inactivity, administrative sessions will be terminated, requiring administrators to re-authenticate.

- **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.

- **TOE Access –** When an administrative session is initially established, the TOE displays an administrator- configurable warning banner. This is used to provide any information deemed necessary by the administrator. After a configurable period of inactivity, administrator and VPN client sessions will be terminated, requiring re-authentication. The TOE also supports direct connections from VPN clients, and protects against threats related to those client connections.

- **Trusted Path / Channels –** The TOE supports establishing trusted paths between it and remote administrators using SSHv2 for CLI access, and TLS/HTTPS 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). The TOE can establish trusted paths of peer-to-peer VPN tunnels using IPsec, and VPN client tunnels using IPsec or TLS. Note that the VPN client is in the operational environment.

- **Stateful Traffic Filtering** (FWEP & VPNGWEP) – 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.

The report concludes that the product has complied with the U.S. Government Protection Profiles for 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 Australia and was completed on 12 October 2016.

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.

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.

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 ASA 9.4(1.13), ASA 9.4(1.240) and ASDM 7.4 against the requirements of the Common Criteria (CC), the NDPP v1.1, FWEP v1.0 and 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 1) 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 Adaptive Security Appliances 9.4(1.13), Adaptive Security Appliances Virtual (ASAv) 9.4(1.240) and ASDM 7.4.

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Cisco Adaptive Security Appliances (ASA), Cisco Adaptive Security Appliances Virtual (ASAv) and ASDM
Software Version	ASA 9.4(1.13), ASA 9.4(1.240) and ASDM 7.4
Hardware Platforms	• ASA 5500 Series (5506-X, 5506-H, 5506-W, 5508-X, 5516-X) • ASAv running on VM ESXi 5.1, 5.5 or 6.0 on the Unified Computing System (UCS) C22 M3, C24 M3, C220 M3, C220 M4, C240 M3, C240 M4, C260 M2, C420 M3, C460 M2, and C460 M4 • ASAv running on VM ESXi 5.1, 5.5 or 6.0 on the UCS EN120E, EN120S M2, E140S

	M1, E140S M2, E140D M1, E160D M2, E160D M1, E180D M2, E140DP M1, E160DP M1 installed on ISR 4451-X
Security Target	Cisco Adaptive Security Appliances and ASA Virtual Security Target, Version 3.0, 10th October 2016
Evaluation Technical Report	Cisco Adaptive Security Appliances Evaluation Technical Report (T0085) REFERENCE: CSC-EFC-T0085-ETR Version 1.0, 11th October 2016
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, September 2012, Version 3.1. Rev 4
Methodology	Common Methodology for Information Technology Security, September 2012, Version 3.1. Rev 4
Conformance	U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) v 1.1.(with Errata #3) Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall v1.0 Network Device Protection Profile (NDPP) Extended Package VPN Gateway v1.1
Developer	Cisco Systems , Inc. 170 West Tasman Drive, San Jose, California 95134 United States
Evaluation Facility	CSC Australia 12 Brindabella Circuit Brindabella Business Park ACT 2609 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

The TOE is ASA 9.4(1.13), ASA 9.4(1.240) and ASDM 7.4.

The TOE consists of hardware and software that provide connectivity and security services onto a single, secure device.

The TOE is comprised of both software and hardware. The model is comprised of the following: ASA 5500 Series (5506-X, 5506-H, 5506-W, 5508-X, 5516-X) and ASAv running on VM ESXi 5.1, 5.5 and 6.0 on the UCS EN120E, EN120S M2, E140S M1, E140S M2, E140D M1, E160D M2, E160D M1, E180D M2, E140DP M1, E160DP M1, C22 M3, C24 M3, C220 M3, C220 M4, C240 M3, C240 M4, C260 M2, C420 M3, C460 M2, and C460 M4. The software is comprised of the Adaptive Security Appliance software image Release 9.4(1.13) or 9.4(1.240), with ASDM 7.4.

The underlying UCS platforms have common hardware characteristics. These 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 ASAv in terms of hardware.

2.3 TOE Functionality

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Security Audit –** The TOE provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE generates an audit record for each auditable event. 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.

- **Cryptological Support –** The TOE provides cryptography in support of other TOE security functionality. The TOE provides cryptography in support of secure connections using IPsec and TLS, and remote administrative management via SSHv2, and TLS/HTTPS. The cryptographic random bit generators (RBGs) are seeded by an entropy noise source.

- **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.

- **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. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec X509v3 certificate based authentication or pre-shared key methods. The TOE provides authentication services for administrative users wishing to connect to the TOEs secure CLI and GUI administrator interfaces. 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. The TOE also implements a lockout mechanism if the number of configured unsuccessful threshold has been exceeded. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH and HTTPS interfaces. The SSHv2 interface also supports authentication using SSH keys. The TOE optionally supports use of any RADIUS AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE.

- **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/HTTPS 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; TOE configuration file storage and retrieval, and the information flow control policies enforced by the TOE including encryption/decryption of information flows for VPNs. The TOE supports an “authorised administrator” role, which equates to any account authenticated to an administrative interface (CLI or GUI, but not VPN), and possessing sufficient privileges to perform security-relevant administrative actions. When an administrative session is initially established, the TOE displays an administrator- configurable warning banner. After a configurable period of inactivity, administrative sessions will be terminated, requiring administrators to re-authenticate.

- **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 TOE is not a general-purpose operating system and access to the TOE memory space is restricted to only TOE 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. Administrators can update the TOE's clock manually, or can configure the TOE to use NTP to synchronise the TOE's clock with an external time source. Additionally, the TOE performs testing to verify correct operation of the appliance itself and that of the cryptographic module. Whenever any system failures occur within the TOE, the TOE will cease operation.

- **TOE Access –** When an administrative session is initially established, the TOE displays an administrator- configurable warning banner. This is used to provide any information deemed necessary by the administrator. After a configurable period of inactivity, administrator and VPN client sessions will be terminated, requiring re-authentication. The TOE also supports direct connections from VPN clients, and protects against threats related to those client connections. The TOE disconnects sessions that have been idle too long, and can be configured to deny sessions based on IP, time, and day, and to NAT external IPs of connecting VPN clients to internal network addresses.

- **Trusted Path / Channels –** The TOE supports establishing trusted paths between it and remote administrators using SSHv2 for CLI access, and TLS/HTTPS 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). The TOE can establish trusted paths of peer-to-peer VPN tunnels using IPsec, and VPN client tunnels using IPsec or TLS. Note that the VPN client is in the operational environment.

- **Stateful Traffic Filtering** (FWEP & VPNGWEP) **–** 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're 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. 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. 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 (permit, deny, log) and applying these access lists to interfaces using crypto map set.

2.4 TOE Architecture

The TOE consists of the following major architectural components:

- The Cisco Adaptive Security Appliances TOE is a purpose-built, firewall platform with VPN capabilities. The Cisco Adaptive Security Appliances Virtual running on UCS platform (TOE) is a firewall platform with VPN capabilities.
- For firewall services, the TOE (ASA 5500 Series and ASAv) provides 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 architecture connection capabilities. All references within this ST to "VPN" connectivity refer to the use of IPsec tunnels to secure connectivity to and/or from the TOE, for example, gateway-to-gateway1 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.

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 Guide (Ref 2).

The scope of the evaluation was limited to those claims made in the Security Target (Ref 1).

2.5.1 Evaluated Functionality

All tests performed during the evaluation were taken from NDDP (Ref 3), FWEP (Ref 4) and VPNGWEP (Ref 5) and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

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 6) 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).

The following components are considered outside of the scope of the TOE:

- Secure Policy Manager
- Filtering of non-IP traffic provided by the EtherType option when configuring information flow policies
- The Smart Call Home feature provides personalised, e-mail-based and web-based notification to customers about critical events involving their individual systems.

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. The TOE Security Policy actions in the Security Target which are inherited from the compliance requirements states that by default, all traffic that passes through the Cisco Adaptive Security Appliance (ASA) is inspected using the Adaptive Security Algorithm and is either allowed through or dropped based on the security policy. In order to maximise the firewall performance, the ASA checks the state of each packet (for example, is this a new connection or an established connection?) and assigns it to either the session management path (a new connection SYN packet), the fast path (an established connection), or the control plane path (advanced inspection). TCP packets that match existing connections in the fast path can pass through the adaptive security appliance without rechecking every aspect of the security policy. This feature maximises performance.

For firewall services, the TOE (ASA 5500 Series and ASAv) provides 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 authorized administrator for firewalls. This header information includes source and destination host (IP) addresses, source and destination port numbers, and the transport service application protocol (TSAP) held within the data field of the IP packet. Depending upon the rule and the results of the match, the firewall either passes or drops the packet. The stateful firewall remembers the state of the connection from information gleaned from prior packets flowing on the connection and uses it to regulate current packets. The packet will be denied if the security policy is violated.

2.7 Usage

2.7.1 Evaluated Configuration

The TOE consists of the following Software and hardware versions.

TOE Configuration	Hardware Configurations	Software Version
ASA 5506-X ASA 5506-H ASA 5506-W ASA 5508-X ASA 5516-X	The Cisco ASA 5500-X Adaptive Security Appliance provides high-performance firewall and VPN services and 4-8 Gigabit Ethernet interfaces, and support for up to 300 VPNs.	ASA release 9.4(1.13)
ASAv	UCS EN120E, EN120S M2, E140S M1, E140S M2, E140D M1, E160D M2, E160D M1, E180D M2, E140DP M1, E160DP M1, C22 M3, C24 M3, C220 M3, C220 M4, C240 M3, C240 M4, C260 M2, C420 M3, C460 M2, and C460 M4 including VM ESXi 6.0	ASA release 9.4(1.240)
ASDM	Included on all ASA models with ASA	7.4

The evaluation was conducted on the default installation and configuration of the TOE using guidance and configuration information drawn from the Cisco Adaptive Security Appliance (ASA) 9.4(1) Preparative Procedures and Operational User Guide for the Common Criteria Certified Configuration (Ref 2).

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:

- Step 1: Before unpacking the security appliance, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment, Cisco Systems or an authorised Cisco distributor/partner.

- Step 2: Verify that the packaging has not been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorised Cisco distributor/partner).
- Step 3: Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems barcoded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorised Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.
- Step 4: Note the serial number of the security appliance on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the security appliance. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorised Cisco distributor/partner).
- Step 5: Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorised Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.
- Step 6: Once the security appliance is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. Also, verify the hardware received is the correct TOE model. If it does not, contact the supplier of the equipment (Cisco Systems or an authorised Cisco distributor/partner).

2.7.3 Installation of the TOE

The Configuration Guide (Ref 2) contains all relevant information for the secure configuration of the TOE.

2.8 Version Verification

The follow steps facilitate version verification:

- To properly verify the integrity of the ASA binary image, that’s part of the CCO image downloaded from Cisco.com, use the “verify” command with the “/signature” option in order to verify the digital signature. The digital signature uses 2048-bit RSA with SHA-512. For example,
  - verify /signature disk0:/ asa941-6-lfbff-k8.SPA Or
  - verify /signature disk0:/asa941-6-smp-k8.bin

- Start your security appliance as described in the “Getting Started” chapter in the online document Cisco ASA 5500 Series Configuration Guide using the CLI. Confirm that your security appliance loads the image correctly and completes internal self-checks. At the prompt, enter the show version command as follows. Verify that the version is 9.4(1). If the security appliance image fails to load, or if the security appliance version is not 9.4(1), contact Cisco TAC. The following is sample output from the show version command output, displaying the security appliance version:

- *hostname# show version Cisco Adaptive Security Appliance Software Version <Check CorrectVersion><truncated output>*

2.9 Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased. Cisco Adaptive Security Appliance (ASA) 9.4(1) Preparative Procedures and Operational User Guide for the Common Criteria Certified Configuration (Ref 2). All guidance material is available for download at **www.cisco.com.** 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:

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 3), FWEP (Ref 4), VPNGWEP (Ref 5), Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4, Parts 2 and 3 (Ref 7 and 8).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4 (Ref 9).

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 Cisco Adaptive Security Appliance (ASA) 9.4(1) Preparative Procedures and Operational User Guide for the Common Criteria Certified Configuration (Ref 2).

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.

3.4 Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report (Ref 10).

3.5 Penetration Testing

The Evaluator 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 following factors have been taken into consideration during the penetration tests:

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.

As a result of testing the Evaluators determined that the TOE is resistant to penetration attacks performed by an attacker possessing a Basic attack potential.

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.

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 product performed by the Australasian Information Security Evaluation Facility, CSC Australia.

CSC Australia **has determined** that Cisco ASA 9.4(1.13), ASA 9.4(1.240) and ASDM 7.4 uphold the claims made in the Security Target (Ref 1) and **has met** the requirements of

- U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) v 1.1 (with Errata #3)
- Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall v1.0
- Network Device Protection Profile (NDPP) Extended Package VPN Gateway v1.1

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 FWEP and VPNEP 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.

4.4 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 6) 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.

Annex A – References and Abbreviations

A.1 References

1. Cisco Adaptive Security Appliances and ASA Virtual Security Target, Version 3.0, 10th October 2016

2. Guidance Documentation:

   - Cisco Adaptive Security Appliance (ASA) 9.4(1) Preparative Procedures and Operational User Guide for the Common Criteria Certified Configuration, Version 2.0, 6th September 2016

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

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

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

6. 2016 Australian Government Information Security Manual (ISM), Australian Signals Directorate (annual edition)

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

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

9. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2016, Version 3.1, Revision 4

10. Cisco ASA Entropy Information Version 2.0, June 2015

11. Cisco Adaptive Security Appliances Evaluation Technical Report (T0085) REFERENCE: CSC-EFC-T0085-ETR Version 1.0, 12th October 2016

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ASA	Adaptive security Appliances
ASD	Australian Signals Directorate
CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
NTP	Network Time Protocol
NDPP	US Government approved Protection Profile for Network Devices
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy