Australian Government
Department of Defence

# Australasian Information Security Evaluation Program

## Certification Report

**Certificate Number: 2012/8282**

**11 Oct 2012**

**Version 1.0**

# Amendment Record

| Version | Date | Description |
|---|---|---|
| 1.0 | 11/10/2012 | Public release. |

# Executive Summary

1 The TOE is Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform version 8.4(4.1). The TOE is a purpose-built security platform that combines application-aware firewall and VPN services for small and medium-sized business (SMB) and enterprise applications. The TOE may be used in both IPv6 and IPv4 environments and may be used with or independent of its firewall, intrusion prevention system, and network antivirus capabilities, as a dedicated-function VPN platform.

2 This report describes the findings of the IT security evaluation of Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform version 8.4(4.1) to the Common Criteria (CC) evaluation assurance level EAL4+. The report concludes that the product has met the target assurance level of EAL4+ 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 in August 2012.

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

a) should use main mode and disable aggressive mode when using ISAKMP;

b) do a risk assessment on the use of TLSv1.0 in their environment;

c) disable the TTL decrement feature; and

d) disable Dynamic Trunking Protocol (DTP), telnet and FTP.

4 This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

5 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 at Ref [1] and read this Certification Report prior to deciding whether to purchase the product.

# Table of Contents

# Chapter 1 - Introduction

## 1.1 Overview

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

## 1.2 Purpose

7 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform version 8.4(4.1), against the requirements of the Common Criteria (CC) evaluation assurance level EAL4+, and

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

8 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

9 The TOE is Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform version 8.4(4.1). The TOE is a purpose-built security platform that combines application-aware firewall and VPN services for small and medium-sized business (SMB) and enterprise applications. The TOE may be used in both IPv6 and IPv4 environments and may be used, with or independent of its firewall, intrusion prevention system, and network antivirus capabilities, as a dedicated-function VPN platform.

10 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 Evaluated Configuration.

**Table 1: Identification Information**

| Item | Identifier |
|---|---|
| Evaluation Scheme | Australasian Information Security Evaluation Program. |
| TOE | Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform version 8.4(4.1). |
| Hardware Models | Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580-20, 5580-40, 5585-S10, 5585-S20, 5585-S40, and 5585-S60. |
| Software Version | Cisco ASA Release 8.4(4.1), Cisco AnyConnect Release 3.0.08057, Cisco VPN Client Releases 5.0.07.0410 or 5.0.07.0440, Cisco Adaptive Security Device Manager (ASDM)6.4(9). |
| Security Target | Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform Security Target Version 1.0 September 2012. |
| Evaluation Level | EAL4+. |
| Methodology | Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, CCIMB-2009-07-004, July 2009 with interpretations as of 28 June 2011. |
| Conformance | Common Criteria Part 2 extended.<br>Common Criteria Part 3 augmented (EAL4 + ALC_FLR.2).<br>The TOE is conformant to the following Protection Profile: US Government Protection Profile for Application-level Firewall in Basis Robustness Environments, Version 1.1, July 2007. |
| Sponsor | Cisco Systems, Inc Inc.<br>170 West Tasman Drive<br>San Jose, California<br>United States |
| Developer | Cisco Systems, Inc Inc.<br>170 West Tasman Drive<br>San Jose, California<br>United States |
| Evaluation Facility | CSC Australia – AISEF<br>217 Northbourne Avenue<br>Turner, ACT 2612<br>Australia |

# Chapter 2 - Target of Evaluation

## 2.1 Overview

11 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

12 The TOE is Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform version 8.4(4.1) developed by Cisco Systems, Inc. The TOE is a purpose-built security platform that combines application-aware firewall and VPN services for small and medium-sized business (SMB) and enterprise applications. It may be used, with or independent of its firewall, intrusion prevention system, and network antivirus capabilities, as a dedicated-function VPN platform. For firewall services, the ASA 5500 Series 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. 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. In addition to IP header information, the TOE mediates information flows on the basis of other information, such as the direction (incoming or outgoing) of the packet on any given firewall network interface. For connection-oriented transport services, the firewall either permits connections and subsequent packets for the connection or denies the connection and subsequent packets associated with the connection.

13 The application-inspection capabilities automate the network to treat traffic according to detailed policies based not only on port, state, and addressing information, but also on application information buried deep within the packet header. By comparing this deep-packet inspection information with corporate policies, the firewall will allow or block certain traffic. For example, it will automatically drop application traffic attempting to gain entry to the network through an open port-even if it appears to be legitimate at the user and connection levels if a business's corporate policy prohibits that application type from being on the network. For VPN Services, the ASA 5500 Series provides a complete remote-

access VPN solution that supports numerous connectivity options, including Cisco VPN Client for IP Security (IPSec), Cisco Clientless SSL VPN, network-aware site-to-site VPN connectivity, and Cisco AnyConnect VPN client. IPSec provides confidentiality, authenticity, and integrity for IP data transmitted between trusted (private) networks over untrusted (public) links or networks. SSL VPN uses a Web browser and Secure Socket Layer (SSL) encryption to secure connections between remote users and specific, supported internal protected resources. AnyConnect uses the Datagram Transport Layer Security (DTLS) and SSL protocols to provide remote users with secure VPN connections to the ASA. Note: these VPN configurations are only supported in Routed Single Context Mode. For management purposes, the ASDM is included. ASDM allows the ASA to be managed from a graphical user interface. Its features include:

a) Rapid Configuration: in-line and drag-and-drop policy editing, auto complete, configuration wizards, appliance software upgrades, and online help;

b) Powerful Diagnostics: Packet Tracer, log-policy correlation, packet capture, regular expression tester, and embedded log reference;

c) Real-Time Monitoring: device, firewall, content security, real-time graphing; and tabulated metrics; and

d) Management Flexibility: A lightweight and secure design enables remote management of multiple security appliances.

## 2.3 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 Security Target (Ref [1] ) contains no explicit security policy statements.

## 2.4 TOE Architecture

14 The TOE consists of the following major subsystems:

a) **VPN/Firewall Subsystem**

The VPN/Firewall subsystem is used to establish and control VPN connections and allow the flow of IP traffic between external and internal network interfaces. Traffic (i.e. packets arriving at the network interface) is handled by the VPN/Firewall subsystem according to its configuration. The VPN/Firewall subsystem enforces the rules (access-lists) to all packets for VPN tunnel setup and traffic control.

b) **VPN Client Subsystem**

The VPN Client Subsystem encompasses the Cisco VPN Client software that is loaded on a client platform and provides the mechanism to establish and support an IPSec VPN connection with the ASA.

c) **AnyConnect Client Subsystem**

The AnyConnect Client Subsystem is comprised of the Cisco AnyConnect Client Software package that provides the mechanism to communicate with the VPN/Firewall subsystem to create a secure SSL/TLS VPN connection over an untrusted network.

d) **ASDM Subsystem**

The ASDM module is used to configure, monitor, and manage the VPN/Firewall Subsystem. It permits an authorised administrator from an HTTPS-tunnelled ASDM connection on a remote connected network to perform various administrative actions.

## 2.5 Clarification of Scope

15 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]) and includes the following.

a) VPN and/or Firewall Information Flow Control;

b) Audit;

c) Identification & Authentication;

d) Management; and

a) Cryptography.

### 2.5.1 Evaluated Functionality

16 The TOE provides the following evaluated security functionality:

a) Audit: The TOE‘s Audit security function supports audit record generation and review. The TOE provides date and time information that is used in audit timestamps. The events generated by the TOE include all commands executed by the authorised administrator, in addition to cryptographic operations, traffic decisions, indication of the logging starting and stopping and other system events.

b) Cryptographic support: The TOE provides cryptographic functionality (RSA key sizes 1024 and 2048; DH groups 14, 19, 20, and 24; AES-128 and AES-256; 3DES; SHA-1 and SHA-2; and HMAC-SHA-1) for two main purposes:

i) Remote administration is supported through SSHv2 and TLS 1.0.

ii) VPN for peer-to-peer tunnels using IPSec (IKEv1 and IKEv2), and for VPN client tunnels using IPSec (IKEv1 and IKEv2) or TLS 1.0.

c) Authentication and User data protection: Authentication performed by the TOE makes use of a reusable password mechanism for access to the TOE by authorised administrators as well as by human users establishing VPN connections. The TOE by default is configured to perform local authentication and stores user names and passwords in an internal user authentication database which is only accessible by the administrator via privileged commands at the CLI or screens in ASDM. The TOE can be configured to use an external authentication server for single-use authentication such that the TOE is responsible for correctly invoking the external authentication mechanism, and for taking the correct actions based on the external server‘s authentication decisions.

d) Security Management: The Management functionality permits an authorised administrator from a physically secure local connection, an SSHv2 encrypted connection (the encryption is subject to FIPS PUB 140-2 security functional requirements) or an HTTPS-tunnelled ASDM connection from an internal trusted host or a remote connected network to perform the administration actions.

e) Protection of the TOE security functions: ie internal data transfer and reliable time stamps.

f) TOE access. The TOE protects itself from tampering by means of access control and audit.

### 2.5.2 Non-evaluated Functionality and Services.

17 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 [2]) 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).

18 The functions and services that have not been included as part of the evaluation are provided below:

a) The TTL decrement feature is excluded from the evaluated configuration;

b) SNMP is excluded from the evaluated configuration;

c) Secure Policy Manager is excluded from the evaluated configuration; and

d) Filtering of non-IP traffic provided by the EtherType option when configuring information flow policies is excluded from the evaluated configuration.

## 2.6 Usage

### 2.6.1 Evaluated Configuration

19 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in this defined evaluated configuration. Australian Government users should refer to the ISM (Ref [2]) to ensure that configuration meet the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

20 The TOE is comprised of the following software components:

a) Cisco ASA Release 8.4(4.1);

b) Cisco AnyConnect Release 3.0.08057;

c) Cisco VPN Client Releases 5.0.07.0410 or 5.0.07.0440; and

d) Cisco Adaptive Security Device Manager (ASDM)6.4(9).

21 The TOE relies on the following hardware:

a) Cisco ASA 5505;

b) 5510;

c) 5520;

d) 5540;

e) 5550;

f) 5580-20;

g) 5580-40;

h) 5585-S10;

i) 5585-S20;

j) 5585-S40;

k) 5585-S60;

The following components are part of the environment and are optional or required by the TOE to support the evaluated configurations:

a) VPN Peer (optional);

b) VPN Client Platform (required);

c) ASDM Management Platform (required);

d) Web Browser (optional);

e) Remote Authentication server (required);

f) NTP server (optional);

g) Peer Certificate Authority (CA) (optional); and

h) Syslog Server (required).

### 2.6.2 Delivery procedures

22 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product. They should then receive the correct version and the customer must check the models received against the list of TOE component hardware models at the beginning of the *Preparative Procedures and Operational User Guidance* 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 "*Verification of Image and Hardware*" instruction included in the wrapper document.

### 2.6.3 Determining the Evaluated Configuration

23 Start the security appliance as described in the "Getting Started" chapter in the online document *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4.* Confirm that the 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 8.4(4.1). If the security appliance image fails to load, or if the security appliance version is not 8.4(4.1), contact Cisco Technical Assistance Centre (TAC).

### 2.6.4 Documentation

24 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available upon request from Cisco.

a) Cisco Adaptive Security Appliance (ASA) 8.4(4.1) Firewall & Virtual Private Network (VPN) Platform Preparative Procedures & Operational User Guide for the Common Criteria Evaluated Configuration. This document provides information regarding the key configuration requirements and directs users to the specific user guidance document(s) for each of the TOE components. The Preparative Procedures and Operational User Guidance (Ref [3]) describe the processes and other relevant information for the secure installation and operation of the various components of Cisco ASA. Additionally these documents describe the usage assumptions and details the technical information regarding the TOE's usage.

### 2.6.5 Secure Usage

25 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.

a) A.PHYSEC

The hardware component of the TOE is physically secure.

b) A. LOWEXPENHEXP

The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low to enhanced.

26 In addition, the following organisational security policies must be in place:

a) P.CRYPTO AES (Advanced Encryption Standard as specified in FIPS 197) encryption (as specified in SP 800-67) must be used to protect remote administration functions, and the associated cryptographic module must comply, at a minimum, with FIPS 140-2 (level 1);

b) P.INTEGRITY The TOE shall support the IETF Internet Protocol Security Encapsulating Security Payload (IPSEC ESP) as specified in RFC2406. Sensitive information transmitted to a VPN peer shall apply integrity mechanisms as specified in Use of HMAC-SHA-1 within ESP and AH (RFC 2404); and

c) P.ACCESS_BANNER The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

# Chapter 3 - Evaluation

## 3.1 Overview

27 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

28 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 3 (Refs [4], [5] and [6]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 3 (CEM) (Ref [7]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [8], [9] and [10]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [11]) were also upheld.

## 3.3 Functional Testing

29 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers. The developers were able to produce evidence that IPv6 testing had been conducted.

## 3.4 Penetration Testing

30 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. The evaluator emphasised the importance of disabling DTP to ensure a securely configured environment.

## 3.5 Certification Result

31 After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref [12]), the Australasian Certification Authority certifies the evaluation of Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network

(VPN) Platform version 8.4(4.1) performed by the Australasian Information Security Evaluation Facility, CSC.

32 CSC has found that Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform version 8.4(4.1) upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL4+.

33 Certification is not a guarantee of freedom from security vulnerabilities.

## 3.6 Assurance Level Information

34 EAL4 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation, to understand the security behaviour.

35 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, implementation representation, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with an Enhanced-Basic attack potential.

36 EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

37 This EAL represents a meaningful increase in assurance from EAL3 by requiring more design description, the implementation representation for the entire TSF, and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development.

## 3.7 Recommendations

38 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 [2]) and New Zealand Government users should consult the GCSB.

39 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [3]), the ACA also recommends that users and administrators:

a) should use main mode and disable aggressive mode when using ISAKMP;

b) do a risk assessment on the use of TLSv1.0 in their environment;

c) disable the TTL decrement feature; and

d) disable DTP, telnet and FTP.

40 This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

41 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 at Ref [1] and read this Certification Report prior to deciding whether to purchase the product.

# Annex A - References and Abbreviations

## A.1 References

[1] ST – Cisco Adaptive Security Appliances (ASA) Firewall and Virtual Private Network (VPN) Platform Security Target, September 2012.

[2] 2012 Australian Government Information Security Manual (ISM), Defence Signals Directorate, (available at www.dsd.gov.au).

[3] User Guidance: Cisco Adaptive Security Appliance (ASA) 8.4(4.1) Firewall & Virtual Private Network (VPN) Platform Preparative Procedures & Operational User Guide for the Common Criteria Evaluated Configuration.

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-001.

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-002.

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-003.

[7] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-209-07-004.

[8] AISEP Policy Manual, APM, Version 4.0, August 2011, Defence Signals Directorate.

[9] AISEP Certifier Policy, ACP. Version 4.0, August 2011, Defence Signals Directorate.

[10] AISEP Evaluator Policy, AEP. Version 4.0, August 2011, Defence Signals Directorate.

[11] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

[12] Evaluation Technical Report: Cisco ASA 5500 Series Security Appliance Evaluation Technical Report (T0070) Reference CSC-EFC-T0070 ETR, COMMERCIAL IN CONFIDENCE, Version 1.0, 27 August 2012.

## A.2 Abbreviations

| | |
|---|---|
| ASDM | Adaptive Security Device Manager |
| AISEF | Australasian Information Security Evaluation Facility |
| AISEP | Australasian Information Security Evaluation Program |
| CC | Common Criteria |
| CEM | Common Evaluation Methodology |
| DSD | Defence Signals Directorate |
| DTP | Dynamic Trunking Protocol |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| GCSB | Government Communications Security Bureau |
| IKE | Internet Key Exchange |
| NTP | Network Time Protocol |
| 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 |
| TLS | Transport Layer Security |
| + | Augmented |