Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report
2013/86

Cisco Adaptive Security Appliances 9.1(2)

5 Sep 2013
Version 1.0

Amendment Record

Version	**Date**	**Description**
1.0	5-Sep-13	Final release

Executive Summary

The Target of Evaluation (TOE) is the Cisco Adaptive Security Appliances 9.1(2).

The Cisco Adaptive Security Appliances (Cisco ASA) consists of both hardware and software solutions to 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 can operate in a number of modes: as a single standalone device with a single-context, or with multiple-contexts within each single/pair; as a transparent firewall when deployed in a single-context, or with one or more contexts connected to two or many IP subnets when configured in router mode.

For management purposes, the Adaptive Security Device Manager (ASDM) is included. ASDM allows the ASA to be managed from a graphical user interface.

This report describes the findings of the IT security evaluation of Cisco Adaptive Security Appliances (Cisco ASA) for compliance with the NDPP v1.1 and the TFFWEP v1.0.

The report concludes that the product has complied with the NDPP and TFFWEP 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 8 August 2013. 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 at Ref [1] and read this Certification Report prior to deciding whether to purchase the product.

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 the Australian Government Information Security Manual (ISM) and New Zealand Government users should consult the GCSB.

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 TOE: Cisco Adaptive Security Appliances (Cisco ASA), for compliance with the NDPP v1.1 and TFFWEP v1.0; and

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 the Cisco Intrusion Adaptive Security Appliances (Cisco ASA). 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

Description	**Version**
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	Cisco Adaptive Security Appliances (Cisco ASA) 9.1(2).
Hardware Models	ASA 5500 series appliances (5505, 5510, 5520, 5540, 5550, and 5580-20-40). ASA 5500-X series appliances (5512-X, 5515-X, 5525-X, 5545-X, and 5555-X). ASA 5585-X series appliances (5585-10, 5585-20, 5585-40, and 5585-60). ASA Services Module (ASA-SM)
Software Version	9.1(2) with ASDM 7.1(3).
Security Target	Cisco Adaptive Security Appliances 9.1(2) Security Target Version 1.0, August 2013.
Protection Profile	US Government Protection Profile for Security Requirements for Network Devices version 1.1 June 8, 2012. US Government Network Device Protection Profile Extended Package: Stateful Traffic Filter Firewall version 1.0 December 19, 2011.
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, September 2012 Version 3.1 Revision 4, CCIMB-2012-09-004 with interpretations as of 11 December 2012.
Sponsor	Cisco Systems, 170 West Tasman Drive, San Jose, California, United States.
Developer	Cisco Systems, 170 West Tasman Drive, San Jose, California, United States.
Evaluation Facility	CSC Australia Pty Limited.

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 the Cisco Adaptive Security Appliances (Cisco ASA), which consists of both hardware and software solutions to 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 can operate in a number of modes: as a single standalone device with a single-context, or with multiple-contexts within each single/pair; as a transparent firewall when deployed in a single-context, or with one or more contexts connected to two or many IP subnets when configured in router mode.

For management purposes, the Adaptive Security Device Manager (ASDM) is included. ASDM allows the ASA to be managed from a graphical user interface.

As a network device the TOE supports self-protection through implementation of authentication for local and remote administration and the use of encrypted communications for remote administration. The TOE also supports generation of audit messages and their encrypted communication to authenticated remote hosts.

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 and this is not a requirement of the NDPP or TFFWEP.

2.4 TOE Architecture

Refer to the Security Target (Ref [1]) for an architectural description of the TOE and the TOE environment.

2.5 Clarification of Scope

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

2.5.1 Evaluated Functionality

The TOE provides the following evaluated security functionality:

a) Security audit

The TOE can generate audit records for events related to cryptography 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.

b) Cryptographic support

The TOE provides cryptography in support of other Cisco ASA security functionality. The TOE provides cryptography in support of VPN connections via TLS and IPSec, and remote administrative management via SSHv2 and TLS. The entropy design description, justification, operation and health tests are assessed and documented in Cisco ASA Entropy Information (Ref [2]).

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 authentications 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, SSH, or ADSM (over TLS) 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 or GUI (ASDM).

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 TLS (ASDM), a secure SSHv2 session, or via a local console connection. The TOE provides the ability to securely manage all the TOE administrative users, all identification and authentication, all audit functionality of the TOE; all cryptographic functionality; the timestamps maintained by the TOE; and TOE configuration file storage and retrieval.

f) Protection of the TOE security functions

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 which is applied to audit records generated by the TOE.

g) TOE access

The TOE can terminate inactive session after an authorised administrator configurable time-period. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session. When an administrative session is initially established, the TOE displays an administrator-configurable warning banner.

h) 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.

i) 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 ensure that 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.

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.

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 [3]) for policy relating to using an evaluated product in an unevaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

The Secure Policy Manager is excluded from the evaluated configuration. Filtering of non-IP traffic is also excluded from the evaluated configuration. Use of this functionality is beyond the scope of this Common Criteria evaluation. These services will be disabled by configuration. The exclusion of the functionality does not affect compliance to the US Government Protection Profile for Security Requirements for Network Devices (NDPP) (Ref [4]) and Traffic Filter Firewall Extended Package (TFFWEP) (Ref [5]).

In the certified configuration, use of IPsec or TLS VPNs is only approved for tunnelling traffic that originates from or terminates at the ASA itself, not for tunnelling traffic between hosts across the ASA.

2.6 Usage

2.6.1 Evaluated Configuration

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 [3]) to ensure that the configuration meets the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

The TOE consists of one or more physical devices as specified in table 2 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 ASA is to be remotely administered, the management station must connect using SSHv2 or 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.

The TOE consists of the ASA software version 9.1(2) and ADSM version 7.1(3). The hardware models in scope for this evaluation are as shown in table 2 on the following page:

Table 2: TOE Components

TOE Components	
Description	**Identification**
ASA 5500 series appliances	Cisco ASA 5505
	Cisco ASA 5510
	Cisco ASA 5520
	Cisco ASA 5540
	Cisco ASA 5550
	Cisco ASA 5580-20-40
ASA 5500-X series appliances	Cisco ASA 5512-X
	Cisco ASA 5515-X
	Cisco ASA 5525-X
	Cisco ASA 5545-X
	Cisco ASA 5555-X
ASA 5585-X series appliances	Cisco ASA 5585-S10
	Cisco ASA 5585-S20
	Cisco ASA 5585-S40
	Cisco ASA 5585-S60

2.6.2 Delivery Procedures

Shipment of units from Cisco Distributers to the user is via 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 packaging slip and information on the stickers, the customer must check 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 components, the customer will access Cisco Connection Online (CCO) to download images. The customer 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 manages 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.

2.6.3 Determining the Evaluated Configuration

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 Preparatory Procedures 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" in the user guidance (Ref [6]).

2.6.4 Documentation

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 does not ship hard copies of the guidance documents with the product. All guidance material is available for download at www.cisco.com.

Cisco Adaptive Security Appliances 9.1(2) Preparative Procedures and Operational User Guide for the Common Criteria Certified Configuration, Version 0.6, July 2013, (Ref [6]) provides information regarding the key configuration requirements and directs users to the specific user guidance document(s) for each of the TOE components. It describes the process for secure installation and operation, any assumptions and provides technical information regarding the TOE's usage.

2.6.5 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.

a) 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.

b) A.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

c) A.TRUSTED_ADMIN

TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

d) 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.

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

e) P.ACCESS_BANNER

The TOE shall display an initial banner for administrator logins describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

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 US Government Protection Profile for Security Requirements for Network Devices version 1.1 June 8, 2012 (Ref [4]), US Government Network Device Protection Profile Extended Package: Stateful Traffic Filter Firewall version 1.0 December 19, 2011 (Ref [5]), Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4 (Refs [7], [8] and [9]).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4 (CEM) (Ref [10]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [11], [12] and [13]).

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [14]) were also upheld.

3.3 Testing

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

Table 3: Requirements tested.

Test ID	Requirement in NDPP
TOE Access	FAU_GEN.1
	FTA_SSL_EXT.1
	FTA__SSL3
	FTA_SSL.4 (Test 1, 2)
	FTA_TAB.1
Identification and authentication	FAU_GEN.1
	FIA_PMG.EXT.1
	FIA_UIA_EXT.1 (Test 1, 2, 3)

	FIA_UAU.7
	FCS_SSH_EXT.1.2 (Test 1, 2)
Protection of the TOE Security Functions	FAU_GEN.1
	FPT_STM (Test 1, 2)
	FPT_TUD_EXT.1 (Test 1, 2)
Trusted Path	FAU_GEN.1
	FPT_ITC.1 (Test 1, 2, 3, 4, 5)
	FTP_TRP.1 (Test 1, 2, 3, 4)
Protocol conformance	FAU_GEN.1
	FAU_STG_EXT.1
	FCS_IPSEC_EXT.1.2 (Test 1, 2)
	FCS_IPSEC_EXT.1.3 (Test 1, 2)
	FCS_IPSEC_EXT.1.4 (Test 1)
	FCS_IPSEC_EXT.1.5 (Test 1)
	FCS_IPSEC_EXT.1.6 (Test 2)
	FCS_IPSEC_EXT.1.7 (Test 1)
	FCS_IPSEC_EXT.1.8 (Test 2)
	FCS_TLS_EXT.1 (Test 1)
	FCS_SSH_EXT.1.2 (Test 2)
	FCS_SSH_EXT.1.3 (Test 1)
	FCS_SSH_EXT.1.4 (Test 1)
	FCS_SSH_EXT.1.7 (Test 1)

Table 4: TFFWEP Requirements tested.

Test ID	Requirement in NDPP
Firewall 1.1-2	FAU_GEN.1
	FFW_RUL_EXT.1.1 (Test 1)
	FFW_RUL_EXT.1.2 (Test 1)
Firewall 1.3-5	FFW_RUL_EXT.1.3 (Test 1)
	FFW_RUL_EXT.1.4 (Test 1)
	FFW_RUL_EXT.1.5 (Test 1)
Firewall 1.6	FFW_RUL_EXT.1.6 (Tests 1 to 6)
Firewall 1.7	FFW_RUL_EXT.1.7 (Test 1, 2)
Firewall 1.8	FFW_RUL_EXT.1.8 (Test 1, 2)
Firewall 1.9	FFW_RUL_EXT.1.9 (Test 1, 2)
Firewall 1.10	FFW_RUL_EXT.1.10 (Tests 1 to 16)

3.4 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.

3.4 Entropy

The entropy design description, justification, operation and health tests are assessed and documented in a separate report (Ref [2]).

3.5 Certification Result

After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref [15]), the Australasian Certification Authority certifies the evaluation of Cisco Adaptive Security Appliances (Cisco ASA) performed by the Australasian Information Security Evaluation Program.

CSC has found that Cisco Adaptive Security Appliances (Cisco ASA) upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the NDPP and TFFWEP.

Certification is not a guarantee of freedom from security vulnerabilities.

3.6 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 provide assurance by a full security target and an analysis of the SFRs 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 and TFFWEP assurance activities, and a vulnerability analysis (based upon TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with an Enhanced-Basic attack potential.

Compliance also provides assurance through evidence of secure delivery procedures.

3.7 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 the ISM (Ref [3]) and New Zealand Government users should consult the GCSB.

Annex A - References and Abbreviations

A.1 References

1. ST – Security Target for Cisco Adaptive Security Appliances version 1.0, August 2013

2. Cisco ASA Entropy Information version 1.1 August 2013.

3. 2013 Australian Government Information Security Manual (ISM), Australian Signals Directorate (formerly DSD). Available at www.dsd.gov.au.

4. US Government approved Protection Profile - Protection Profile for Network Devices version 1.1 June 8, 2012.

5. US Government Network Device Protection Profile Extended Package: Stateful Traffic Filter Firewall version 1.0 December 19, 2011.

6. User Guidance: Cisco Adaptive Security Appliances 9.1(2) Preparative Procedures and Operational User Guide for the Common Criteria Certified Configuration, Version 0.6, July 2013.

7. Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model September 2012 Version 3.1 Revision 4 CCMB-2012-09-001.

8. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2012 Version 3.1 Revision 4 CCMB-2012-09-002.

9. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2012 Version 3.1 Revision 4 CCMB-2012-09-003.

10. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2012, Version 3.1, Revision 4, CCMB-2012-09-004.

11. AISEP Policy Manual, APM, Version 4.0, August 2011, Australian Signals Directorate.

12. AISEP Certifier Policy, ACP. Version 4.0, August 2011, Australian Signals Directorate.

13. AISEP Evaluator Policy, AEP. Version 4.0, August 2011, Australian Signals Directorate.

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

15. Evaluation Technical Report: Cisco Adaptive Security Appliances, Reference CSC-EFC-T0076-ETR Version 1.0 (proprietary).

A.2 Abbreviations

ACA	Australasian Certification Authority
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ASA	Cisco Adaptive Security Appliances
ASD	Australian Signals Directorate (formerly DSD)
ASDM	Cisco Adaptive Security Device Manager
CA	Certification Authority
CC	Common Criteria
CCO	Cisco Connection Online
CLI	Command Line Interface
CSC	Computer Sciences Corporation
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate (now ASD)
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau, New Zealand
IP	Internet Protocol
IPsec	Internet Protocol Security
NTP	Network Time Protocol
NDPP	US Government approved Protection Profile for Network Devices
PP	Protection Profile
RFC	Request for Comments
SFP	Security Function Policy
SFR	Security Functional Requirements
SSH	Secure Shell
ST	Security Target
TFFEWP	Traffic Filter Firewall Extended Package (extending NDPP)
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TLS	Transport Layer Security
VPN	Virtual Private Network