Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Maintenance Report Supplementing Certificate Report 2013/86

19 December 2014
Version 1.0

Amendment Record

Version	Date	Description
1.0	19/12/2014	Final release

Table of Contents

Chapter 1 – Introduction

1.1 Purpose

This document is an addendum to the Certification Report (Ref [1]) that describes the relevant baseline evaluation of the Cisco Adaptive Security Appliances.

The purpose of this Maintenance Report is to describe the status of the assurance continuity activities undertaken by Cisco for the Cisco Adaptive Security Appliances against the requirements contained in the Assurance Continuity: CCRA Requirements (Ref [2]).

Cisco provided information about their assurance continuity activities in the form of an Impact Analysis Report (IAR) (Ref [5]). The IAR lists the changes made to the certified TOE, the evidence updated as the result of the changes and the security impact of the changes.

This report should be read in conjunction with:

a) The certified TOE's Certification Report (Ref [1]).
b) The certified TOE's Security Target (Ref [3]) which provides a full description of the security requirements and specifications that were used as the basis of the baseline evaluation.
c) The new Security Target (Ref [4]) which includes the updated version numbers.
d) Common Criteria Operational User Guidance and Preparative Procedures (Ref [6]).

1.2 Identification

Table 1: Identification Information

Item	Identifier
Impact Analysis Report	Impact Analysis Report for Cisco Adaptive Security Appliances Version 0.02, dated 3rd December 2014
Evaluation Scheme	Australasian Information Security Evaluation Program
Developer	Cisco Systems, Inc
Certified TOE	Cisco Adaptive Security Appliances running ASA 9.1(2) with ASDM 7.1(3)
Maintained TOE	Cisco Adaptive Security Appliances running ASA 9.1(5.12) with ASDM 7.1(6)
Certified Security Target	Cisco Adaptive Security Appliances Security Target Version 1.0 dated, August 2013
Maintained Security	Cisco Adaptive Security Appliances Security Target

Target	Version 1.1 dated, November 2014
Certificate Number	2013/86

Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to Section 1.4: Evaluated Configuration of the Security Target (Ref [4]).

Chapter 2 – IAR Summary

2.1 Description of changes

The Impact Analysis Report (IAR) indicated that the following minor changes have been made to the Cisco Adaptive Security Appliances.

- New features and bug fixes as described below.

2.2 Software changes

All bug fixes and new features implemented to the certified TOE are categorised into these two minor change types:

- Minor changes with little or no security relevance. These changes may be related to the TSF in some way, though may or may not relate directly to an SFR defined within the ST.

- Minor changes with some security relevance. The changes in this section relate to the TSF in some way though the affect of the change is only to ensure the TOE functions as expected and does not add or detract from the stated requirements in the ST. Therefore, changes in this category result in no adverse affect to the assurance baseline.

The following minor changes are with little or no security relevance; they are not related to the TSF and fall out of the scope of evaluated functionality:

- Fixes for License issues
- Fixes for Multicast and Broadcast traffic
- Fixes for Memory Leaks
- Fixes for SNMP Management
- Fixes for Switching and Routing protocols
- Fixes for Availability
- Fixes for System Load Testing
- Fixes for NAT/PAT
- Fixes for QoS
- Fixes for Network Services
- Fixes for WebVPN
- Fixes for Miscellaneous bugs as described in the IAR.

The following minor changes are related to the TSF with some security relevance. They were considered and found not to impact the developer evidence. Therefore, the changes have no adverse affect to the assurance baseline:

- Fixes for TCP protocol processing
- Fixes for Firewall Rule processing
- Fixes for IPsec protocol processing
- One fix for specific syslog messages
- Fixes for Miscellaneous bugs as described in the IAR.

Each bug fix was applied to make the TOE function as originally intended, no additional security functionality was added, and no existing security functionality was removed.

Each bug fix was unit tested, and the 9.1(5.12) image has had a limited amount of automated regression testing to confirm a baseline of functionality.

Internal and external keyword searches were done for vulnerabilities related to the TOE and none were found.

The following new feature has minor security relevance to the TSF and it will be disabled in evaluated configuration.

New Feature	Description	How it was addressed
Secure Copy client	The ASA now supports the Secure Copy (SCP) client to transfer files to and from a SCP server. The following commands were introduced: **ssh pubkey-chain**, **server (ssh pubkey-chain)**, **key-string**, **key-hash**, **ssh stricthostkeycheck**. The following command was modified: **copy scp**.	Will be disabled in the evaluated configuration resulting in no impact to the evaluated configuration of the TOE.

All other new features of the product were analysed and determined to have no security relevance as they were not applicable to the TSF.

2.3 Hardware changes

No hardware changes were made.

2.4 Development environment changes

The changes to the development environment do not have a follow on effect on any assurance components outside the development environment.

2.5 Documentation updated

The certified Security Target and the Operational User Guidance and Procedures were updated due to the software changes.

Table 1 Affected Developer Evidence

Assurance Family	Document title & outline of changes	Date and Version
ASE	Security Target: • Updated for new software version numbers. • Updated section 1.7: Excluded Functionality • Inserted note in TSS that FIPS	November 2014, version 1.1

AGD_PRE	Common Criteria Operational User Guidance and Preparative Procedures: • Updated for new software version numbers. • Updated items prohibited from use • Updated instructions for disabling prohibited features	November 2014, version 1.1

Chapter 3 - Assurance Continuity

3.1 Assurance Continuity Result

After consideration of the Impact Analysis Report (IAR) provided by Cisco, Australasian Certification Authority (ACA) has determined that the proposed changes are minor. The ACA agrees that the resultant change in the TOE can be classified as minor and that certificate maintenance is the correct path to continuity of assurance. The ACA agrees that the original assurance result is maintained for the Cisco Adaptive Security Appliances ASA 9.1(5.12) with ASDM 7.1(6).

References and Abbreviations

A.1 References

1. Australasian Information Security Evaluation Program, Certification Report, 2013/86, Cisco Adaptive Security Appliances 9.1(2), 5 Sep 2013, Version 1.0
2. CCRA requirements, Common Criteria Interpretation Management Board, CCIMB-2012-06-01, Version 2.1, June 2012
3. Cisco Adaptive Security Appliances Security Target Version 1.0 dated, August 2013
4. Cisco Adaptive Security Appliances Security Target Version 1.1 dated, November 2014
5. Cisco Adaptive Security Appliance Impact Analysis Report for Common Criteria Assurance Maintenance Update of Cisco Adaptive Security Appliances running IOS version ASA 9.1(2) with ASDM 7.1(3) to Cisco Adaptive Security Appliances running IOS version ASA 9.1(5.12) with ASDM 7.1(6), Version 0.02, dated 3rd December 2014
6. Common Criteria Operational User Guidance and Preparative Procedures, Version 1.1, dated November 2014

A.2 Abbreviations

ACA	Australasian Certification Authority
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
ASD	Australian Signals Directorate
IAR	Impact Analysis Report
TOE	Target of Evaluation
TSF	TOE Security Function