Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report
2013/84

Cisco Intrusion Prevention System 7.2(1)

11 Sept 2013
Version 1.1

Amendment Record

Version	Date	Description
1.1	11/09/13	Final release

Executive Summary

The Target of Evaluation (TOE) is the Cisco Intrusion Prevention System 7.2(1).

The Cisco Intrusion Prevention System (Cisco IPS) is a family of network-based intrusion detection and prevention appliances. As a network device the TOE supports self protection through the implementation of protection mechanisms for local and remote administration and the use of encrypted communications for remote administration. The TOE also supports the generation of security relevant audit messages and their transmission over encrypted communications to remote authenticated hosts. This IPS functionality includes the ability to react to traffic in real time and ability to analyse the content of each packet. The Cisco IPS can analyse single packet or a complete flow of attacks while maintaining flow state, allowing for the detection of multi-packet attacks. The Cisco IPS uses a rule based expert system to analyse the packet information to determine the type of attack.

All data collection and analysis is conducted by the Cisco IPS which is placed at strategic points throughout a target network. The Cisco IPS has several options that include generating an alarm, logging the alarm event, dropping and modifying packets, sending a command to a Cisco router, switch or firewall to block traffic or terminate sessions. Key features include:

- Provides distributed protection from many attacks;
- Provide risk based IPS policy provisioning. Based on the risk rating, different policy actions can be assigned;
- Offers inline inspection of traffic passing through any combination of router LAN or WAN interfaces in both directions;
- Offers promiscuous mode in which a duplicate stream of traffic is sent to the TOE;
- Cisco anomaly detection provides protection against zero day attacks; and
- Uses patented anti-evasion technology to defend and monitor.

This report describes the findings of the IT security evaluation of Cisco Intrusion Prevention System (Cisco IPS) for compliance with the NDPP v1.1.

The report concludes that the product has complied with the NDPP 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 25 June 2013.

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

a) should test the IPS using a trusted penetration tester annually.

b) be aware that IPS functionality is outside the scope of the scope of evaluation and was not tested in this case. The development of an extended package to NDPP to cover IPS systems is in progress and expected to complete in 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.

Table of Contents

1. **Executive Summary** ..... **iv**

2. **Table of Contents** ..... **vi**

3. **Chapter 1 – Introduction** **1**

1.1 Overview *1*

1.2 Purpose *1*

1.3 Identification *1*

4. **Chapter 2 - Target of Evaluation** **3**

2.1 Overview *3*

2.2 Description of the TOE *3*

2.3 Security Policy *4*

2.4 TOE Architecture *4*

2.5 Clarification of Scope *5*

2.5.1 Evaluated Functionality 5

2.5.2 Non-evaluated Functionality and Services. 6

2.6 Usage *6*

2.6.1 Evaluated Configuration 6

2.6.2 Delivery Procedures 7

2.6.3 Determining the Evaluated Configuration 8

2.6.4 Documentation 8

2.6.5 Secure Usage 8

5. **Chapter 3 - Evaluation** **10**

3.1 Overview *10*

3.2 Evaluation Procedures *10*

3.3 Testing *10*

3.4 Penetration Testing *11*

3.4 Entropy *11*

3.5 Certification Result *11*

3.6 Assurance *11*

3.7 Recommendations *12*

6. **Annex A - References and Abbreviations** **13**

A.1 References *13*

A.2 Abbreviations *14*

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 Intrusion Prevention System (Cisco IPS) for compliance with the NDPP v1.1 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 Prevention System (Cisco IPS).

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	Cisco Intrusion Prevention System (Cisco IPS) 7.2(1).
Hardware Models	IPS 4300 and 4500 series sensors (4345, 4360, 4510, and 4520). IPS Hardware models for ASA 5585-X (IPS-SSP-10, SSP-20, SSP-40, and SSP-60) IPS software modules on ASA 5500-X

Software Version	7.2(1)
Security Target	Cisco Intrusion Prevention System 7.2(1) Security Target Version 1.2, July 2013.
Protection Profile	US Government Protection Profile for Security Requirements for Network Devices version 1.1 June 8, 2012
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 29 November 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.

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.

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

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.

The TOE is a family of network based intrusion detection and prevention appliances. These appliances offer a range of specialised security functionality that is outside the scope of the evaluation as defined by the NDPP. This functionality does not interfere with the evaluated functionality and can be enabled in the certified configurations.

The IPS functionality includes the ability to monitor and react to network traffic in real time and analyse the packets. The Cisco IPS can analyse single packets or a complete flow for attacks while maintaining flow state allowing for the detection of multi-packet attacks. The Cisco IPS uses a rule based expert system to analyse packet information to determine the type of attack.

Sensors are placed at strategic points. In response to an attack, the IPS has several options that include generating an alarm, logging an alarm, dropping and modifying packets. Key features include:

- Provides distributed protection from attacks;
- Provide risk based IPS Policy provisioning. Based on the risk rating, different policy actions can be assigned;
- Offers inline inspection of traffic passing through any combination of router LAN or WAN interfaces in both directions;
- Offers promiscuous mode in which a duplicate stream of traffic is sent to the TOE;
- Cisco anomaly detection provides protection against zero day attacks; and
- Uses patented anti-evasion technology to defend and monitor.

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.

2.4 TOE Architecture

The TOE consists of the following major subsystems:

a) **Cisco IPS4300 and 4500 Sensors.**

The Cisco IPS 4300 and 4500 sensors are stand alone IPS appliances that provide hardware accelerated deep packet inspection and automated threat assessment. Deep packet inspection can be done on can be done on encapsulated traffic including routing encapsulated (GRE), Multiprotocol Label Switching (MPLS), 802.1q, IPv4 in IPv4, IPv4 in IPv6, and Q in Q double VLAN.

b) **Cisco IPS SSP hardware modules.**

The IPS SSP hardware modules install to ASA 5500-X series firewalls. The host ASA provides power and cooling for the hardware module, but the hardware module provides its own physical management port. The IPS hardware module runs its own IPS operating system independent of the ASA operating system, with its own set of administrative users, its own audit configurations. Administrators of the ASA cannot authenticate to the IPS and thus cannot modify the configuration of the IPS.

c) **Cisco IPS SSP software modules.**

The IPS SSP software models function just like the hardware modules except that they rely on the host ASA to provide physical interfaces for local and remote administration of the IPS. The IPS SSP software module and the ASA share the network based management interface (used for remote access and audit log transmission), however each have their own separate MAC and IP addresses. The IPS administrator configures the IP address of the IPS management interface within the IPS operating system. Physical characteristics such as enabling the interface are performed in the ASA operating system by the ASA administrator.

The IPS SSP software modules can be installed to the ASA in any of the ASA 5500-X models.

d) **Cisco IPS Device Manager (IDM).**

The Cisco IDM is a web based application for sensor configuration and management. It can be accessed through Internet Explorer, Netscape or Mozilla by using the browser to connect to the IPS management interface and when downloaded it initiates its own Transport Layer Security (TLS) connection to the IPS for remote administration.

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 audit events related to cryptography functionality, identification and authentication and administrative actions. The Cisco IPS Routers generate an audit record for each auditable event. The administrator configures auditable events, backs up and manages audit data storage. The TOE provides audit data protection by providing audit trail protection using remote backup to a syslog server.

b) Cryptographic support

The TOE provides cryptography in support of remote administrative users via SSHv2 and TLSv1.0, TLSv1.1 and TLSv1.2. The cryptographic services include RSA signature services, SP800-90, RBG, SSH and AES. The entropy design description, justification, operation and health tests are assessed and documented in Cisco IPS Entropy Information (Ref [13]).

c) Full residual information protection

The TOE ensures that no information flows from the TOE that contains residual information from previous traffic.

d) Identification and authentication

The TOE provides authentication services for administrative users wishing to connect to the TOE's secure CLI administrative interface. The TOE provides authentication of administrators to a local user database, supporting password based authentication at either the serial console or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys.

e) Security management

All TOE administration occurs either through 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 internally maintains the date and time which is applied to audit records generated by the TOE.

g) Trusted path channels

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 and TLSv1.2. When configured by an administrator to dynamically modify access control lists on compatible network traffic filtering devices such as routers and firewalls, the TOE supports initiation of SSH connections to those network devices.

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 [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).

The IPS functionality is outside the scope of the scope of evaluation. The development of an extended package to NDPP to cover IPS systems is in progress and expected to complete in 2013.

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

The TOE consists of the Software version.7.2 (1). The hardware models in scope for these evaluation areas follows.

Table 2 TOE Components

TOE Components	
Description	**Identification**
Hardware	Cisco IPS 4345 Sensor
	Cisco IPS 4360 Sensor
	Cisco IPS 4510 Sensor
	Cisco IPS 4520 Sensor
These are software only IPS products	Cisco ASA 5512-X
	Cisco ASA 5515-X
	Cisco ASA 5525-X
	Cisco ASA 5545-X
	Cisco ASA 5555-X
SSP runs on the ASA 5585 –X firewalls	Cisco ASA 5585-X SSP-10
	Cisco ASA 5585-X SSP-20
	Cisco ASA 5585-X SSP-40
	Cisco ASA 5585-X SSP-60

2.6.2 Delivery Procedures

a) Hardware

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 customer.

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.

b) Software

For software, 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 PRE-wrapper document. This document is made available on the Cisco website for download.

In addition to verifying model numbers for hardware components, the software versions must also be verified by the customer recipient. Software versions can be checked by following the "Identifying *the Evaluated Hardware and Software*" in the user guidance (Ref [3]).

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 Intrusion Prevention System 7.2(1) Common Criteria Operational User Guidance and Preparative Procedures. Version .02, April 1, 2013, (Ref [3]). 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. It describes the process for secure installation and operation. It describes the 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 is 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 addition, the following organisational security policy must be in place:

d) 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]), Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4 (Refs [5], [6] and [7]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4 (CEM) (Ref [8]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [9], [10] and [11]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [12]) were also upheld.

3.3 Testing

Testing is determined in the Assurance activities in the Protection Profile.

Table 3 Requirements tested.

Mapping of Testing to NDPP requirements	
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 (Test1,2 & 3)
	FIA_UAU.7
Protection of the TOE Security Functions	FAU_GEN.1
	FPT_STM (Test1 & 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(Test1,2,3 & 4)
Protocol conformance	FAU_GEN.1
	FAU_STG_EXT.1
	FCS_TLS_EXT.1(Test 1)
	FCS_SSH_EXT.1.2(Test 1 & 2)
	FCS_SSH_EXT.1.3 (Test 1)
	FCS_SSH_EXT.1.4(Test 1)
	FCS_SSH_EXT.1.7(Test 1)

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.

- Denial of service attack: The evaluators changed the TOE address to prevent access to the TOE by the network. The evaluator discovered that after arp cache poisoning was stopped, the TOE was inaccessible via IDM, however after restarting the TOE, connections to the TOE via IDM were restored. The evaluators determined that should the environment switches be insecurely configured the TOE is unable to prevent this type of attack.

3.4 Entropy

The entropy design description, justification, operation and health tests are assessed and documented in a separate report (Ref [14]).

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 [3]), the Australasian Certification Authority certifies the evaluation of Cisco Intrusion Prevention System (Cisco IPS) performed by the Australasian Information Security Evaluation Program. CSC has found that Cisco Intrusion Prevention System (Cisco IPS upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the NDPP.

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 a DSD-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 assurance activities, and a vulnerability analysis (based upon TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

Compliance also provides assurance through evidence of secure delivery procedures.

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 ISM (Ref [2]) 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 (Ref [3]), the ACA also recommends that users and administrators:

a) should test the IPS using a trusted penetration tester annually.

b) be aware that IPS functionality is outside the scope of the scope of evaluation and was not tested. The development of an extended package to NDPP to cover IPS systems is in progress and expected to complete in 2013.

Annex A - References and Abbreviations

A.1 References

1. ST – Security Target for Cisco Intrusion Prevention System version 1.2, July 2013.

2. 2013 Australian Government Information Security Manual (ISM), Australian Signals Directorate, (available at www.dsd.gov.au).

3. User Guidance: Cisco Intrusion Prevention System 7.2(1) Common Criteria Operational User Guidance and Preparative Procedures. version 1.0, July 2013.

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

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

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

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

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

9. AISEP Policy Manual, APM, Version 4.0, August 2011, Defence Signals Directorate.

10. AISEP Certifier Policy, ACP. Version 4.0, August 2011, Defence Signals Directorate.

11. AISEP Evaluator Policy, AEP. Version 4.0, August 2011, Defence Signals Directorate.

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

13. Evaluation Technical Report: Cisco Intrusion Prevention System, Reference CSC-EFC-T0075-ETR Version 1.0 (proprietary).

14. Cisco IPS Entropy Information version 1.2 August 2013.

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CA	Certification Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
IDM	IPS Device Manager
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
TLS	Transport Layer Security