Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2007/41

March 2007

Version 1.0

Amendment Record

Version	Date	Description
1.0	21/3/2007	Public Release

Executive Summary

1 IOS/IPSec 12.4(6)T3, 12.4(7) and 12.2(33)SRA is a product that is designed to provide an implementation of the IPSec security standard within Cisco routers. This can provide a secure virtual private network (VPN) between trusted networks over an untrusted network. IOS/IPSec 12.4(6)T3, 12.4(7) and 12.2(33)SRA is the Target of Evaluation (TOE).

2 This report describes the findings of the IT security evaluation of Cisco Systems Inc's IOS/IPSec 12.4(6)T3, 12.4(7) and 12.2(33)SRA, to the Common Criteria (CC) evaluation assurance level EAL 2. The report concludes that the product has met the target assurance level of EAL 2 and that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by CSC Australia Pty Limited and was completed in March 2007.

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

4 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

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

1.2 Purpose

6 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, IOS/IPSec 12.4(6)T3, 12.4(7) and 12.2(33)SRA, against the requirements of the Common Criteria (CC) evaluation assurance level EAL 2, and

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

7 This report should be read in conjunction with the TOE Security Target (Ref [1]) that provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

8 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	IOS/IPSec 12.4(6)T3, 12.4(7) and 12.2(33)SRA.
Security Target	Security Target for Cisco IOS/IPSEC, Version 1.0, March 2007.
Evaluation Level	EAL 2.
Evaluation Technical Report	Evaluation Technical Report for Cisco IOS/IPSEC, Version 3.0, March 2007.
Criteria	CC Version 2.3, August 2005.
Methodology	CEM Version 2.3, August 2005.
Conformance	CC Part 2 Conformant. CC Part 3 Conformant.
Sponsor	Cisco Systems Australia Pty Ltd.
Developer	Cisco Systems Inc.
Evaluation Facility	CSC Australia Pty Limited.

Chapter 2 - Target of Evaluation

2.1 Overview

9 This chapter contains information about the Target of Evaluation (TOE), including: a description of functionality provided; its architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

10 The TOE is IOS/IPSec 12.4(6)T3, 12.4(7) and 12.2(33)SRA developed by Cisco Systems Inc. Its primary role is to implement the IPSec security standard within Cisco Systems routers.

11 Cisco routers run an embedded operating system called IOS (Internetworking Operating System), which is a proprietary operating system kernel written by Cisco Systems. Cisco's IOS supports a wide range of internetworking functions and capabilities, and operates on a number of Cisco platforms.

12 The Cisco IPSec implementation is a software function included in IOS. The cryptographic processing required for IPSec can be performed either in software, or using an optional hardware acceleration module that can be plugged into the router platform. The TOE comprises Cisco's implementation of IPSec in IOS release 12.4(6)T3, 12.4(7) and 12.2(33)SRA on various specified router platforms, with specified built in or optional IPSec hardware cryptographic acceleration modules included (see Table 2 – Evaluated Configurations).

13 The TOE provides confidentiality, authentication and integrity for IP data transmitted between Cisco Systems routers. A common application of this functionality is the construction of Virtual Private Networks (VPNs).

2.3 Security Policy

14 The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. There is an explicitly defined TSP in the Security Target (Ref [1]) in the form of an explicitly stated Security Function Policy (SFP). A summary is provided below.

15 Information Flow Control TSP:

The TOE provides authentication, integrity and confidentiality to packet flows based on the following security attributes.

- Receiving/transmitting interface

- Source/destination Internet Protocol (IP) address

- Source/destination Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port number

- Other IPSec attributes in the Encapsulating Security Payload (ESP) header

2.4 TOE Architecture

16 The TOE consists of the following major architectural subsystems:

a) Access Control Lists (ACL) - The purpose of the ACL subsystem is to permit or deny traffic flows through the TOE based on TSP.

b) Clock - The Clock subsystem maintains the run time clock function of the TOE.

c) Command Line Interface (CLI) - The TOE platform accepts administrative user input via the command line interface from an external terminal connected via the serial line or via a secure remote terminal connection to interfaces approved in organisational security policy.

d) Power-up Self Tests - The purpose of the power-on self test subsystem is to perform self tests when the TOE platform is started and upon user initiation of self-tests.

e) Crypto Engine - The purpose of the crypto engine is to provide cryptographic processing services to other subsystems.

f) IPSec - The purpose of the IPSec subsystem is to provide the mechanisms for the transmission of packets via, and the establishment of, a secure channel, over an insecure medium.

g) IPSec Internet Key Exchange (IKE) - The purpose of the IKE subsystem is to establish shared policy and keys in the form of security associations (SAs) between the TOE and an IPSec peer.

h) Logger - The purpose of the logger subsystem is to receive system event messages that are generated as normal part of TOE operation and store them in an internal or external buffer so they can be retrieved and reviewed by an authorised administrative user.

i) Public Key Infrastructure (PKI) - The purpose of the PKI subsystem is to authenticate the TOE with IPSec peers using digital certificates.

j) User Authentication - The purpose of the user authentication subsystem is to authenticate administrative users before they are permitted to access and/or configure the TOE.

2.5 Clarification of Scope

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

2.5.1 Evaluated Functionality

18 The TOE provides the following evaluated security functionality:

a) IPSec implementation including IKE and ESP.

b) Key management in support of the IPSec implementation.

c) Packet Filtering in support of the IPSec implementation.

d) Configuration and Management of the IPSec function, primarily via an interactive CLI. Event logging facilities with reliable timestamps are also provided.

2.5.2 Unevaluated Functionality

19 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 the Australian Government Information and Communications Technology Security Manual (ACSI 33) (Ref [2]) for policy relating to using an evaluated product in an unevaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

20 IOS provides many other non-IPSec services and functions that have not been included as part of the evaluation.

2.6 Usage

2.6.1 Evaluated Configuration

21 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 these defined evaluated configurations. Australian Government users should refer to ACSI 33 (Ref [2]) to ensure

that configurations meet the minimum Australian Government policy requirements. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

22 The evaluated configurations are shown in Table 2 below.

Table 2: Evaluated Configurations

Model Family	Supported Models	IPSec Hardware Acceleration Module	IOS Release
800	871, 876, 877, 878, 851, 851W, 857, 857W	Built In	12.4(6)T3
1800	1801, 1802, 1803, 1811, 1812	Built In	12.4(6)T3
	1841	Optional with AIM-VPN/BPII-PLUS	12.4(7)
2800	2801,2811, 2821, 2851	Optional with AIM-VPN/EPII-PLUS	12.4(7)
3800	3825	Optional with AIM-VPN/EPII-PLUS	12.4(7)
	3845	Optional with AIM-VPN/HPII-PLUS	12.4(7)
7200	7204, 7206	SA-VAM2+	12.4(7)
7300	7301	SA-VAM2+	12.4(7)
7600 Catalyst 6500	Any 6500/7600 with Supervisor Engine 720, 720-3B, or 720-3BXL	SPA-IPSEC-2G	12.2(33)SRA

23 For more information on the versions of the IPSec hardware acceleration modules in the evaluated configuration and the actual IOS image names used for the evaluated configurations see the document Installation and Configuration for Common Criteria EAL2 Evaluated Cisco IOS/IPSec, January 2007 (Ref [3]).

2.6.2 Delivery procedures

24 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product.

25 The Secure Installation and Configuration guide (Ref [3]), provides detailed steps, within the section entitled “Verification of Image and Hardware IPSec Module”, to enable the purchaser to verify the product is received in a secure manner. The document discusses how to:

a) Verify the package has in fact been sent by Cisco by inspecting the physical packaging and looking for the correct logo’s and markings;

b) Verify that the packaging has not obviously been opened and resealed and bears Cisco Tamper evident seals, and that those seals are in fact intact;

c) Validate serial numbers of components received, by comparing them with the serial numbers located on the invoice received prior to shipment; and

d) Download the correct image from the Cisco website.

2.6.3 Determining the Evaluated Configuration

26 The purchaser is able to verify that the product received is the evaluated product by consulting the section entitled “Installation Notes” within the Secure Installation and Configuration guide (Ref [3]). This section details how to verify the correct image has been installed via the IOS show version CLI command. The command output must indicate that the correct IOS version relative to the hardware model is being used. The command output will also allow the purchaser to determine if the hardware acceleration module is being used.

27 In addition, verification that the software image has not been tampered with may be gained by checking the Message-Digest #5 (MD5) hash value (generated by using a MD5 tool) against the table of hash values for the installed image listed within the Secure Installation and Configuration guide (Ref [3]).

28 The purchaser is also able to verify the correct hardware acceleration module has been received by comparing the output of the show diag command (show idprom module command for the 7600 / 6500) against the part and revision numbers located within the section entitled “Hardware Versions of Hardware IPSec/VPN Modules” within the Secure Installation and Configuration guide (Ref [3]).

2.6.4 Documentation

29 In order to ensure its secure usage, it is important that the TOE is used in accordance with guidance documentation. Australian Government users should refer to ACSI 33 (Ref [2]) to ensure that selected cryptography meets Australian Government policy requirements. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

30 The following document is available for download from the Cisco website:

a) Installation and Configuration for Common Criteria EAL2 Evaluated Cisco IOS/IPSec, January 2007 (Ref [3]).

2.6.5 Secure Usage

31 During the evaluation of the TOE, the following assumptions were made about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met:

a) The administrators are appropriately trained and trustworthy.

b) The TOE is physically secure.

c) The IT environment, including Certificate Authority (CA) and Network Time Protocol (NTP) services, is trustworthy.

d) The information flow policy for the TOE to enforce is valid.

Chapter 3 - Evaluation

3.1 Overview

32 This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

33 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation (Refs [4], [5] and [6]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [7]). The evaluation was also 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

34 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: developers test coverage and depth; test plans and procedures; and expected and actual results.

35 The evaluators used the test plans and scripts provided by the developer as the basis for validating the developer test results, as well as for developing the test cases for evaluator independent testing of the following TOE security functionality:

a) Identification and authentication.

b) Generation of keys and certificates.

c) IPSec Internet Key Exchange (IKE).

d) Management of time.

e) Management interfaces.

f) System messages.

g) Packet filtering.

h) IPSec Encapsulating Security Payload (ESP).

i) Encryption and hashing validation.

36 The evaluators included all hardware accelerator modules in the testing. Routers that have optional hardware acceleration were tested both with and without acceleration for tests associated with the functionality provided by IPSec IKE, IPSec ESP, cryptographic maps and key management.

3.4 Penetration Testing

37 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. Inputs into the vulnerability analysis included other evaluation deliverables, public domain sources and internal Cisco sources. The developers were able to show that no identified possible vulnerabilities were exploitable in the intended environment for the TOE.

38 The evaluators performed an independent vulnerability analysis using the developer's vulnerability analysis, as well as their own (independent) search of vulnerabilities in the public domain as of 30 January 2007, to devise and perform the following penetration tests:

a) Password Length.

b) Logging Buffer Overflow.

c) User Lockout.

d) Nessus Scan.

39 The analyses conducted by the evaluators, and subsequent testing, indicated that the TOE would resist an attacker with a low attack potential, consistent with the requirements of an EAL 2 evaluation.

Chapter 4 - Certification

4.1 Overview

40 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Certification Result

41 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 IOS/IPSec 12.4(6)T3, 12.4(7) and 12.2(33)SRA performed by the Australasian Information Security Evaluation Facility, CSC Australia Pty Limited.

42 CSC Australia Pty Limited has found that IOS/IPSec 12.4(6)T3, 12.4(7) and 12.2(33)SRA upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL 2.

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

4.3 Assurance Level Information

44 EAL2 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation and the high-level design of the Target of Evaluation (TOE), to understand the security behaviour.

45 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities.

46 EAL2 also provides assurance through a configuration list for the TOE, and evidence of secure delivery procedures.

4.4 Recommendations

47 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 ACSI 33 (Ref [2]) and New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

48 For Australian Government users the specific cryptographic configuration that must be used is:

a) DSD Approved Cryptographic Algorithms (DACA).

b) Key generation using parameters that meet ACSI 33 (Ref [2]).

c) IKE Phase 1 using Main Mode, IKE Phase 2 using Quick Mode.

d) Security Association (SA) establishment using a Group that meets ACSI 33 (Ref [2]).

e) Maximum SA lifetime of 4 hours (14400 seconds).

f) Use Keyed-Hash Message Authentication Code (HMAC) that uses a DSD approved hashing algorithm from ACSI 33 (Ref [2]).

g) ESP Tunnel Mode Operation.

49 Consumers should also ensure that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [3]).

Annex A - References and Abbreviations

A.1 References

[1] Security Target (ST) for Cisco IOS/IPSEC, Version 1.0, March 2007, Cisco Systems Inc.

[2] Australian Government Information and Communications Technology Security Manual (ACSI 33), September 2006, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] Installation and Configuration for Common Criteria EAL2 Evaluated Cisco IOS/IPSec, January 2007, (available at http://www.cisco.com/ univercd/cc/td/doc/product/software/ios124/124sup/ccipsec3.htm).

[4] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 2.3, August 2005, CCIMB-2005-08-001.

[5] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC), Version 2.3, August 2005, CCIMB-2005-08-002.

[6] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC), Version 2.3, August 2005, CCIMB-2005-08-003.

[7] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology (CEM), Version 2.3, August 2005, CCMB-2005-08-004.

[8] Australasian Information Security Evaluation Program (AISEP) Publication No. 1, Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[9] Australasian Information Security Evaluation Program (AISEP) Publication No. 2, Certifier Guidance, AP 2, Version 3.1, 29 September 2006, Defence Signals Directorate.

[10] Australasian Information Security Evaluation Program (AISEP) Publication No. 3, Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, Defence Signals Directorate.

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

[12] Cisco IOS/IPSec Evaluation Technical Report, Version 3.0, March 2007, CSC Australia Pty Limited, (COMMERCIAL-IN-CONFIDENCE).

A.2 Abbreviations

ACA	Australasian Certification Authority
ACL	Access Control List
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CA	Certificate Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
DACA	DSD Approved Cryptographic Algorithm
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
HMAC	Keyed-Hash Message Authentication Code
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IOS	Cisco’s Internetworking Operating System
IP	Internet Protocol
IPSec	IETF standards for Internet Protocol Security
MD5	Message-Digest #5
NTP	Network Time Protocol
PKI	Public Key Infrastructure
PP	Protection Profile
SA	Security Association
SFP	Security Function Policy
SFR	Security Functional Requirements
SHA-1	Secure Hash Algorithm #1
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functions

TSP	TOE Security Policy
UDP	User Datagram Protocol
VPN	Virtual Private Network