Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2006/38

September 2006

Version 1.0

Amendment Record

Version	Date	Description
1.0	29/9/2006	Public release.

Executive Summary

1 IOS/IPSec 12.3(6a) 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 12.3(6a) is the Target of Evaluation (TOE).

2 This report describes the findings of the IT security evaluation of Cisco Systems Inc's IOS/IPSec 12.3(6a), to the Common Criteria (CC) evaluation assurance level EAL 4. The report concludes that the product has met the target assurance level of EAL 4 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 and was completed on 26 May 2006.

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 12.3(6a), against the requirements of the Common Criteria (CC) evaluation assurance level EAL 4, 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'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

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 12.3(6a)
Security Target	Security Target for Cisco IOS/IPSEC, Version 4.8, May 2006
Evaluation Level	EAL 4
Evaluation Technical Report	Evaluation Technical Report for Cisco IOS/IPSec, Version 2.0, May 2006
Criteria	CC Version 2.1, August 1999, with interpretations as of 6 June 2003.
Methodology	CEM-99/045 Version 1.0, August 1999, with interpretations as of 6 June 2003.
Conformance	CC Part 2 Extended CC Part 3 Conformant
Sponsor	Cisco Systems Australia Pty. Ltd.
Developer	Cisco Systems Inc
Evaluation Facility	CSC Australia

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 12.3(6a) 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 12.3(6a) on various specified router platforms with specified IPSec acceleration hardware included.

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

16 Other TSPs were also identified by the developer. These are listed below:

17 Management Session TSP

The TOE ensures that only authorised users are permitted to initiate an interactive security function management session.

18 System Message Management TSP

Only privileged users are permitted to view the logs or modify the logging configuration.

19 Time Management TSP

Only privileged users can modify the timekeeping configuration of the TOE.

2.4 TOE Architecture

20 The TOE consists of the following major architectural subsystems:

a) Access Control Lists.

b) Clock.

c) Command Line Interface (CLI).

d) Crypto Engine.

e) IPSec.

f) IPSec Internet Key Exchange (IKE).

g) Logger.

h) Public Key Infrastructure (PKI).

i) User Authentication .

2.5 Clarification of Scope

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

2.5.1 Evaluated Functionality

22 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 Non-evaluated Functionality

23 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 and Technology Security Manual (ACSI 33) (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).

24 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

25 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).

26 The evaluated configurations are shown in Table 2 below. Note that to be in an evaluated configuration use of the specified hardware acceleration modules is mandatory.

Table 2: Evaluated Configurations

Hardware Family	Supported Models	IPSec Hardware Acceleration Module	IOS Software Version
Cisco 1700 series	1720, 1721, 1760	MOD1700-VPN	Cisco IOS 12.3(6a)
Cisco 2600XM series	2610XM, 2611XM, 2620XM, 2621XM, 2650XM, 2651XM	AIM-VPN/EP	Cisco IOS 12.3(6a)
		AIM-VPN-BPII	Cisco IOS 12.3(6a)
Cisco 3600 series	3660	AIM-VPN/HP	Cisco IOS 12.3(6a)
Cisco 3700 series	3725	AIM-VPN/EPII	Cisco IOS 12.3(6a)
	3745	AIM-VPN/HPII	Cisco IOS 12.3(6a)
Cisco 7200 series	7204, 7206	SA-VAM2	Cisco IOS 12.3(6a)
Cisco 7300 series	7301	SA-VAM2	Cisco IOS 12.3(6a)

27 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 EAL4 Evaluated Cisco IOS/IPSec (Ref [3]).

2.6.2 Delivery procedures

28 At the time of Certification it is not possible to order the evaluated configuration from Cisco. Potential customers should contact Cisco for further information about the status of their evaluated products and their products that are currently undergoing evaluation.

29 For pre-existing hardware, serial numbers can be checked against paper or electronic invoice records. The Cisco IOS CLI command `show diag` can be used to ascertain the serial number of the installed IPSec hardware acceleration module.

30 Users who want to use the evaluated version of software should use the table of Message-Digest #5 (MD5) hash values for IOS software images

contained in Installation and Configuration for Common Criteria EAL4 Evaluated Cisco IOS/IPSec (Ref [3]). A tool to calculate a file MD5 hash is required. It is assumed that administrators know how to download the applicable software image into the router in a way that survives power down.

2.6.3 Determining the Evaluated Configuration

31 Users should be aware of the IOS `show version` CLI command. It must indicate that IOS version 12.3(6a) is being used and that the hardware acceleration module is being used.

2.6.4 Documentation

32 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The relevant documentation is in Installation and Configuration for Common Criteria EAL4 Evaluated Cisco IOS/IPSec (Ref [3]). Note that in this case the use of IPSec hardware acceleration is mandatory. 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).

2.6.5 Secure Usage

33 The following assumptions were made during the evaluation concerning the operational environment of the TOE:

a) The administrators are appropriately trained and trustworthy.

b) The TOE is physically secure

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

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

Chapter 3 - Evaluation

3.1 Overview

34 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

35 The criteria against which the Target of Evaluation (TOE) has been evaluated are expressed in the Common Criteria for Information Technology Security Evaluation (Refs [4], [5],[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]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [10]) were also upheld.

3.3 Functional Testing

36 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the developer's testing effort. Evidence analysed included developer test plans and results, as well as developer coverage and depth analysis. The evaluators repeated a sample of the developer tests to gain confidence in their overall validity.

37 The evaluators also devised additional tests to gain assurance that the TOE operates as specified. These additional tests exercised aspects of the TOE security functionality listed below:

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).

3.4 Penetration Testing

38 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 as of May 2005. The developers were able to show that no identified possible vulnerabilities were exploitable in the intended environment for the TOE.

39 The evaluators also performed an independent vulnerability analysis. The evaluators used the developer vulnerability analysis and their own (independent) vulnerability analysis to generate penetration tests. These analyses, and subsequent testing, indicated that the TOE will resist an attacker with a low attack potential.

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 [11]), the Australasian Certification Authority certifies the evaluation of IOS/IPSec 12.3(6a) performed by the Australasian Information Security Evaluation Facility, CSC Australia.

42 CSC Australia has determined that IOS/IPSec 12.3(6a) upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL 4.

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

4.3 Assurance Level Information

44 EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behaviour. Assurance is additionally gained though an informal model of the TOE security policy.

45 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, evidence of a developer search for obvious vulnerabilities, and an independent vulnerability analysis demonstrating resistance to penetration attackers with a low attack potential.

46 EAL4 also provides assurance though the use of development environment controls and additional TOE configuration management including automation, 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 (DACAs).

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 meets ACSI 33 (Ref [2]).

g) ESP Tunnel Mode Operation.

49 The Australasian Certification Authority (ACA) also notes that strong passwords for router logon and router administration must be used to prevent the success of password guessing attacks. Australian Government users should refer to ACSI 33 (Ref [2]) for policy on password selection.

Annex A - References and Abbreviations

A.1 References

[1] Security Target for Cisco IOS/IPSEC, Version 4.8, Cisco Systems Inc.

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

[3] Installation and Configuration for Common Criteria EAL4 Evaluated Cisco IOS IPSec, Version 2.4, August 2005, (at http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123sup/ccipsec2.htm).

[4] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 2.1, August 1999, CCIMB-99-031, incorporating interpretations as of 6 June 2003.

[5] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC), Version 2.1, August 1999, CCIMB-99-032, incorporating interpretations as of 6 June 2003.

[6] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC), Version 2.1, August 1999, CCIMB-99-033, incorporating interpretations as of 6 June 2003.

[7] Common Methodology for Information Technology Security Evaluation (CEM), Version 1.0, August 1999, CEM-99/045, incorporating interpretations as of 6 June 2003.

[8] AISEP Publication No. 1 – Description of the AISEP, AP 1, Version 2.0, February 2001, Defence Signals Directorate.

[9] AISEP Publication No. 2 – The Licensing of the AISEFs, AP 2. Version 2.1, February 2001, Defence Signals Directorate.

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

[11] Cisco IOS/IPSec Evaluation Technical Report, Version 2.0, May 2006, CSC Australia. (EVALUATION-IN-CONFIDENCE)

A.2 Abbreviations

ACA	Australasian Certification Authority
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
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
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