Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2007/42

25 May 2007

Version 1.0

Amendment Record

Version	Date	Description
1.0	25/05/2007	Public release.

Executive Summary

1 Remote Access VPN is a product that is designed to allow trusted IT systems to securely communicate over an untrusted network. Remote Access VPN including Cisco VPN Client for Windows 4.8.00, Cisco VPN Client for Linux 4.8.00, Cisco VPN Client for Solaris 4.6.02, Movian VPN Client for Pocket PC 4.00, Movian VPN Client for Palm OS 4.00, Antha VPN Client for Windows CE.NET 5.6.2, Cisco VPN 3002 and 3002-8E Hardware VPN Clients 4.7.2.D, Cisco PIX 501 6.3(5), Cisco 831 and 837 Routers IOS 12.4(5a), Cisco VPN 3005, 3015, 3020, 3030, 3060 and 3080 Concentrators 4.1.7.N and CiscoSecure ACS 4.0 are the Target of Evaluation (TOE).

2 This report describes the findings of the IT security evaluation of Cisco Systems Inc's Remote Access VPN, to the Common Criteria (CC) evaluation assurance level EAL2. The report concludes that the product has met the target assurance level of EAL2 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 21 May 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, Remote Access VPN, against the requirements of the Common Criteria (CC) evaluation assurance level EAL2, 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	Remote Access VPN
Version	Cisco VPN Client for Windows 4.8.00, Cisco VPN Client for Linux 4.8.00, Cisco VPN Client for Solaris 4.6.02, Movian VPN Client for Pocket PC 4.00, Movian VPN Client for Palm OS 4.00, Antha VPN Client for Windows CE.NET 5.6.2, Cisco VPN 3002 and 3002-8E Hardware VPN Clients 4.7.2.D, Cisco PIX 501 6.3(5), Cisco 831 and 837 Routers running IOS 12.4(5a), Cisco VPN 3005, 3015, 3020, 3030, 3060 and 3080 Concentrators 4.1.7.N and CiscoSecure ACS 4.0
Security Target	Security Target for Cisco Remote Access VPN, Version 1.17. (Ref [1])
Evaluation Level	EAL2
Evaluation Technical Report	Evaluation Technical Report for Cisco Remote Access VPN, Version 3.0, 21 May 2007. (Ref [13])
Criteria	CC Version 2.1, August 1999, with interpretations as of 30 July 2002.
Methodology	CEM-99/045 Version 1.0, August 1999, with interpretations as of 30 July 2002.
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 the Remote Access VPN developed by Cisco Systems Inc and some additional third party software clients. Its primary role is to provide remote users with secure access to centralised resources via an untrusted communications network.

11 The TOE supports a model where remote users connect to a centralised server using the Internet Engineering Task Force (IETF) IPSec protocol to ensure confidentiality, authentication and integrity.

12 The centralised server is known as the VPN Concentrator. It is a specialised network appliance that is designed to support many simultaneous IPSec connections. For large rollouts the VPN Concentrator may be required to handle the server end of many thousands of IPSec connections.

13 The client end of each IPSec connection can be handled by a single client computer running one of several supported operating systems and the appropriate client software. Alternatively, an IPSec connection for a handful of computers on a small LAN can be handled by a small network appliance known as a VPN Hardware Client.

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. The TSP is defined in the Security Target (Ref [1]). A summary of the explicitly stated TSP is provided below:

15 Access Control TSP:

a) Only the suitably privileged administrator can access configuration information.

b) Cryptographic keying material on the VPN Concentrator is not available to users.

16 Information Flow Control TSP:

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

a) Source / Destination IP address.

b) Source / Destination port number.

c) Authentication credentials including:

   i) Shared group keys.

   ii) Digital certificates.

   iii) Name and password.

2.4 TOE Architecture

17 The TOE consists of the following major architectural components:

a) The VPN Concentrator.

b) The VPN Client.

c) External Authentication Server (optional).

18 The Developer's Architectural Design identifies the following components of the TOE:

a) IPSec Implementation:

   i) IPSec Authentication.

   ii) IPSec Encryption.

b) Filtering Controls:

   i) VPN Concentrator Interface Access Control.

   ii) VPN Client Access Control.

   iii) VPN Client Split Tunnelling.

c) Management:

   i) VPN Concentrator Configuration and Operation.

   ii) VPN Client Configuration and Operation.

   iii) Authentication Server Configuration and Operation.

iv) Management of Groups and Users.

v) Digital Certificate Management.

vi) Logging of Events.

vii) Maintenance of Time.

2.5 Clarification of Scope

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

2.5.1 Evaluated Functionality

20 The TOE provides the following evaluated security functionality:

a) IPSec implementation including IKE and ESP.

b) Packet Filtering in support of IPSec and control of Split Tunnelling.

c) Management of the IPSec and ancillary TOE functions.

2.5.2 Non-evaluated Functionality

21 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).

2.6 Usage

2.6.1 Evaluated Configuration

22 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 GCSB.

Component	Description	Version	Host Operating System
Software VPN Clients	Cisco VPN Client for Windows	4.8.00 (0440)	Windows XP Professional (SP2)
	Cisco VPN Client for Linux	4.8.0 (0490)	Redhat Linux 3.2.2-5 (kernel 2.4.20-8)
	Cisco VPN Client for Solaris	4.6.02 (0030)	Solaris 10 (SPARC)
	Movian VPN Client for Pocket PC	4.00 Build 113.12c	Pocket PC 2002 v3.0.11171
	Movian VPN Client for PalmOS	4.00 Build 112.15P	Garret V5.4.9 PalmOS
	Antha VPN Client for Windows CE.NET	5.6.2	Windows CE.NET 4.20
Hardware VPN Clients	Cisco VPN 3002 and 3002-8E	4.7.2.D	N/A – integrated OS
	Cisco PIX 501	6.3(5)	N/A – integrated OS
	Cisco 831 and 837 Routers	12.4(5a) (fc3)	N/A – integrated OS
VPN Concentrator	Cisco VPN 3005 and 3015 Concentrators	4.1.7.N	N/A – integrated OS
VPN Concentrator with Scalable Encryption Processors (SEPs)	Cisco VPN 3020, 3030, 3060 and 3080 Concentrators	4.1.7.N	N/A – integrated OS
Authentication Server	CiscoSecure ACS	4.0(1) Build 27	Windows Server 2003 (standard ed)
SEPs	Scaleable Encryption Processor	SEP-E	4.0 or later

23 The TOE components listed above can be configured in many different ways. For further information on correct configuration see the document Installation and Configuration for Common Criteria EAL2 Evaluated Cisco Remote Access VPN (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. The document Installation and Configuration for Common Criteria EAL2 Evaluated Cisco Remote Access VPN (Ref [3]) provides information on secure delivery of Cisco VPN Concentrator and VPN Client Hardware,

and Cisco VPN Concentrator and Client Software including Cisco Secure ACS for Windows. This document also provides information on verification of the Movian and Antha VPN Client software within the scope of the TOE.

2.6.3 Determining the Evaluated Configuration

25 The document Installation and Configuration for Common Criteria EAL2 Evaluated Cisco Remote Access VPN (Ref [3]) provides information on configuration options compatible with the evaluated configuration.

2.6.4 Documentation

26 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. As well as the document Installation and Configuration for Common Criteria EAL2 Evaluated Cisco Remote Access VPN (Ref [3]) mentioned above, a suite of documentation is available from Cisco to aid the secure installation and use of the TOE.

Components	**Installation Information**
Cisco VPN Concentrators	Cisco VPN 3000 Getting Started, Release 4.1
Cisco VPN Software VPN Clients	VPN Client Administrator Guide, Release 4.1 VPN Client User Guide, Release 4.1
Cisco VPN Hardware VPN Clients	VPN 3002 Hardware Client getting Started Guide, Release 4.1 Cisco PIX 501 Firewall Quick Start Guide, Version 6.3 Loading Cisco IOS Software Cisco Easy VPN Remote Configuring Certification Authority Interoperability
Certicom movianVPN Software VPN Clients	movianVPN Version 4.0, User's Guide for PalmOS movianVPN Version 4.0, User's Guide for WinCE Pocket PC and Handheld PC
anthaVPN Software VPN Clients	AnthaVPN User Guide Ed.2
Cisco Secure ACS Authentication Server	Installation Guide for Cisco Secure ACS for Windows Servers, Release 4.0

2.6.5 Secure Usage

27 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.

28 Section 3 Assumptions in the Security Target (Ref [1]) provides a full description of the assumptions. It is important to note that security can only be maintained if passwords, tokens and certificates used in the system are all secure.

29 It is vital that all users are aware that the use of a VPN product does not protect against vulnerabilities in a remote VPN Client host operating system. In fact, the use of a VPN means that weaknesses in VPN Client host operating systems can be used as a good launching pad for attacks on the otherwise protected centralised corporate data.

Chapter 3 - Evaluation

3.1 Overview

30 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

31 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], [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] - [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 Functional Testing

32 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: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

33 The evaluators verified developer tests of the IPSec.Encrypt, Filtering.Interface, Filtering.Client, Filtering.SplitControl, Mgt.Conc and Mgt.EventLog TOE Security Functions. They devised independent tests to cover the IPSec.Auth, IPSec.Encrypt, Mgt.Client, Mgt.AuthServ, Mgt.User, Mgt.CertMgt, Mgt.EventLog and Mgt.Clock TOE Security Functions.

34 Whilst only a subset of possible TOE configurations were tested, all TOE images were included in the tests.

3.4 Penetration Testing

35 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.

36 Based on the developer's vulnerability analysis, the evaluators devised and conducted a series of penetration tests. They found two residual vulnerabilities of note:

a) Weak user and group passwords can be guessed very quickly using freely available tools. Similarly, these passwords can be read off client hosts that are physically compromised or running compromised operating systems or applications. This is a residual vulnerability because of the assumptions A.Password and A.Soft-Secure contained in the ST (Ref [1]).

b) For correct operation of the TOE, some commonly used network services such as DHCP might be required. System administrators should ensure that the host operating system is properly patched. Any host vulnerabilities are outside the scope of the TOE and are thus classified as residual vulnerabilities.

Chapter 4 - Certification

4.1 Overview

37 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

38 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [13]), the Australasian Certification Authority (ACA) certifies the evaluation of Remote Access VPN performed by the Australasian Information Security Evaluation Facility, CSC Australia.

39 CSC Australia has found that Remote Access VPN upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL2.

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

4.3 Assurance Level Information

41 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.

42 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.

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

4.4 Recommendations

44 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).

45 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [3]), some specific ACA recommendations are made below.

46 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.

47 The ACA also notes that strong passwords for VPN concentrator logon and 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.

48 As indicated in Section 2.6.5 and Section 3.4 of this report, VPN Client host operating systems and physical security must be suitably secure. VPN Client software does not protect against Client host vulnerabilities or physical security vulnerabilities. If these other vulnerabilities are exploited then the VPN communications can be compromised as well.

49 In addition to the assumptions on client security detailed in Section 3.4 of this report, the use of group passwords should be strictly limited to situations where there is no conflict of interest between all clients sharing a given password. Knowledge of the group password allows man-in-the-middle attacks whereby the end user cannot authenticate the VPN concentrator to which they are connected, thus allowing a full compromise of the end user session via VPN Concentrator spoofing.

Annex A - References and Abbreviations

A.1 References

[1] Security Target for Cisco Remote Access VPN, Version 1.17, 16 May 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 Remote Access VPN, March 2007, (available at: http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/products_installation_and_configuration_guides_list.html).

[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 30 July 2002.

[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 30 July 2002.

[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 30 July 2002.

[7] Common Methodology for Information Technology Security Evaluation (CEM), Version 1.0, August 1999, CEM-99/045, incorporating interpretations as of 30 July 2002.

[8] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[9] AISEP Publication No. 2 – Certifier Guidance, AP 2, Version 3.0, 21 February 2006, Defence Signals Directorate.

[10] AISEP Publication No. 3 – Evaluator Guidance, AP 3, Version 3.1, 29 September 2006, Defence Signals Directorate.

[11] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4, Version 3.1, 29 September 2006, Defence Signals Directorate.

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

[13] Cisco Remote Access VPN Evaluation Technical Report, Version 3.0, 21 May 2007, CSC Australia.

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
DACA	DSD Approved Cryptographic Algorithm
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
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
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
VPN	Virtual Private Network