Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Cisco AnyConnect Secure Mobility Desktop Client version 4.1

Certification Report
2015/96

08-10-2015
Version 1.0

Amendment Record

Version	Date	Description
1.0	08-10-2015	Final

Executive Summary

This report describes the findings of the IT security evaluation of Cisco AnyConnect Secure Mobility Desktop Client version 4.1 against the Protection Profile for IPsec Virtual Private Network (VPN) Clients. The Target of Evaluation (TOE) is Cisco AnyConnect Secure Mobility Desktop Client version 4.1. The TOE is a product that is designed as a VPN client. A VPN client provides protection of data in transit across a public network. The VPN client implements IPsec to establish a cryptographic tunnel protecting the transmission of data between IPsec peers. The VPN client is intended to be located outside an organisation's private network, protecting data flows between a host and the Cisco 5500 Series Adaptive Security Appliance (ASA) VPN Gateway.

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Cryptographic Support** – A FIPS 140-2 validated cryptographic module is included providing cryptographic services for IPsec session establishment and ESP encryption.
- **User Data Protection** – Network packets sent from the TOE do not include residual information.
- **Identification and Authentication** – The TOE requires successful X.509v3 certificate authentication and validation of the VPN Gateway prior to establishing an IPsec connection.
- **Security Management** – The TOE provides interfaces to specify the configuration of IPsec and X.509 certificate validation.
- **Protection of the TSF** – The TOE provides trusted updates and executes a suite of self-tests during start-up to verify its correct operation.
- **Trusted Path / Channels** – The TOE implements IPsec to provide a trusted channel between the TOE platform and a remote VPN Gateway.

The report concludes that the product has complied with the Protection Profile for IPsec Virtual Private Network (VPN) Clients, 12-10-2013 version 1.4 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 Australia Pty Ltd and was completed on 28 August 2015.

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

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
b) Configure and operate the TOE according to the vendor's product administrator guidance
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
d) Ensure the VPN Gateway is not configured or operated in BYPASS mode.

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 and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

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 AnyConnect Secure Mobility Desktop Client Version 4.1 against the requirements of the Common Criteria (CC) and the Protection Profile for IPsec Virtual Private Network (VPN) Clients, 12-10-2013 version 1.4.

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 Cisco AnyConnect Secure Mobility Desktop Client version 4.1.

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	Cisco AnyConnect Secure Mobility Desktop Client
Software Version	4.1
Hardware Platforms	The TOE relies on the Microsoft Windows 7, 8, 8.1 Operating System Platform.
Security Target	Cisco AnyConnect Secure Mobility Desktop Client Security Target Version 1.0 16-9-2015

Evaluation Technical Report	Evaluation Technical Report version B.0, dated 25-8-2015, Document reference CSC-EFC-T0082-ETR
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, 09-2012, Version 3.1.Rev 4
Methodology	Common Methodology for Information Technology Security Version 3.1 Rev 4 09-2012
Conformance	Protection Profile for IPsec Virtual Private Network (VPN) Clients, version 1.4, 12-10-2013
Developer	Cisco Systems, Inc.
Evaluation Facility	CSC Australia Pty Ltd 12 Brindabella Circuit Brindabella Business Park ACT 2609

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

The TOE is Cisco AnyConnect Secure Mobility Desktop Client version 4.1.

A VPN Client allows remote users to use client computers to establish an encrypted IPsec tunnel across an unprotected public network to an organization's private network. The VPN Client protects the data between itself and a VPN Gateway, providing confidentiality, integrity, and protection of data in transit as it traverses a public network.

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Cryptographic Support** – The TOE provides ESP symmetric cryptography for bulk AES encryption/decryption and SHA-2 algorithm for hashing. In addition the TOE provides the cryptography to support Diffie-Hellman key exchange and derivation function used in the IKEv2 protocol. The TOE incorporates the FIPS Object Module (FOM) v4.1 in accordance with the FIPS 140-2 standard. The Cisco FOM is a FIPS 140-2 validated cryptographic module, certificate #2100. The TOE platform provides asymmetric cryptography for IKE peer authentication using digital signature and hashing services. In addition the TOE platform provides a DRBG.
- **User Data Protection** – The TOE and TOE platform ensures that residual information from previously sent network packets processed through the platform are protected from being passed into subsequent network packets.
- **Identification and Authentication** – The TOE and TOE platform perform device-level X.509 certificate-based authentication of the VPN Gateway during IKE v2 key exchange. Device-level authentication allows the TOE to establish a secure channel with a trusted VPN Gateway. The secure channel is established only after each endpoint authenticates each other.
- **Security Management** – The TOE, TOE platform, and VPN Gateway provide the management functions to configure the security functionality provided by the TOE.
- **Protection of the TSF** – The TOE performs a suite of self-tests during initial start-up to verify correct operation of its FIPS 140-2 validated algorithms. Upon execution, the integrity of the TOE's software executables is also verified. The TOE and TOE Platform provide for verification of TOE software updates prior to installation.

- **Trusted Path / Channels** – The TOE's implementation of IPsec provides a trusted channel ensuring sensitive data is protected from unauthorised disclosure or modification when transmitted from the host to a VPN gateway.

2.3 TOE Functionality

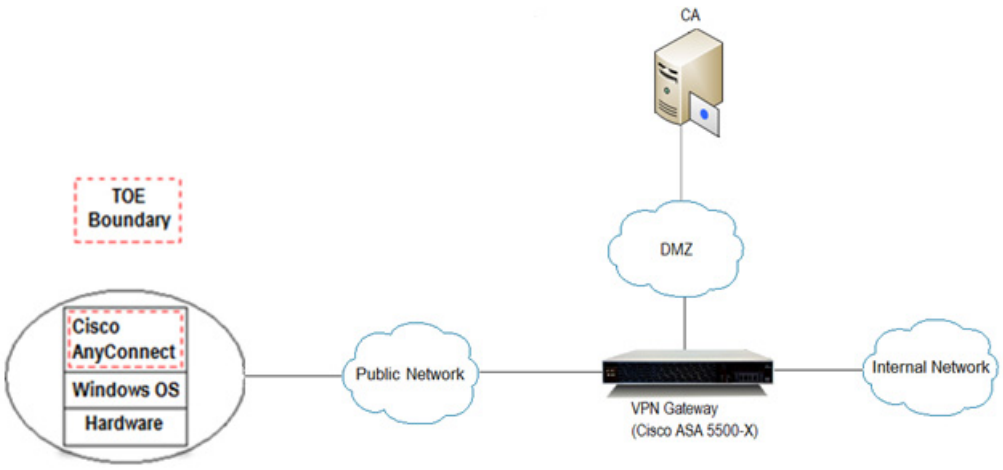
The TOE is the core VPN component of the Cisco AnyConnect Secure Mobility Desktop Client (herein after referred to as the VPN client, or the TOE). The Cisco AnyConnect Secure Mobility client is a next-generation VPN client, providing remote users with secure IPsec (IKEv2) VPN connections to the Cisco 5500 Series Adaptive Security Appliance (ASA) VPN Gateway. The TOE is a software-only product running on Windows 7, 8, or 8.1.

The VPN client implements IPsec to establish a cryptographic tunnel protecting the transmission of data between IPsec peers. The VPN client is intended to be located outside an organisation's private network, protecting data flows between a host and the Cisco 5500 Series Adaptive Security Appliance (ASA) VPN Gateway.

2.4 TOE Architecture

The TOE consists of the following major architectural components:

- software-only IPsec VPN client application that protects data in transit on both IPv4 and IPv6 networks



2.5 Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per the Cisco AnyConnect Secure Mobility Desktop Client CC Configuration Guide (Ref 2).

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

2.5.1 Evaluated Functionality

All tests performed during the evaluation were taken from Protection Profile for IPsec Virtual Private Network (VPN) Clients (Ref 3) and sufficiently demonstrate the security functionality of the TOE.

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 4) 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 following components are considered outside of the scope of the TOE:

- Non-FIPS 140-2 mode of operation on the TOE.

2.6 Security

2.6.1 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 a summary of the functionality to be evaluated:

- Cryptographic Support
- User Data Protection / Information Flow Control
- Identification and Authentication
- Security Management
- Protection of the TSF
- Trusted Path/Channel.

2.7 Usage

2.7.1 Evaluated Configuration

The TOE consists of the VPN client software. The TOE environment consists of a Certificate Authority used to provide valid digital certificates, Microsoft Windows 7,

8, 8.1 Operating System Platform, and the Cisco ASA 5500-X, which functions as the head-end VPN Gateway.
The evaluation was conducted on the default installation and configuration of the TOE with additional guidance and configuration information drawn from the Cisco AnyConnect Secure Mobility Desktop Client CC Configuration Guide (Ref 2).

2.7.2 Secure Delivery

To ensure that the software downloaded is the evaluated product the customer must check the version details received against the list specified in the TOE.

Customers will access CCO (Cisco Connection Online) to download Cisco software products. Customers 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.

Upon download, if the Digital Signature information says the signature is "**not valid**" as displayed in the example below:

Do not continue to install the VPN module and contact Cisco Technical Support for assistance.

2.7.3 Installation of the TOE

The Configuration Guide (Ref 2) contains all relevant information for the secure configuration of the TOE

2.8 Version Verification

The verification of the TOE is largely automatic.

2.9 Documentation and Guidance

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. All guidance material is available for download at www.cisco.com.
All common criteria guidance material is available at **www.commoncriteriaportal.org**. The Information Security Manual (ISM) is available at **www.asd.gov.au**.

2.10 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.

- This Cisco usage document assumes that you are familiar with the basic concepts and terminologies used in internetworking, and understand your

network topology and the protocols that the devices in your network can use, that you are a trusted individual, and that you are trained to use the operating systems on which you are running your network.

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 Protection Profile for IPsec Virtual Private Network (VPN) Clients and Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4, Parts 2 and 3 (Ref 5 and 6).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4 (Ref 7).

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP).

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref 8) were also upheld.

- The evaluation was based on the default installation and configuration of the TOE with additional configuration taken from Cisco AnyConnect Secure Mobility Desktop Client CC Configuration Guide Version 1.0, 09-2015 (Ref 2).

3.3 Testing

3.3.1 Testing Coverage

All tests performed by the evaluators were taken from the Protection Profile for IPsec Virtual Private Network (VPN) Clients. These tests are designed in such a way as to provide a full coverage of testing for all security functions claimed by the TOE. All SFRs listed in the Security Target and the Protection Profile packages were exercised during testing.

3.3.2 Testing

Testing is determined in the assurance activities in the Protection Profile. The test cases were developed in accordance with the National Association of Testing Authorities (NATA) requirements defined in section 5.4 of ISO/IEC 17025.

Sampling

- In terms of selecting the TOE software, the evaluators have tested the only software version in scope, but selected to run it on a subset of the platforms based on the following: The TOE can be run on 3 versions of Windows; however there is no fundamental difference between each Operating System

3.4 Entropy Testing

This requirement (paraphrased below) was passed by the evaluators.

For each platform listed in the ST, the evaluator shall examine the ST of the platform to ensure that the RBG functions claimed in that platform's ST contains the RBG functions in the VPN Client's ST. The evaluator shall also examine the TSS of the VPN Client's ST to verify that it describes (for each supported platform) how the RBG functionality is invoked for each operation they are used for in the VPN client (it should be noted that this may be through a mechanism that is not implemented by the VPN Client; nonetheless, that mechanism will be identified in the TSS as part of this assurance activity).
Further information on this topic is available from NIST publication SP800-90A Recommendations for Random Number Generation Using Deterministic Random Bit Generation, 01-2012 (Ref 10).

3.5 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. This analysis included a search for possible vulnerability sources in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time)

b) Specialist technical expertise required (specialist expertise)

c) Knowledge of the TOE design and operation (knowledge of the TOE)

d) Window of opportunity

e) IT hardware/software or other equipment required for the exploitation.

Chapter 4 – Certification

4.1 Overview

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

4.2 Assurance

This certification is focused on the evaluation of product compliance with a Protection Profile that covers the technology area of IPsec Virtual Private Network (VPN) Clients. Agencies can have confidence that the scope of an evaluation against an ASD 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). PPs provide assurance by a full security target and an analysis of the SFR 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 Protection Profile for IPsec Virtual Private Network (VPN) Clients 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.

4.3 Certification Result

After due consideration of the conduct of the evaluation as reported to the certifiers and of the Evaluation Technical Report (Ref 11) the Australasian Certification Authority **certifies** the evaluation of the product performed by the Australasian Information Security Evaluation Facility, CSC Australia Pty Ltd.

CSC Australia Pty Ltd **has determined** that Cisco AnyConnect Secure Mobility Desktop Client version 4.1 upholds the claims made in the Security Target (Ref 1) and **has met** the requirements of version Protection Profile for IPsec Virtual Private Network (VPN) Clients version 1.4 dated 12 -10-2013.

4.3 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 the Australian Government Information Security Manual (Ref 4) and New Zealand Government users should consult the Government

Communication Security Bureau (GCSB) In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed, the ACA also recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
b) Configure and Operate the TOE according to the vendor's product administrator guidance
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
d) Ensure the VPN Gateway is not configured or operated in BYPASS mode.

Annex A – References and Abbreviations

A.1 References

1. Cisco AnyConnect Secure Mobility Desktop Client Security Target Version 1.0 16-09-2015

2. Guidance Documentation:

   - Cisco AnyConnect Secure Mobility Desktop Client CC Configuration Guide Version 1.0 09- 2015

3. Protection Profile for IPsec Virtual Private Network (VPN) Clients version 1.4 12-10- 2013

4. 2015 Australian Government Information Security Manual (ISM), Australian Signals Directorate

5. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-09-002

6. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-20012-09-003

7. Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-09-004.

8. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 02-07-2014.

9. Workbook Documents

   - Configuration Management (CMC) worksheet for Cisco AnyConnect, Reference CSC-EFC-T0082-WS-CMC 1.0

   - Vulnerability Analysis Evaluation (VAN) worksheet for Cisco AnyConnect,CSC-EFC-T0082-WS-NDPP_VAN 2.0

   - Operation User Guidance Evaluation (OPE) worksheet for Cisco AnyConnect, CSC-EFC-T0082-WS-VPNIC-OPE 2.0 Reference CSC-EFC-T0082-WS-OPE 2.0

   - Security Target Evaluation (ASE) worksheet for Cisco AnyConnect, Reference CSC-EFC-T0082-WS-VPNIC_ST 2.0

- Preparative Procedures Evaluation (PRE) worksheet for Cisco AnyConnect, CSC-EFC-T0082-WS-VPNIC-PRE 1.0

- Independent Testing Evaluation (IND) worksheet for Cisco AnyConnect, CSC-EFC-T0082-WS-VPNIC-IND 2.0

10. NIST publication SP800-90A Recommendations for Random Number Generation Using Deterministic Random Bit Generation, 01-2012.

11. Cisco AnyConnect Secure Mobility Desktop Client, Evaluation Technical Report (T0082), REFERENCE: CSC-EFC-T0082-ETR, Version 1.0 17-09-2015

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
ETR	Evaluation Technical Report
FOM	FIPS object module
FTP	File Transfer Protocol
GCSB	Government Communications Security Bureau
IPSec	Internet Protocol Security
NTP	Network Time Protocol
NDPP	US Government approved Protection Profile for Network Devices
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SNMP	Secure Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
VPN	Virtual Private network