National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Cisco Systems, Inc.

**170 West Tasman Dr.
San Jose, CA 95134**

AnyConnect Secure Mobility Client for Windows 10

Report Number:	**CCEVS-VR-VID10771-2017**
Dated:	**January 3, 2017**
Version:	**1.0**

**National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899**

**National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940**

ACKNOWLEDGEMENTS

Validation Team

Herbert Ellis
Kelly Hood
Ken Stutterheim
Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Tammy Compton
Chris Keenan
Khai Van
Katie Sykes
Gossamer Security Solutions
Catonsville, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco AnyConnect Secure Mobility Client for Windows 10 (IVPNCPP14) solution provided by Cisco Systems, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in December 2016. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013.

The Target of Evaluation (TOE) is the Cisco AnyConnect Secure Mobility Client for Windows 10.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory’s findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the *Cisco AnyConnect Secure Mobility Client for Windows 10 Security Target, Version 1.0, December 15, 2016* and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Cisco AnyConnect Secure Mobility Client for Windows 10
Protection Profile	Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013
ST:	Cisco AnyConnect Secure Mobility Client for Windows 10 Security Target, Version 1.0, December 15, 2016
Evaluation Technical Report	Evaluation Technical Report for Cisco AnyConnect Secure Mobility Client for Windows 10, Version 0.2, December 15, 2016
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Herbert Ellis Kelly Hood Ken Stutterheim Aerospace Corporation Columbia, MD

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The TOE is the core VPN component of the Cisco AnyConnect Secure Mobility Client for Windows 10. The Cisco AnyConnect Secure Mobility client is the 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 allows installed applications to communicate as though connected directly to the enterprise network.

The TOE is a software-only product that 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 organization’s private network, protecting data flows between a host and the Cisco 5500 Series Adaptive Security Appliance (ASA) VPN Gateway.

3.1 TOE Evaluated Configuration

The TOE is a VPN client application executing on a Microsoft Windows 10 platform. It requires one of the following Common Criteria certified Microsoft Windows 10 Operating System to run:

- Microsoft Windows 10 Home Edition (32-bit and 64-bit versions)
- Microsoft Windows 10 Pro Edition (32-bit and 64-bit versions)
- Microsoft Windows 10 Enterprise Edition (32-bit and 64-bit versions)

Refer to the Microsoft Windows 10 Security Target[1] certified on 2016-04-05 for information regarding the evaluated configuration requirements.

The TOE requires x86 Pentium class processor or greater and 100 MB available hard disk space.

3.2 Physical Boundaries

The TOE is a software-only VPN client application. The underlying platform on which the TOE resides is the Microsoft Windows operating system and is considered part of the IT environment.

The underlying platform provides some of the security functionality required in the VPNv1.4 Client PP, which is denoted with the phrase "TOE Platform" in the Security Target.

4 Security Policy

This section summarizes the security functionality of the TOE:

- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- Trusted path/channels

4.1 Cryptographic support

The TOE provides cryptography in support of IPsec with 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 and ESP protocols. The cryptographic algorithm implementation has been validated for CAVP conformance.

The TOE platform provides asymmetric cryptography, which is used by the TOE for IKE peer authentication using digital signature and hashing services. The TOE platform also provides a DRBG.

[1] http://www.commoncriteriaportal.org/products/

4.2 User data protection

The TOE platform ensures that residual information from previously sent network packets processed through the platform are protected from being passed into subsequent network packets.

4.3 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.

4.4 Security management

The TOE, TOE platform, and VPN Gateway provide the management functions to configure the security functionality provided by the TOE.

4.5 Protection of the TSF

The TOE performs a suite of self-tests during initial start-up to verify correct operation of its CAVP tested algorithms. Upon execution, the integrity of the TOEs software executables is also verified. The TOE Platform provides for verification of TOE software updates prior installation.

4.6 Trusted path/channels

The TOE's implementation of IPsec provides a trusted channel ensuring sensitive data is protected from unauthorized disclosure or modification when transmitted from the host to a VPN gateway.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013 (IVPNCPP14). That information has not been reproduced here and the IVPNCPP14 should be consulted if there is interest in that material.

6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the Protection Profile for IPsec Virtual Private Network (VPN) Clients and performed by the evaluation team).
2. This evaluation covers only the specific product version identified in this document, and not any earlier or later versions released or in process.
3. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines

an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

4. The functionality evaluated is scoped exclusively to the security functional requirements specified in the IVPNCPP14 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following documentation was used as evidence for the evaluation of the Cisco AnyConnect Secure Mobility Client for Windows 10:

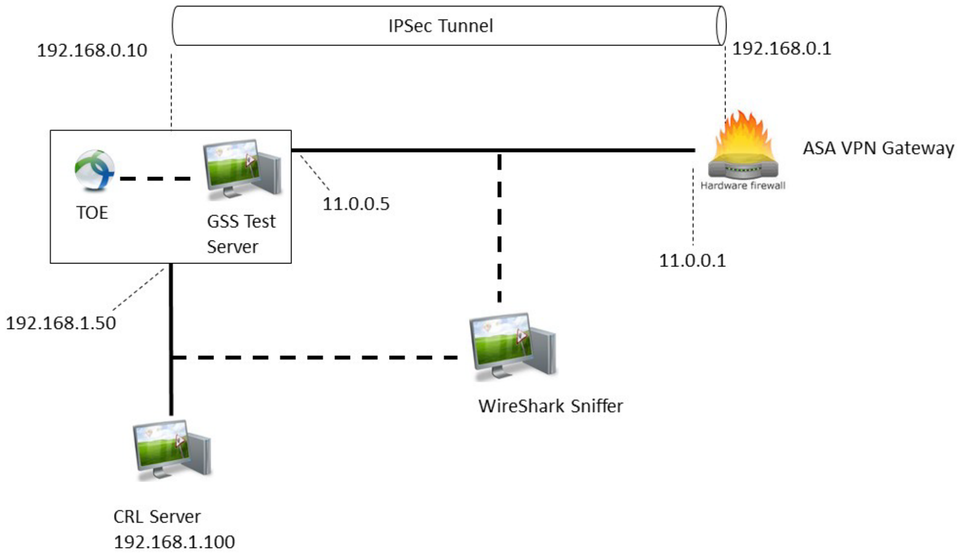
- Cisco AnyConnect Secure Mobility Client v4.3 for Windows 10 CC Configuration Guide, Version 1.0, September 2016

Any additional customer documentation delivered with the product or available through download was not included in the scope of the evaluation and hence should not be relied upon when using the products as evaluated.

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Detailed Test Report (IVPNCPP14) for AnyConnect Secure Mobility Client for Windows 10, Version 0.2, December 15, 2016, which is not publicly available. The *Assurance Activity Report (IVPNCPP14) for Cisco AnyConnect Secure Mobility Client for Windows 10, Version 0.4, 12/15/16 (*AAR*)*, provides a non-proprietary overview of testing and the prescribed assurance activities. A generalized depiction of the test

environment is below:



8.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the Cisco AnyConnect Secure Mobility Client v4.3 for Windows 10 CC Configuration Guide, Version 1.0, September 2016 document and ran the tests specified in the IVPNCPP14.

9 Evaluated Configuration

The evaluated configuration consists of the Cisco AnyConnect Secure Mobility Client for Windows 10 configured as specified in Cisco AnyConnect Secure Mobility Client v4.3 for Windows 10 CC Configuration Guide, Version 1.0, September 2016.

10 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Cisco AnyConnect Secure Mobility Client for Windows 10 TOE to be Part 2 extended, and to meet the SARs contained in the IVPNCPP14.

10.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco AnyConnect Secure Mobility Client for Windows 10 product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the IVPNCPP14 related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the IVPNCPP14 and recorded the results in a Test Report, summarized in the AAR.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (NVD) (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (VND) (http://www.kb.cert.org/vuls/) with the following search terms: "Cisco Anyconnect", "Anyconnect ", "Anyconnect 4.3", "ikev2" and "esp" .

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

10.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

11 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the TOE. The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the TOE, that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

The Cisco ASDM management platform, although required in the operational environment was not evaluated. Consumers should note that the evaluated environment is to make use of a Cisco ASA 5500 series VPN Gateway utilizing software 9.1 or later. Its use is required in the VPN Client configuration guidance provided by Cisco, and its configuration enforces the requirements for cryptographic algorithms. Note that the ASA 5500-x gateway product was not evaluated. Furthermore, note that the ASA requires that appropriate licenses be installed to permit the use of the AnyConnect IPsec VPN.

In the security target, readers may find a reference to the use of split-tunneling. Per the platform evaluation split tunneling is not allowed and the consumer is therefore cautioned that the use of split tunneling takes the product out of the evaluated configuration.

Astute readers may grasp that the platform versions may not be the latest versions of Windows. Therefore it is suggested that administrators take note of NIAP Policy 22, not only as it relates to the evaluated product, but as it relates to the underlying evaluated platform and required gateway.

12 Annexes

Not applicable.

13 Security Target

The ST for this product's evaluation is Cisco AnyConnect Secure Mobility Client for Windows 10 Security Target, Version 1.0, December 15, 2016.

14 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

15 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4] Protection Profile for IPsec Virtual Private Network (VPN) Clients, Version 1.4, 21 October 2013

[5] Cisco AnyConnect Secure Mobility Client for Windows 10 Security Target, Version 1.0, December 15, 2016 (ST)

[6] Assurance Activity Report (IVPNCPP14) for Cisco AnyConnect Secure Mobility Client for Windows 10, Version 0.4, 01/04/17 (AAR)

[7] Detailed Test Report (IVPNCPP14) for AnyConnect Secure Mobility Client for Windows 10, Version 0.2, 12/15/16 (DTR)