National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

Cisco Secure Client - AnyConnect 5.0 for Windows 10

Report Number: CCEVS-VR-VID11433-2023
Dated: December 19, 2023
Version: 1.0

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

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers
Meredith Martinez
The Aerospace Corporation

Common Criteria Testing Laboratory

Cody Cummins
Matai Spivey
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary 1
2 Identification 2
3 Architectural Information 3
3.1 TOE Description 3
3.2 TOE Evaluated Platforms 3
3.3 Physical Scope of the TOE 3
4 Security Policy 4
4.1 Cryptographic support 4
4.2 User data protection 5
4.3 Identification and authentication 5
4.4 Security management 5
4.5 Privacy 5
4.6 Protection of the TSF 5
4.7 Trusted channels 5
5 Assumptions & Clarification of Scope 5
6 Documentation 6
7 IT Product Testing 7
7.1 Developer Testing 7
7.2 Evaluation Team Independent Testing 7
8 Evaluated Configuration 7
8.1 Excluded Functionality 7
9 Results of the Evaluation 7
9.1 Evaluation of the Security Target (ASE) 8
9.2 Evaluation of the Development (ADV) 8
9.3 Evaluation of the Guidance Documents (AGD) 8
9.4 Evaluation of the Life Cycle Support Activities (ALC) 8
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) 9
9.6 Vulnerability Assessment Activity (VAN) 9
9.7 Summary of Evaluation Results 9
10 Validator Comments/Recommendations 10
11 Annexes 10
12 Security Target 10
13 Glossary 10
14 Bibliography 11

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Cisco Secure Client - AnyConnect 5.0 for Windows 10 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 Columbia, MD, United States of America, and was completed in December 2023. 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 PP-Configuration for Application Software and Virtual Private Network (VPN) Clients, Version 1.3, 07 April 2023 which includes the Base PP: Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14) with the PP-Module for Virtual Private Network (VPN) Clients, Version 2.4, 31 March 2022 (VPNC24).

The Target of Evaluation (TOE) is the Cisco Secure Client - AnyConnect 5.0 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 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). 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 Secure Client - AnyConnect 5.0 for Windows 10 Security Target, version 0.4, December 6, 2023 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 Secure Client - AnyConnect 5.0 for Windows 10 (Specific models identified in Section 8)
Protection Profile	PP-Configuration for Application Software and Virtual Private Network (VPN) Clients, Version 1.3, 07 April 2023 which includes the Base PP: Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14) with the PP-Module for Virtual Pr
ST	Cisco Secure Client - AnyConnect 5.0 for Windows 10 Security Target, version 0.4, December 6, 2023
Evaluation Technical Report	Evaluation Technical Report for Cisco Secure Client - AnyConnect 5.0 for Windows 10, version 0.2, December 11, 2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
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. Columbia, MD
CCEVS Validators	Jerome Myers, *The Aerospace Corporation* Meredith Martinez, *The Aerospace Corporation*

3 Architectural Information

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

The TOE is Cisco Secure Client - AnyConnect 5.0 for Windows 10 (herein after referred to as the VPN client, or the TOE). The TOE enables remote users within an organization to communicate securely as if their devices were directly connected to a private network.

The TOE is a VPN Client software application. A virtual private network (VPN) extends the organization's private network across a shared or public network. A VPN client establishes a IKEv2/IPsec connection to a VPN Gateway which allows the remote user to securely connect to the organization's private network.

3.1 TOE Description

This section provides an overview of the Target of Evaluation (TOE). The Cisco AnyConnect TOE is a client application that provides remote users a secure VPN tunnel to protect data in transit on both IPv4 and IPv6 networks. The TOE provides IPsec to authenticate and encrypt network traffic travelling across an unprotected public network. By protecting the communication from unauthorized disclosure or modification, remote users can securely connect to an organization's network resources and applications.

3.2 TOE Evaluated Platforms

As a software application, the evaluated configuration is Cisco Secure Client - AnyConnect 5.0 installed on Windows 10. Refer to the Common Criteria Administrator's Guide referenced in Section 6 for instructions on installing and configuring the TOE.

3.3 Physical Scope of the TOE

The TOE is a software-only VPN client application. The underlying Windows 10 platform on which the TOE resides is considered part of the IT environment. The following figure depicts a typical TOE installation and operating environment.

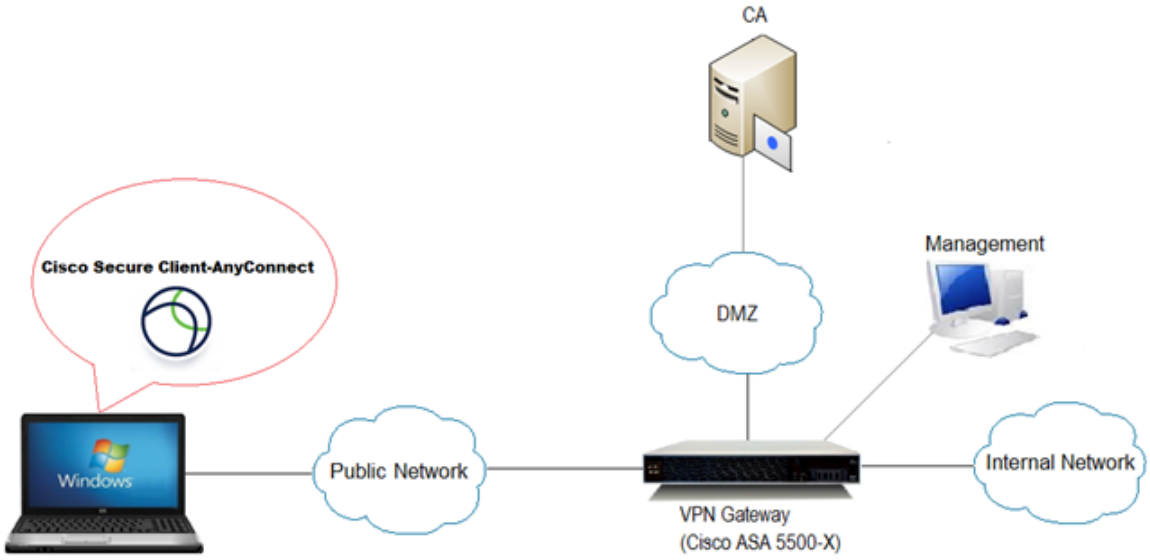

Figure 1: TOE and Environment

4 Security Policy

This section summaries the security functionality of the TOE:

1. Cryptographic support
2. User data protection
3. Identification and authentication
4. Security management
5. Privacy
6. Protection of the TSF
7. Trusted channels

4.1 Cryptographic support

The TOE incorporates a cryptographic module, CiscoSSL FIPS Object Module, to provide the 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 Elliptic-Curve Diffie-Hellman key exchange and the derivation function used in the IKEv2 and ESP protocols. The cryptographic algorithm implementation has been validated for CAVP conformance. See Table 15 in section 7 of the ST for certificate references.

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

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 successfully 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. The TOE provides a Security Administrator role and only the Security Administrator can perform the above security management functions.

4.5 Privacy

The TOE does not store or transmit Personally Identifiable Information (PII) over a network.

4.6 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 to installation.

4.7 Trusted 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 & Clarification of Scope

Assumptions
The Security Problem Definition, including the assumptions, may be found in the following documents:

- Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14)
- PP-Module for Virtual Private Network (VPN) Clients, Version 2.4, 31 March 2022 (VPNC24)

That information has not been reproduced here and the ASPP14/VPNC24 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the ASPP14/VPNC24 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

Clarification of scope

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

- 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 Application Software Protection Profile with the VPNC module and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific VPN client application models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- 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.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the ASPP14/VPNC24 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation. In particular, the security functionality mentioned in Section 8.1 of this report is explicitly excluded from the scope of this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- Cisco Secure Client - AnyConnect 5.0 for Windows 10 CC Configuration Guide, Version 0.3, December 6, 2023

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for Cisco Secure Client - AnyConnect 5.0 for Windows 10, Version 0.2, December 11, 2023 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the ASPP14/VPNC24 including the tests associated with optional requirements. The AAR, in section 3.4 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The evaluated configuration is Cisco Secure Client - AnyConnect 5.0 installed on the Windows 10 and configured in accordance with the documentation reference above in Section 6.

8.1 Excluded Functionality

The functionality listed below is not included in the evaluated configuration.

Function Excluded	Rationale
Non-FIPS mode of operation	This mode of operation includes non-FIPS allowed operations.
SSL Tunnel with DLTS tunneling options	[MOD_VPNC_V2.4] permits only an IPsec VPN tunnel.

9 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 5 and CEM version 3.1 rev 5. The evaluation determined the Cisco Secure Client - AnyConnect 5.0 for Windows 10 TOE to be Part 2 extended, and to meet the SARs contained in the ASPP14/VPNC24.

9.1 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 Secure Client - AnyConnect 5.0 for Windows 10 products 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.

9.2 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 ASPP14/VPNC24 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.

9.3 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.

9.4 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.

9.5 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 ASPP14/VPNC24 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.

9.6 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.

On 12/11/2023, the evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/vuln/search), Vulnerability Notes Database (http://www.kb.cert.org/vuls/), Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities), Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories), cve.org CVE Database (https://www.cve.org/), Tenable Network Security (http://nessus.org/plugins/index.php?view=search), Offensive Security Exploit Database (https://www.exploit-db.com/) with the following search terms: "anyconnect 5.0", "cisco anyconnect ikev2", "cisco anyconnect encapsulating security payload", "cisco anyconnect", "anyconnect windows 10", "rapidxml", "boost", "libcurl", "ciscossl", "cisco fom", "zlib", "intel core i5-1135g7".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.

9.7 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.

10 Validator Comments/Recommendations

All validator concerns and issues are adequately addressed in other parts of this document

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: Cisco Secure Client - AnyConnect 5.0 for Windows 10 Security Target, Version 0.4, December 6, 2023.

13 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.

14 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 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14).

[5] PP-Module for Virtual Private Network (VPN) Clients, Version 2.4, 31 March 2022 (VPNC24).

[6] Cisco Secure Client - AnyConnect 5.0 for Windows 10 Security Target, Version 0.4, December 6, 2023 (ST).

[7] Assurance Activity Report for Cisco Secure Client - AnyConnect 5.0 for Windows 10, Version 0.2, December 11, 2023 (AAR).

[8] Detailed Test Report for Cisco Secure Client - AnyConnect 5.0 for Windows 10, Version 0.2, December 11, 2023 (DTR).

[9] Evaluation Technical Report for Cisco Secure Client - AnyConnect 5.0 for Windows 10, Version 0.2, December 11, 2023 (ETR)