National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report
for
PP-Configuration for Application Software and Virtual Private Network Clients, Version 1.0

August 13, 2021

Report Number:	**CCEVS-VR-PP-0074**
Dated:	**23 January 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

Common Criteria Testing Laboratory
Base and Additional Requirements
Gossamer Security Solutions, Inc.
Columbia, 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 the PP-Configuration for Application Software and Virtual Private Network Clients (CFG_APP-VPNC_V1.0). This PP-Configuration defines how to evaluate a TOE that claims conformance to the Protection Profile for Application Software (PP_APP_V1.3) Base-PP and the PP-Module for Virtual Private Network (VPN) Clients, Version 2.3 (MOD_VPNC_V2.3). It presents a summary of the CFG_APP-VPNC_V1.0 and the evaluation results.

Gossamer Security Solutions, Inc., located in Columbia, Maryland, performed the evaluation of the PP_APP_V1.3 and MOD_VPNC_V2.3 contained within the PP-Configuration, concurrent with the first product evaluation against the PP-Configuration's requirements. The evaluated product was Cisco AnyConnect Secure Mobility Client v4.10 for Windows 10 (Cisco AnyConnect).

This evaluation addressed the base security functional requirements of MOD_VPNC_V2.3 as part of CFG_APP-VPNC_V1.0. The PP-Module defines additional requirements, some of which the Cisco AnyConnect devices evaluation claimed. The PP_APP_V1.3 Base-PP was previously validated to ensure compliance with Common Criteria requirements. The results of that evaluation were included in Validation Report Number CCEVS-VR-PP-0057, Version 1.3, dated 31 January 2020. The Validation Report (VR) author independently performed an additional review of the PP-Configuration and PP-Module as part of the completion of this VR, to confirm they meet the claimed ACE requirements.

The evaluation determined the CFG_APP-VPNC_V1.0 is both Common Criteria Part 2 Extended and Part 3 Extended. An accredited Information Technology Security Evaluation Facility (ITSEF) evaluated the PP-Configuration and PP-Module identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Release 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Revision 5). The Security Target (ST) includes material from both PP_APP_V1.3 and MOD_VPNC_V2.3; completion of the ASE work units satisfied the ACE work units for this PP-Module, but only for the materials defined in this PP-Module, and only when the PP-Module is in the defined PP-Configuration.

The evaluation laboratory conducted this evaluation in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence given.

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 CCTLs. CCTLs evaluate products against Protection Profiles (PPs) and PP-Modules that have Evaluation Activities, which are interpretations of the Common Methodology for Information Technology Security Evaluation (CEM) v3.1 work units specific to the technology described by the PP or PP-Module. Products may only be evaluated against PP-Modules when a PP-Configuration is defined to include the PP-Module with at least one corresponding Base-PP.

In order to promote thoroughness and efficiency, the evaluation of the CFG_APP-VPNC_V1.0 and MOD_VPNC_V2.3 was performed concurrent with the first product evaluation to claim conformance to the PP-Configuration. In this case, the Target of Evaluation (TOE) was Cisco AnyConnect Secure Mobility Client v4.10 for Windows 10, performed by Gossamer Security Solutions, Inc. in Columbia, MD.

This evaluation addressed the base security functional requirements of MOD_VPNC_V2.3 as part of CFG_APP-VPNC_V1.0. The PP-Module defines additional requirements, some of which the Cisco AnyConnect evaluation claimed.

MOD_VPNC_V2.3 contains a set of base requirements that all conformant STs must include, and additionally contains optional and selection-based requirements. Optional requirements fall into three categories:

- Strictly optional requirements may be claimed at the vendor’s discretion, and do not need to be claimed if the TOE does not support the functionality described by the requirements.
- Implementation-dependent requirements must be claimed if the TOE implements a particular capability, but do not need to be claimed if that capability is not implemented.
- Objective requirements are the same as strictly optional requirements except that they are under consideration to become mandatory requirements in future iterations of the standard, so product developers should be considering how to update their products in the future to conform to them if they do become required.

Selection-based requirements are those that must be included based upon the selections made in other requirements and the capabilities of the TOE.

The VR authors evaluated all discretionary requirements not claimed in the initial TOE evaluation as part of the evaluation of the ACE_REQ work units performed against the PP-Module. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include reference to this as additional evidence that the corresponding portions of the CFG_APP-VPNC_V1.0 were evaluated.

The following identifies the PP-Module in the PP-Configuration evaluated by this VR. It also includes supporting information from the initial product evaluation performed against this PP-Module.

PP-Configuration	PP-Configuration for Application Software and Virtual Private Network Clients, Version 1.0, 2021-08-13
Base-PP	Protection Profile for Application Software, Version 1.3, 2019-03-01 (PP_APP_V1.3)

Module(s) in PP-Configuration	PP-Module for Virtual Private Network (VPN) Clients, Version 2.3, 10 August 2021 (CFG_VPNC_V2.3)
ST (Base)	Cisco AnyConnect Secure Mobility Client v4.10 for Windows 10 Security Target, Version 0.4, December 6, 2021
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL	Gossamer Security Solutions, Inc. Columbia, MD

3 CFG_APP-VPNC_V1.0 Description

CFG_APP-VPNC_V1.0 is a PP-Configuration that combines the following:

- Protection Profile for Application Software, Version 1.3 (PP_APP_V1.3)
- PP-Module for Virtual Private Network (VPN) Clients, Version 2.3 (MOD_VPNC_V2.3)

This PP-Configuration defines a conformant TOE as a software application that provides VPN client capability. The PP and PP-Module that the PP-Configuration contains define the security boundary for software applications and VPN clients, respectively.

A VPN Client is a piece of software that allows a computer to establish a VPN with a remote peer or gateway. The VPN allows for confidentiality and integrity of the network traffic that passes over it. Different protocols can be used to implement VPNs, but MOD_VPNC_V2.3 defines IPsec as the specific mechanism it requires to implement a VPN. CFG_APP-VPNC_V1.0 specifically refers to VPN Clients that are packaged as third-party software applications that can run on a general-purpose computer, rather than being bundled as an integrated part of a desktop or mobile operating system.

4 Security Problem Description and Objectives

4.1 Assumptions

Table 1 shows the assumptions defined in the individual components of CFG_APP-VPNC_V1.0.

Table 1: Assumptions

Assumption Name	Assumption Definition
From PP_APP_V1.3	
A.PLATFORM	The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.
From MOD_VPNC_V2.3	
A.NO_TOE_BYPASS	Information cannot flow onto the network to which the VPN client's host is connected without passing through the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

4.2 Threats

Table 2 shows the threats defined in the individual components of CFG_APP-VPNC_V1.0.

Table 2: Threats

Threat Name	Threat Definition
From PP_APP_V1.3	
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.
From MOD_VPNC_V2.3	
T.TSF_CONFIGURATION	Configuring VPN tunnels is a complex and time-consuming process, and prone to errors if the interface for doing so is not well-specified or well-behaved. The inability to configure certain aspects of the interface may also lead to the mis-specification of the desired

Threat Name	Threat Definition
	communications policy or use of cryptography that may be desired or required for a particular site. This may result in unintended weak or plaintext communications while the user thinks that their data are being protected. Other aspects of configuring the TOE or using its security mechanisms (for example, the update process) may also result in a reduction in the trustworthiness of the VPN client.
T.TSF_FAILURE	Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise of the TSF.
T.UNAUTHORIZED_ACCESS	This PP-Module does not include requirements that can protect against an insider threat. Authorized users are not considered hostile or malicious and are trusted to follow appropriate guidance. Only authorized personnel should have access to the system or device that contains the IPsec VPN client. Therefore, the primary threat agents are the unauthorized entities that try to gain access to the protected network (in cases where tunnel mode is used) or to plaintext data that traverses the public network (regardless of whether transport mode or tunnel mode is used). The endpoint of the network communication can be both geographically and logically distant from the TOE, and can pass through a variety of other systems. These intermediate systems may be under the control of the adversary, and offer an opportunity for communications over the network to be compromised. Plaintext communication over the network may allow critical data (such as passwords, configuration settings, and user data) to be read and/or manipulated directly by intermediate systems, leading to a compromise of the TOE or to the secured environmental system(s) that the TOE is being used to facilitate communications with. IPsec can be used to provide protection for this communication; however, there are myriad options that can be implemented for the protocol to be compliant to the protocol specification listed in the RFC. Some of these options can have negative impacts on the security of the connection. For instance, using a weak encryption algorithm (even one that is allowed by the RFC, such as DES) can allow an adversary to read and even manipulate the data on the encrypted channel, thus circumventing countermeasures in place to prevent such attacks. Further, if the protocol is implemented with little-used or non-standard options, it may be compliant with the protocol specification but will not be able to interact with other, diverse equipment that is typically found in large enterprises. Even though the communication path is protected, there is a possibility that the IPsec peer could be duped into thinking that a malicious third-party user or system is the TOE. For instance, a middleman could intercept a connection request to the TOE, and respond to the request as if it were the TOE. In a similar manner, the TOE could also be duped into thinking that it is establishing communications with a legitimate IPsec peer when in fact it is not. An attacker could also mount a malicious man-in-the-middle-type of attack, in which an intermediate system is compromised, and the traffic is proxied, examined, and modified by this system. This attack can even be mounted via

Threat Name	Threat Definition
	encrypted communication channels if appropriate countermeasures are not applied. These attacks are, in part, enabled by a malicious attacker capturing network traffic (for instance, an authentication session) and "playing back" that traffic in order to fool an endpoint into thinking it was communicating with a legitimate remote entity.
T.USER_DATA_REUSE	Data traversing the TOE could inadvertently be sent to a different user; since these data may be sensitive, this may cause a compromise that is unacceptable. The specific threat that must be addressed concerns user data that is retained by the TOE in the course of processing network traffic that could be inadvertently re-used in sending network traffic to a user other than that intended by the sender of the original network traffic.

4.3 Organizational Security Policies

Table 3 shows the organizational security policies defined in the individual components of CFG_APP-VPNC_V1.0.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
From PP_APP_V1.3	
No OSPs defined in PP_APP_V1.3.	
From MOD_VPNC_V2.3	
No OSPs defined in MOD_VPNC_V2.3.	

4.4 Security Objectives

Table 4 shows the security objectives for the TOE defined in the individual components of CFG_APP-VPNC_V1.0.

Table 4: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
From PP_APP_V1.3	
O.INTEGRITY	Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom, if ever, shipped without errors. The ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options.
O.QUALITY	To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex

TOE Security Objective	TOE Security Objective Definition
	operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs.
O.MANAGEMENT	To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII.
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data.
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application.
From MOD_VPNC_V2.3	
O.AUTHENTICATION	To address the issues associated with unauthorized disclosure of information in transit, a compliant TOE's authentication ability (IPsec) will allow the TSF to establish VPN connectivity with a remote VPN gateway or peer and ensure that any such connection attempt is both authenticated and authorized. This objective also ensures the protection of data in transit by ensuring that interfaces exist for non-TOE entities to invoke the TSF to establish an IPsec channel.
O.CRYPTOGRAPHIC_FUNCTIONS	To address the issues associated with unauthorized disclosure of information in transit, a compliant TOE will implement cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE.
O.KNOWN_STATE	The TOE will provide sufficient measures to ensure it is operating in a known state. At minimum this includes management functionality to allow the security functionality to be configured and self-test functionality that allows it to assert its own integrity. It may also include auditing functionality that can be used to determine the operational behavior of the TOE.
O.NONDISCLOSURE	To address the issues associated with unauthorized disclosure of information at rest, a compliant TOE will ensure that non-persistent data is purged when no longer needed. The TSF may also implement measures to protect against the disclosure of stored cryptographic keys and data through implementation of protected storage and secure erasure methods. The TOE may optionally also enforce split-tunneling prevention to ensure that data in transit cannot be disclosed inadvertently outside of the IPsec tunnel.

Table 5 shows the security objectives for the Operational Environment defined in the individual components of CFG_APP-VPNC_V1.0.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
From PP_APP_V1.3	
OE.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
OE.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.
OE.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.
From MOD_VPNC_V2.3	
OE.NO_TOE_BYPASS	Information cannot flow onto the network to which the VPN client's host is connected without passing through the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
OE.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

5 Functional Requirements

As indicated above, CFG_APP-VPNC_V1.0 includes both PP_APP_V1.3 and MOD_VPNC_V2.3. The functional requirements from PP_APP_V1.3 were evaluated separately so this section applies only to requirements of MOD_VPNC_V2.3.

Requirements in the MOD_VPNC_V2.3 are comprised of the "base" requirements and additional requirements that are dependent on the Base-PP that the PP-Module is used with. The following table contains the "base" requirements that were validated as part of the Cisco AnyConnect evaluation activities referenced above as well as the additional requirements that depend on the Base-PP that is claimed. In the case of the Cisco AnyConnect evaluation, only those that apply when PP_APP_V1.3 is the Base-PP were claimed by the TOE; those associated with other Base-PPs did not apply and have been evaluated through evaluation of the PP-Module work units.

Table 6: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
Applicable when the Protection Profile for General Purpose Operating Systems is the Base-PP		
FCS: Cryptographic Support	FCS_CKM_EXT.2: Cryptographic Key Storage	PP-Module Evaluation
FIA: Identification and Authentication	FIA_X509_EXT.3: X.509 Certificate Authentication	PP-Module Evaluation
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF Trusted Channel	PP-Module Evaluation
Applicable when the Protection Profile for Mobile Device Fundamentals is the Base-PP		
No additional SFRs when the MDF PP is the Base-PP.		
Applicable when the Protection Profile for Application Software is the Base-PP		
FCS: Cryptographic Support	FCS_CKM_EXT.2: Cryptographic Key Storage	PP-Module Evaluation
	FCS_CKM_EXT.4: Cryptographic Key Destruction	PP-Module Evaluation
Applicable when the Protection Profile for Mobile Device Management is the Base-PP		
No additional SFRs when the MDM PP is the Base-PP.		
Applicable to all TOEs		
FCS: Cryptographic Support	FCS_CKM.1/VPN: Cryptographic Key Generation (IKE)	Cisco AnyConnect Secure Mobility Client v4.10 for Windows 10
	FCS_IPSEC_EXT.1: IPsec	Cisco AnyConnect Secure Mobility Client v4.10 for Windows 10
FDP: User Data Protection	FDP_RIP.2: Full Residual Information Protection	Cisco AnyConnect Secure Mobility Client v4.10 for Windows 10
FMT: Security Management	FMT_SMF.1/VPN: Specification of Management Functions (VPN)	Cisco AnyConnect Secure Mobility Client v4.10 for Windows 10
FPT: Protection of the TSF	FPT_TST_EXT.1: TSF Self-Test (VPN Client)	Cisco AnyConnect Secure Mobility Client v4.10 for Windows 10

The following table contains the "**Optional**" requirements contained in Appendix A, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given optional requirement, the VR author has evaluated it through the completion of the relevant ACE work units and has indicated its verification through "Module Evaluation."

Table 7: Optional Requirements

Requirement Class	Requirement Component	Verified By
Strictly Optional Requirements		
The MOD_VPNC_V2.3 does not define any strictly optional requirements.		
Objective Requirements		
FAU: Security Audit	FAU_GEN.1/VPN: Audit Data Generation (VPN Client)	PP-Module Evaluation
	FAU_SEL.1/VPN: Selective Audit (VPN Client)	PP-Module Evaluation
Implementation-Dependent Requirements		
FDP: User Data Protection	FDP_IFC_EXT.1/VPN: Subset Information Flow Control (VPN)	PP-Module Evaluation

The following table contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant ACE work units and has indicated its verification through "Module Evaluation."

Table 8: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
FIA: Identification and Authentication	FIA_PSK_EXT.1: Pre-Shared Key Composition	PP-Module Evaluation

6 Assurance Requirements

The PP-Configuration defines its security assurance requirements as those required by PP_APP_V1.3. The SARs defined in that PP are applicable to MOD_VPNC_V2.3 as well as CFG_APP-VPNC_V1.0 as a whole.

7 Results of the Evaluation

Note that for ACE elements and work units identical to ASE elements and work units, the lab performed the ACE work units concurrent to the ASE work units.

Table 10: Evaluation Results

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	Module evaluation
ACE_CCL.1	Pass	Module evaluation
ACE_SPD.1	Pass	Module evaluation
ACE_OBJ.1	Pass	Module evaluation
ACE_ECD.1	Pass	Module evaluation
ACE_REQ.1	Pass	Module evaluation
ACE_MCO.1	Pass	Module evaluation
ACE_CCO.1	Pass	Module evaluation

8 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 unambiguously that a given implementation is correct with respect to the formal model.
- **Evaluation**. An IT product's assessment against the Common Criteria using the Common Criteria Evaluation Methodology as the supplemental guidance, interprets it in the MOD_VPNC_V2.3 Evaluation Activities to determine whether the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **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 the CCEVS Validation Body uses that leads to the issuance 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.

9 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, dated: April 2017.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

[5] PP-Module for Virtual Private Network (VPN) Clients, Version 2.3, 10 August 2021

[6] Protection Profile for Application Software, Version 1.3, 01 March 2019

[7] PP-Configuration for Application Software and Virtual Private Network (VPN) Clients, Version 1.0, 13 August 2021.

[8] Cisco AnyConnect Secure Mobility Client v4.10 for Android 11 Security Target, Version 0.7, 06 December 2021