National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Cisco 1000V Cloud Services Router VPN Client

Report Number: CCEVS-VR-10719-2016
Dated: November 23, 2016
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

Jerome Myers
Meredith Hennan
Robert Heald

Common Criteria Testing Laboratory

Kevin Micciche
Madelyn Lanoue

CGI IT Security Labs

Table of Contents

List of Tables

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should read carefully the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of Cisco 1000V Cloud Services Router VPN Client (hereafter referenced as Cisco CSR 1000V). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of Cisco 1000V was performed by CGI IT Security Labs in Manassas, Virginia, in the United States and was completed in November 2016. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in Protection Profile for IPsec VPN Client, Version 1.4. The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The CGI ITSL evaluation team determined that Cisco CSR 1000V is conformant to the claimed Protection Profiles (PPs) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST.

The Cisco 1000V Cloud Services Router TOE is a software-only virtual form factor router that securely connects distributed sites within an organization.

Table 1: Platform Models in the Evaluated Configuration

Platform Model	Hypervisor	Processor
Cisco EN120E 208	VMware ESXi 5.5	Intel Atom
Cisco EN120S M2	VMware ESXi 5.5	Intel Xeon

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the 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.

Table 2: Evaluation Details

Item	Identifier
Evaluated Product	Cisco 1000V Cloud Services Router VPN Client
PP	Protection Profile for IPsec VPN Client, Version 1.4
ST	Cisco 1000V Cloud Services Router VPN Client, Version 1.0, November 23, 2016
ETR	Evaluation Technical Report for Cisco Cloud Services Router 1000V XE 3.16 Common Criteria IPSec VPN Client PP 1.4, version 1.0, August 30, 2016
Sponsor & Developer	Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134
CCTL	CGI IT Security Labs 9700 Capital Court Manassas, VA 20110
Completion Date	November 23, 2016
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
Disclaimer	The information contained in this Validation Report is not an endorsement of the Cisco CSR 1000V by any agency of the U.S. Government and no warranty is either expressed or implied.
Evaluation Personnel	Kevin Micciche Madelyn Lanoue
Validation Personnel	Jerome Myers Meredith Hennan Robert Heald

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) 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 Product Compliant List (PCL).

The following table identifies the evaluated Security Target and TOE.

Table 3: ST and TOE Identification

Name	Description
ST Title	Cisco 1000V Cloud Services Router VPN Client
ST Version	1.0
Publication Date	November 23, 2016
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco 1000V Cloud Services Router
TOE Hardware Models	Cisco CSR 1000V
TOE Software Version	IOS XE 3.16
Keywords	VPN Client

3 Architectural Information

The TOE is the VPN component of the Cisco 1000V Cloud Services Router, version 3.16. The TOE provides IPsec VPN tunnel to authenticate and encrypt network traffic travelling across an unprotected public network protecting an organization's network communication from unauthorized disclosure or modification. The TOE allows an organization to securely connect a remote site to a headend site.

The following figure provides a simplified visual depiction of an example TOE deployment. The boundary is surrounded with a hashed red line.

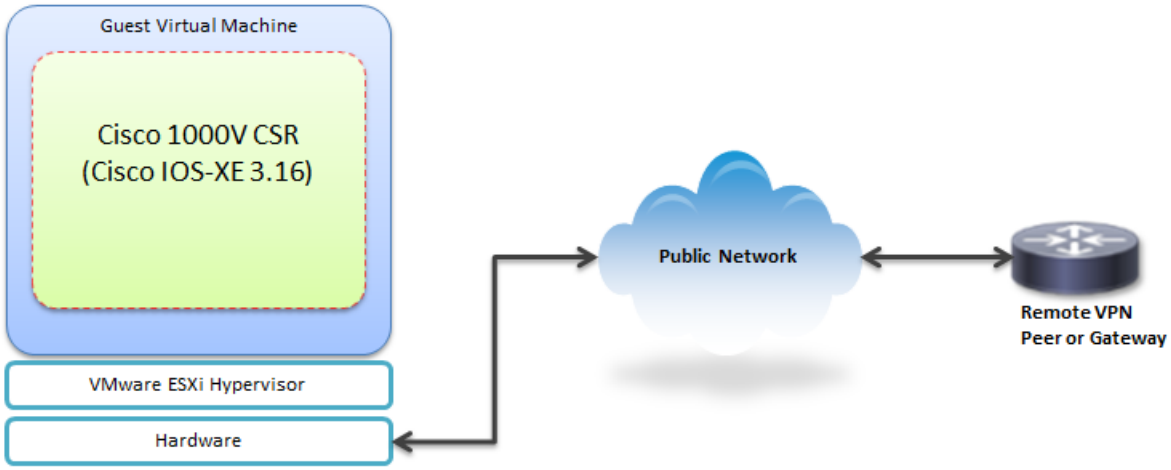


Figure 1: TOE Deployment Example

The underlying platform on which the TOE resides is the guest virtual machine and VMware ESXi Hypervisor. The Guest VM contains the virtualized hardware environment on which the TOE executes. The guest virtual machine, VMware ESXi Hypervisor, and physical hardware are considered part of the IT environment.

4 Assumptions, Threats, and Scope

4.1 Assumptions

The ST identifies the following assumptions about the use of the product:

Table 4: Assumptions

Assumption	Assumption Definition
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

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

Table 5: Threats

Threat	Threat Definition
T.TSF_CONFIGURATION	Failure to allow configuration of the TSF may prevent its users from being able to adequately implement their particular security policy, leading to a compromise of user information.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender because it is not rendered inaccessible after it is done being used.

4.3 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 claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation.

4. 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.

5 Security Policy

The TOE enforces the following security policies as described in the ST.

5.1 Cryptographic Support

The TOE provides cryptography in support of:

- Symmetric cryptography for bulk AES encryption/decryption
- Diffie-Hellman key exchange
- DRBG
- Asymmetric cryptography for digital signatures (RSA/ECDSA), hashing, and HMAC services
- Asymmetric cryptography for IKE peer authentication using X.509 digital certificates

The cryptographic algorithm implementation has been validated for CAVP conformance.

5.2 Identification and Authentication

The TOE performs device-level authentication of the remote device (IPsec peers or VPN Gateway). Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec mutual authentication. The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec sessions.

5.3 Security Management

The TOE provides all the capabilities necessary to securely manage the TOE. The administrative user can connect to the TOE using the CLI to perform these functions via IPsec, SSH, a terminal server, or at the local console. Refer to the Guidance documentation for configuration syntax, commands, and information related to each of these functions. All of these functions can be performed via the CLI either locally or remotely.

5.4 Protection of the TSF

The TOE runs a suite of self-tests during initial start-up to verify correct operation of cryptographic modules. If any of the tests fail, the Authorized Administrator will have to log into the CLI to determine which test failed and why. If the tests pass successfully the POST event logs will show successful for each test. During the system boot process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the software component.

The TOE has specific versions that can be queried by an administrator. When updates are made available by Cisco, an administrator can obtain and install those updates. The updates can be downloaded from the Cisco.com web site. Authorized Administrators can download the Common Criteria evaluated software image file from Cisco.com onto a trusted computer system for usage in the trusted update functionality. Software images are available from Cisco.com at the following: http://www.cisco.com/cisco/software/navigator.html

When a replacement image is installed on the TOE, the digital signature will be validated and the image will be successfully installed. When an invalid image is attempted to be installed, the administrator, after loading the image onto the device, needs to perform a verify operation to confirm if it is valid. The TOE will identify if the image is valid or not, and then the administrator will manually reject a bad image and does not proceed with the installation.

5.5 Trusted Path/Channels

The TOE implements IPsec to protect communications with peer devices.

5.6 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.

6 Documentation

Cisco offers a number of guidance documents along with a CC-specific supplemental document describing the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features.

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- Cisco 1000V Cloud Services Router with Cisco IOS XE Software Release 3.16 Common Criteria Configuration Guide, Version 1.0, October 6, 2016

This document in turn references the following documents that provide additional detailed guidance for specific TOE capabilities. Note that the evaluation examined these referenced documents only to the extent necessary to complete the assurance activities specified in the claimed PPs.

Table 6: Supporting TOE Guidance Documentation

#	Title	Link
[1]	Cisco CSR 1000V Series Cloud Services Router Software Configuration Guide	http://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/csr1000Vswcfg.html
[2]	Cisco CSR 1000V Series Cloud Services Router Release Notes	http://www.cisco.com/c/en/us/td/docs/routers/csr1000/release/notes/csr1000v_3Srn.html
[3]	Configuration Fundamentals Configuration Guide Cisco IOS XE Release 3S	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/xe-3s/fundamentals-xe-3s-book.html
[4]	Loading and Managing System Images Configuration Guide, Cisco IOS XE Release 3S	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sys-image-mgmt/configuration/xe-3s/sysimgmgmt-xe-3s-book.html
[5]	Managing Configuration Files Configuration Guide, Cisco IOS XE Release 3S	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/config-mgmt/configuration/xe-3s/config-mgmt-xe-3s-book.html
[6]	The Integrated File System Configuration Guide, Cisco IOS XE Release 3S	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ifs/configuration/xe-3s/ifs-xe-3s-book.html
[7]	Public Key Infrastructure Configuration Guide, Cisco IOS XE Release 3S	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-3s/sec-pki-xe-3s-book.html
[8]	Security for VPNs with IPsec Configuration Guide, Cisco IOS XE Release 3S	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/xe-3s/sec-sec-for-vpns-w-IPsec-xe-3s-book.html
[9]	Configuring Internet Key Exchange Version 2	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-3s/asr1000/sec-flex-vpn-xe-3s-asr1000-book/sec-cfg-ikev2-flex.html
[10]	Internet Key Exchange for IPsec VPNs Configuration Guide, Cisco IOS XE Release 3S	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ikevpn/configuration/xe-3s/sec-ike-for-IPsec-vpns-xe-3s-book.html
[11]	Cisco IOS Security Command Reference: Commands A to C	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book.html
[12]	Cisco IOS Security Command Reference: Commands D to L	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/d1/sec-d1-cr-book.html
[13]	Cisco IOS Security Command Reference: Commands M to R	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/m1/sec-m1-cr-book.html

#	Title	Link
[14]	Cisco IOS Security Command Reference: Commands S to Z	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-cr-book.html

The above documents are considered to be part of the evaluated TOE. Any additional customer documentation delivered with the TOE or made available through electronic downloads should not be relied upon for using the TOE in its evaluated configuration.

The Security Target used is:

- Cisco 1000V Cloud Services Router VPN Client Security Target

7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following:

- Independent Test Plan for Cisco 1000V Cloud Services Router VPN Client, Version 1.2, October 20, 2016

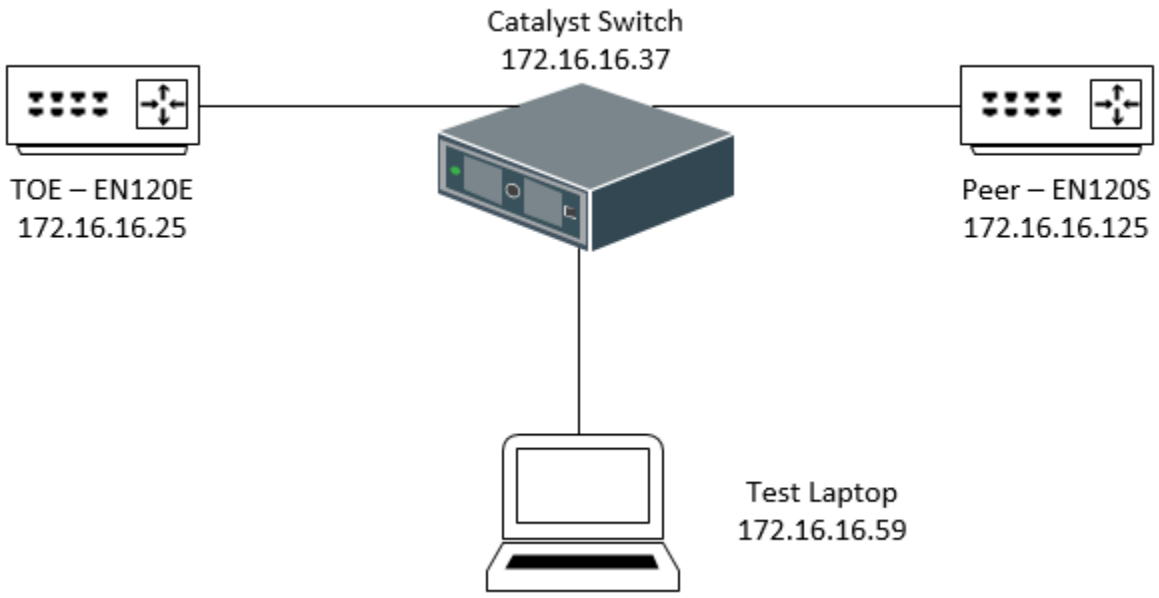
A non-proprietary version of the tests performed and samples of the evidence that was generated is summarized in the following document:

- Assurance Activities Report for Cisco 1000V Cloud Services Router VPN Client XE 3.16, Version 1.4, November 23, 2016

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to the Protection Profile for IPsec VPN Client 1.4. Independent testing took place at the CGI ITSL location in Manassas, Virginia.

The following depicts a diagram of the test environment with a list of tools used by the evaluators:

Figure 1: Cisco Systems TOE environment setup



Cisco CSR #1 (TOE)	
Model:	Cisco ISR 2911 with UCS-EN120E (Intel Atom)
OS:	Cisco IOS 3.16
IPv4:	172.16.16.25

Cisco CSR #2 (TOE/Peer)	
Model:	Cisco ISR 4351 with UCS-EN120S (Intel Xeon)
OS:	Cisco IOS XE 3.16

IPv4:	172.16.16.125

Cisco Catalyst Switch	
Model:	Cisco Catalyst Switch 3750X
OS:	Cisco IOS 15.0(2) SE4
IPv4:	172.16.16.37

Testing Workstation
IP: 172.16.16.59
Tools: • Windows 10 64-bit • OpenSSL 1.0.2 • Putty 0.67 • Cygwin 2.4.0 • Syslog Watcher Version 4.8.5

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for the *Protection Profile for IPsec Virtual Private Network (VPN) Clients*, version 1.4 have been fulfilled.

8 Evaluated Configuration

The evaluated version of the TOE is running IOS XE 3.16, as installed and configured according to the CC Configuration Guide as well as the supporting guidance documentation identified in Table 6.

The TOE evaluated configuration requires the following:

- VMware ESXi 5.0, 5.1, 5.5, or 6.0 Hypervisor
- A single Guest Virtual Machine supporting:
    - Single hard disk
    - 8 GB virtual disk
    - The following virtual CPU configurations are supported:
        - 1 virtual CPU, requiring 4 GB minimum of RAM
        - 2 virtual CPUs, requiring 4 GB minimum of RAM
        - 4 virtual CPUs, requiring 4 GB minimum of RAM
        - 8 virtual CPUs, requiring 4 GB minimum of RAM
    - 2 or more virtual network interface cards
- Remote VPN peer or gateway

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in Protection Profile for IPsec VPN Client, Version 1.4, in conjunction with version 3.1, revision 4 of the CC and the CEM.

Examinations were performed on the Security Target, Development documentation, Test Documentation, and Guidance documentation. The validation team also performed an assessment on the evaluation lab's Assurance Activities Report.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the CGI CCTL.

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 1000V CSR VPN Client 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 PP 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 PP 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 proprietary Penetration Test Report prepared by the evaluator, and summarized in the AAR. Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluation team found no vulnerabilities were applicable to the TOE version or hardware. The list of keywords searched include:

- Cisco CSR
- Cloud Services Router
- CSR 1000V
- VMware ESXi Hypervisor
- IOS XE 3.16
- IC2Mv
- IC2M
- Cisco IPsec

The evaluation lab examined each result provided from NVD and Exploit Search to determine if the current TOE version or component within the environment was vulnerable. Based upon the analysis, any issues found that were generated were patched in the TOE version and prior versions, mitigating the risk factor.

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

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 Cisco 1000V Cloud Services Router, to include the routing functionality and other features of Cisco IOS-XE that are outside the scope of IPsec, are not covered by this evaluation, need to be assessed separately, and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

Cisco 1000V Cloud Services Router 1000V, Version 1.0, November 23, 2016

13 Abbreviations and Acronyms

AAA	Authentication, Authorization and Accounting
AAR	Assurance Activities Report
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	CC Testing Laboratory
CEM	Common Methodology for IT Security Evaluation
CLI	Command Line Interface
EP	Extended Package
ESP	Encapsulating Security Payload
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
IKE	Internet Key Exchange
IOS	Inter-network Operating System
IPsec	Internet Protocol security
ISR	Integrated Service Router
IT	Information Technology
LAN	Local Area Network
NDPP	Network Device Protection Profile
NIAP	National Information Assurance Partnership
NIM	Network Interface Module
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PCL	Product Compliant List
PP	Protection Profile
RFC	Request For Comment
SA	Security Association
SAR	Security Assurance Requirement
SFP	Small Form-factor Pluggable
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification
VPN	Virtual Private Network
VR	Validation Report

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, Version 3.1, Revision 4, September 2012.

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

[5] Cisco 1000V Cloud Services Router VPN Client Security Target, version 1.0, November 23, 2016

[6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[7] Evaluation Technical Report for Cisco Cloud Services Router 1000V XE 3.16 Common Criteria IPSec VPN Client PP 1.4, version 1.0, August 30, 2016.

[8] Assurance Activities Report for Cisco 1000V Cloud Services Router VPN Client XE 3.16, Version 1.4, November 23, 2016