Indian CC Certification Scheme (IC3S)

Certification Report

Report Number	:	**IC3S/MUM01/CISCO/cPP/0119/0016/CR**
Product / system	:	**Cisco ASR900 Series and NCS4200 Series running IOS-XE 16.9**

Dated: 3rd Dec 2019

Version: 1.0

Government of India
Ministry of Electronics & Information Technology
Standardization, Testing and Quality Certification Directorate
6. CGO Complex, Lodi Road, New Delhi – 110003
India

This report contains a total of 14 pages. In case it needs to be reproduced, all the pages must be included.

Product developer: Cisco Systems, Inc. 170 West Tasman Dr.
San Jose, CA 95134-1706 USA

TOE evaluation sponsored by: Cisco Systems, Inc. 170 West Tasman Dr.
San Jose, CA 95134-1706 USA

Evaluation facility: Acucert Labs LLP, D-509 Neelkanth Business Park Vidyavihar
West, Mumbai 400086, India

Evaluation Personnel: Rupal Gupta, Kamlesh Ahuja and Shaunak Shah

Evaluation report: Evaluation Technical Report for a Target of Evaluation
Version 1.0 November 21, 2019

Validation Personnel: Subhendu Das, Scientist G

Table of Contents

Contents

PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY

A.1 Certification Statement

The product below has been evaluated under the terms of the Indian Common Criteria Certification Scheme (IC3S) and has met the stated Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor	Cisco Systems, Inc. 170 West Tasman Dr. San Jose, CA 95134-1706 USA
Developer	Cisco Systems, Inc. 170 West Tasman Dr. San Jose, CA 95134-1706 USA
The Target of Evaluation (TOE)	Cisco ASR 900 Series and NCS4200 Series running IOS-XE 16.9. ASR902, ASR903, ASR907, ASR920 and NCS4201, NCS4202, NCS4206, NCS4216. The ASR900 Series and NCS4200 Series that comprises the TOE has common hardware characteristics. These characteristics affect only non-TSF relevant functions of the platforms (such as throughput and amount of storage) and therefore support security equivalency of the platforms in terms of hardware.
Security Target	Cisco ASR900 Series and NCS4200 Series Switches running IOS-XE 16.9 ST Version 1.0, October 11, 2019
Brief description of product	The Cisco ASR900 Series and NCS4200 Series running with IOS-XE 16.9 are single-device security, routing and switching solutions for protecting the network. In support of their routing capabilities, both these devices provide IPsec connection capabilities to facilitate secure communications with external entities, as required and also provide VPN functionality The TOE is intended for simplified management to small businesses as well as metro and enterprise size business, service providers and carriers.
CC Part 2 [CC-II]	Conformant
CC Part 3 [CC-III]	Conformant
EAL/ PP	NDcPP , ver. 2.1 AND VPNGWEP ver. 2.1
Evaluation Lab	Acucert Labs LLP , D-509 Neelkanth Business Park Vidyavihar West, Mumbai 400086, India
Date Authorized	5/4/2019 (IC3S/CB/2019/0001 dt 5/4/2019)

A.2 About the Certification Body

STQC IT Certification Services, the IT Certification Body of Standardization Testing and Quality Certification – was established in 1998 and offers a variety of services in the context of security evaluation and validation. It is the first Certification Body in India for BS 7799/ISO 27001 certification of Information Security Management Systems (ISMS). The Indian CC Certification Scheme (IC3S) is the IT security evaluation & certification Scheme based on Common Criteria standards, it is established by Govt. of India under Department of Information Technology, STQC Directorate to evaluate & certify the trustworthiness of security features in Information Technology (IT) products and systems. The IC3S is an Indian independent third party evaluation and certification scheme for evaluating the security functions or mechanisms of the IT products. It also provides framework for the International Mutual Recognition of such certificates with the member countries of CCRA (Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security). The principal participants in the scheme are:

a) Applicant (Sponsor/Developer) of IT security evaluations;

b) STQC Certification Body (STQC/DeitY/MCIT/Govt. of India);

c) Common Criteria Testing Laboratories (CCTLs).

A.3 Specifications of the Certification Procedure

The certification body operates under the official administrative procedures according to the criteria and procedures laid down in the following:

- ISO/IEC Guide 65, and the requirements laid down in Annex C of CCRA
- Indian Common Certification Scheme (IC3S)
- STQC/CC/DO2: Standard Operating Procedure (SOP) for Certification Body - Quality Manual – describes the quality management system for the Scheme.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, Version 3.1
- Common Evaluation Methodology (CEM) Version 3.1.

A.4 Process of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The TOE has undergone the certification procedure at **STQC IT Certification Body**. The evaluation of the product was conducted by the evaluation body M / S Acucert Labs LLP , D-509 Neelkanth Business Park Vidyavihar West, Mumbai 400086, India. The evaluation facility is recognized under the IC3S scheme of STQC IT Certification Body.

Cisco Systems, Inc. 170 West Tasman Dr. San Jose, CA 95134-1706 USA is the developer and sponsor of the TOE evaluation. The certification process is concluded with the completion of this certification report.

This evaluation was completed on 21st November 2019 after submission of [ETR] to the validator certification body. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stated condition regarding configuration and operation, as given in part B of this report, are observed,
- The product is operated – where indicated – in the environment described.

This certification report applies only to the version and release of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant applies for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

A.5 Publication

The following Certification Results consist of Sections B1 to B11 of this report. The TOE will be included in the list of the products certified under IC3S Scheme of STQC IT Certification Body. The list of certified products is published at regular intervals in the Internet at http://www.commoncriteria-india.gov.in. Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form on request to the Certification Body.

PART B: CERTIFICATION RESULTS

B.1 Executive Summary

B.1.1 Introduction

The Certification Report documents the outcome of Common Criteria security evaluation of the TOE. It presents the evaluation results and the conformance results. This certificate is intended to assist the prospective buyers and users when judging the suitability of the IT security of the product for specified requirements.

Prospective buyers and users are advised to read this report in conjunction with the referred [ST] of the product, which specifies the functional, environmental and assurance requirements.

The evaluation was performed by Acucert Labs LLP , D-509 Neelkanth Business Park Vidyavihar West, Mumbai 400086, India. The information in the test report is derived from the [ST] written by the developer and the Evaluation Technical Report [ETR] written by M/S Acucert Labs LLP. The evaluation team determined the product to be conformant to NDcPP, ver. 2.1 and VPNGWEP ver. 2.1.

B.1.2 Evaluated product and TOE

The TOE is '**Cisco ASR 900 Series and NCS4200 Series running IOS-XE 16.9'**.

The evaluated sub-set and configuration of the product is described in this report as the Target of Evaluation (TOE). The Evaluated Configuration, its security functions, assumed environment, architectural information and evaluated configuration are given below (Refer B2 to B5).

B.1.3 Security Claims

The [ST] specifies the security objectives of the TOE and the threats that they counter (Refer 3.3 and 4.1 of ST). All the Security Functional Requirements (SFRs) (listed in 6.1 of ST) are taken from **NDcPP, ver. 2.1 24 Sept 2018 and VPNGWEP ver. 2.1 8 March 2017**.

B.1.4 Conduct of Evaluation

The evaluation was initiated by the IC3S Certification Scheme of STQC IT Certification Body vide communication no. IC3S/CB/2019/0001 dated 5th April 2019.

The TOE as described in the [ST] is 'Cisco ASR900 Series and NCS4200 Series running with IOS-XE 16.9'. The TOE was evaluated through evaluation of its documentation; testing and vulnerability assessment, using methodology stated in **Common Evaluation Methodology [CEM] and Supporting Document Mandatory Technical Document Evaluation Activities for Network Device cPP, ver. 2.1 September 2018** .

B.1.5 Independence of Certifier

The certifier did not render any consulting or other services for the company ordering the certification and there was no relationship between them, which might have an influence on this assessment.

B.1.6 Disclaimers

The certification results only apply to the version and release of the product as indicated in the certificate. The certificate is valid for stated conditions as detailed in this report. This certificate is not an endorsement of the IT product by the Certification Body or any other organization that recognizes or gives effect to this certificate. It is also not an endorsement of the target of evaluation (TOE) by any agency of the Government of India and no warranty of the TOE is either expressed or implied.

B.1.7 Recommendations and conclusions

- The conclusions of the Certification Body are summarized in the Certification Statement at Section A1.
- The specific scope of certification should be clearly understood by reading this report along with the [ST].
- The TOE should be used in accordance with the environmental assumptions mentioned in the [ST].
- The TOE should be used in accordance with the supporting guidance documentation.
- This Certification report is only valid for the evaluated configurations of the TOE.

B.2 Identification of TOE

The TOE is single-device security, routing and switching solutions for protecting the network. In support of their routing capabilities, CISCO ASR900 and NCS4200 Series devices provide IPsec connection capabilities to facilitate secure communications with external entities, as required and provide VPN functionality. The TOE is intended for simplified management to small businesses as well as metro and enterprise size business, service providers and carriers.

Table 1: TOE components along with users' manuals

TOE Component	Description
The TOE	Cisco ASR900 Series and NCS4200 Series running with IOS-XE 16.9
The TOE Guidance documentation	Listed in the Cisco ASR900 Series and NCS4200 Series Common Criteria Operational User Guidance and Preparative Procedures document at http://cisco.com web site
TOE Hardware model	ASR902, ASR903, ASR907, ASR920 and NCS4201, NCS4202, NCS4206, NCS4216. The ASR900 Series and NCS4200 Series that comprises the TOE has common hardware characteristics. These characteristics affect only non-TSF relevant functions of the platforms (such as throughput and amount of storage) and therefore support security equivalency of the platforms in terms of hardware.
TOE Software	IOS-XE 16.9

Non-TOE Environment:

The TOE supports the following hardware, software, and firmware components in its operational environment. All of the following environment components are supported by all TOE evaluated configurations.

Component	Usage/Purpose Description for TOE performance
Audit (Syslog) Server	This includes any syslog server to which the TOE would transmit syslog messages over IPsec.
Certification Authority (CA)	This includes any IT Environment Certification Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.
Local Console	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
Management Workstation with SSH client	This includes any IT Environment Management workstation that is used by the TOE administrator to support TOE administration using SSHv2 protected channels. Any SSH client that supports SSHv2 may be used.

Component	Usage/Purpose Description for TOE performance
RADIUS AAA Server	This includes any IT environment RADIUS AAA server that provides authentication services to TOE administrators.
TOE (VPN) Peer	This includes any TOE (VPN) peer with which the TOE participates in secure (IPsec) communications. The TOE (VPN) peer may be any device that supports secure (IPsec) communications.

B.3 Security policy

There are following organizational security policy (ies) that the TOE must meet.

Table 2: Organizational Security Policies

P.Type	Description
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

B.4 Assumptions

There are following assumptions exist in the TOE environment.

Table 3: Assumptions

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device’s physical interconnections and correct operation. This protection is assumed sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

Assumption	Assumption Definition
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

B.5 Evaluated configuration

The TOE consists of one or more physical devices as specified in section B.2 and includes the Cisco IOS-XE 16.9 software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XE configuration determines how packets are handled to and from the TOE's network interfaces. The TOE configuration will determine how traffic flows, received on an interface will be handled.

In addition, if the ASR900 Series and NCS4200 Series is to be remotely administered, then the management workstation must be connected to an internal network, where SSHv2 is used to securely connect to the TOE. A syslog server is used to store audit records, where IPsec is used to secure the transmission of the audit records. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Security Audit
2. Cryptographic Support
3. Identification and Authentication
4. Security Management
5. Packet Filtering
6. Protection of the TSF
7. TOE Access
8. Trusted Path/Channels

The TOE provides cryptography in support of other security functionalities. All the algorithms have CAVP certificates (Operation Environment – ASR900 Series, PPC e5500 and NCS4200 series PPC e5500 and PPC e500v2).

The TOE leverages the IOS Common Crypto Module (IC2M) Rel5. The IOS-XE software calls the IC2M, certificate 2388 which has been validated for conformance to the requirements of FIPS 140-2 Level 1.

The ASR900 Series and NCS4200 Series that comprises the TOE has common hardware characteristics. These characteristics affect only non-TSF relevant functions of the platforms (such as throughput and amount of storage) and therefore support security equivalency of the platforms in terms of hardware.

The ASR900 Series and NCS4200 Series platforms contain the following processors:

Chassis	CPU Designation
ASR902	CPU NXP T1042 and CPU Core PPC e5500
ASR903	CPU NXP T1042 and CPU Core PPC e5500

Chassis	CPU Designation
ASR907	CPU NXP T1042 and CPU Core PPC e5500
ASR920	CPU NXP T1042 and CPU Core PPC e5500
NCS4201	CPU NXP P2020 and CPU Core PPC e500v2
NCS4202	CPU NXP T1042 and CPU Core PPC e5500
NCS4206	CPU NXP P2020 and CPU Core PPC e500v2
NCS4216	Requires at least one RSP – NCS420X-RSP - CPU NXP T1042 and CPU Core e5500 and/or NCS4216-RSP - CPU NXP T1042, CPU Core e5500

B.6 Document Evaluation

The evaluator performed document analysis to address technology specific aspects covering specific SARs (ASE_TSS.1, ADV_FSP.1, AGD_OPE.1) as mandated in SD document [REF-3] – this is in addition to the CEM work units.

B.6.1 Documentation

The list of documents, those were presented, as evaluation evidences to the evaluators at the evaluation facility, are given below:

1. **Security Target**: Cisco ASR900 Series and NCS4200 Series running IOS-XE 16.9 Common Criteria Certification Security Target, ver.1.0 dated 11 October 2019 [DA-1]
2. **Guidance**: Cisco ASR900 Series and NCS4200 Series running IOS-XE 16.9 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration Version 1.0, 11 October 2019 [DA-2]
3. **Entropy Information**: Cisco ASR900 Series and NCS4200 Series running IOS XE 16.9 Hardware Entropy Information Version 1.0 11 October 2019 [DA-3]
4. **Bill of material** (15-14208-01.xlsx and ASR-920-24SZ-M.xls), in support of ALC_CMS.1 evidence [DA-4]
5. **An excerpt from the original build file** (ALC_CMS.1_IC2M.docx), in support of ALC_CMS.1 evidence[DA-5]

B.6.2 Analysis of document

The documents related to the following areas were analyzed using [CEM] and [SD]. The summary of analysis is as below:

Development process:

The evaluator examined the interface documentation [DA-3] for the description, the purpose and method of use for each TSFI. The TSFIs examined are as follows:

- SSH Server is for remote TOE CLI access.
- Serial interface is for local TOE CLI access
- IPsec for communication with secure peer
- external audit servers using IPsec,
- remote AAA servers using IPsec,
- remote VPN gateways/peers using IPsec,
- a CA server using IPsec

The evaluation activities cover ADV_FSP.1-1 to ADV_FSP1-7.

Guidance Documents: The evaluator performed the tasks of the CEM work units associated with the AGD_OPE.1 and AGD_PRE.1.

The Evaluator has confirmed the following aspects have been adequately addressed in the Guidance document [DA-3]:

1. the guidance documentation is appropriate to the Administrators and the Users of the TOE.

2. the guidance documentation is appropriate to every operational environment that the product supports for all platforms, as claimed in the Security Target.
3. the guidance documentation contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE.
4. the guidance documentation provides warning to the administrator when other cryptographic engines, which was not evaluated nor tested during the CC evaluation of the TOE.

The evaluation activities cover work units AGD_OPE.1-1 to AGD_OPE.1-8.

The evaluator performed the CEM work units associated with the AGD_PRE.1 on the Guidance document [DA-3] along with the sample instances of the TOE. The following aspects have been ensured:

1. the guidance document includes a description of how the administrator verifies that the operational environment can fulfil its role to support the security functionality
2. the guidance document includes description for every supported Operational Environment and Platforms, as claimed in the Security Target
3. The guidance document includes instructions to install the TSF, successfully, in each Operational Environment
4. The guidance document includes instructions to manage the security of the TSF, successfully, as a product and as a component of the larger operational environment.
5. The guidance document includes instructions to provide a protected administrative capability
6. The guidance document identifies TOE passwords that have default values associated with them and includes instructions to change those values.

The evaluation activities cover work units AGD_PRE.1-1 to AGD_PRE.1-3.

Life-cycle support:

The evaluator found that each instance of the TOE are labelled with the same hardware identifier, that is found, in the ST and hence concluded that the TOE reference is consistence with ST. The Validator has confirmed the same during witness testing. The evaluation activities cover work units ALC_CMC.1-1 and ALC_CMC.1-2.

Configuration management: The evaluator examined the bill of material [DA-4] and snapshot of the 'build log' [DA-5] shared by the developer to complete evaluation tasks against the CEM work units ALC_CMS.1-1 and ALC_CMS.1-2.

B.7 Product Testing

B.7.1 Independent testing by the Evaluator

The Evaluator has drawn the test plans for the TOE according to the direction given in [REF-2] & [REF-3] and completed ALL tests.

The TOE sample instances considered for ATE_IND are ASR 920-24SZ-M SN. CAT2107V10L and NCS 4201-SA SN: CAT2107V0RR, conform to 'Equivalency Analysis for Cisco ASR900 and NCS4200' presented by the evaluation team. Some of the tests were witnessed by the validation.

B.7.3 Vulnerability Analysis and Penetration testing

Evaluation team conducted vulnerability Assessment and Penetration testing as per the guidance given in NDcPP Supporting document [REF3].

B.8 Evaluation Results

The evaluator presented ‘Assurance Activity Report for Security Target and other assurance components ’ , ‘Entropy Analysis Report’, ‘ Equivalency Analysis document for justification of TOE instances &Test logs’ and ‘Vulnerability Assessment report’ in support of evaluation results. A summary of the evaluation results have been documented in the [ETR] following CC Standards ver3.1.

The evaluation activities performed using methodology stated in [CEM] and SD [REF-3].

B.8.1 Documentation evaluation results:

The evaluator have analyzed the Security Target, the Guidance document and the development life- cycle document / evidences for TOE are analyzed by the in view of the requirements of the respective PP [REF-1] & [REF-2] and the supporting document [REF-3]. The final versions of the documents are found to comply with the requirements of NDcPP, ver. 2.1, VPNGW, ver. 2.1. and Supporting Document Mandatory Technical Document Evaluation Activities for Network Device cPP, ver 2.1

The Validator is concurrence with the evaluation result and agreed to the Evaluator’s verdict, as ‘PASS’, against the work units ADV_FSP.1-1 to ADV_FSP1-7, AGD_OPE.1-1 to AGD_OPE.1-8., AGD_PRE.1-1 to AGD_PRE.1-3. , ALC_CMC.1-1 and ALC_CMC.1-2 and ALC_CMS.1-1 and ALC_CMS.1-2.

B.8.2 Entropy Analysis:

The developer presented the description of the entropy source used in the TOE as a separate document, ‘Cisco ASR900 Series and NCS4200 Series running IOS XE 16.9 Hardware Entropy Information Version 1.0 11 October 2019 [DA-3]’. The evaluator presented an analysis on the Entropy document, in respect of its Design description, Entropy justification, Operating condition and Health Testing as per the requirements of NDcPP, Appendix D and arrived at ‘PASS’ verdict. The validator is in concurrence with the evaluator’s verdict.

The Entropy data for cryptographic function of the TOE is provided from ACT2 via its well-defined API.

The entropy source has been certified (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/2125#) under NIST CMVP program. The validator draws confidence from this certificate and declares concurrence with the evaluator’s ‘PASS’ verdict.

B.8.3 Testing:

All tests as directed in NDcPP Supporting Document document [REF-3] and in VPNGWEP [REF-2] conducted for both the TOE sample instances ASR 920-24SZ-M SN. CAT2107V10L and NCS 4201-SA SN: CAT2107V0RR.

An isolated network created at M/S Acucert Labs LLP, Mumbai with ASR 920-24SZ-M and NCS 4201-SA.

92 Tests are conducted on the TOE to cover the security functionalities stated in NDcPP [REF-1] and 20 test to cover the security functionalities of VPNGW[REF-2]. ALL the tests have successfully PASSED. The validator witnessed some selected tests and confirmed repeatability and reproducibility of the test results.

B.8.4 Vulnerability assessment and penetration testing:

The evaluator searched on the sources listed in Section A4 of the NDcPP SD v2.1 to determine a list of potential flaw hypotheses that are more recent that the publication date of the NDcPP, and those that are specific to the TOE and its components as specified in NDcPP SD v2.1. The evaluator examined results of information publicly available and found NO vulnerabilities exist that are exploitable by attackers with ‘Basic Attack Potential’ as defined in the CEM. So, the original flaw hypothesis is disproved.

The evaluator examined the following documents:

1. collaborative Protection Profile for Network Devices (NDcPP) v2.1
2. Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway (VPNGWEP) v2.1
3. NDcPP Supporting Document v2.1
4. Hardware Entropy Information v1.0, Cisco ASR900 Series and NCS4200 Series running IOS-XE 16.9 Common Criteria Security Target (ST) v1.0
5. Cisco ASR900 Series and NCS4200 Series running IOS-XE 16.9 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration v1.0.

Additionally, evaluator examined the NIAP Technical Decisions (TD) to analyse which were applicable based on TOE product type, the PP claims and the security functions claimed in above documents.
The evaluator also performed independent functional tested as per the guidance given in NDcPP Supporting document v2.1.
Based on all documentation analysis and functional testing, the evaluator did not find any residual vulnerabilities, which could be exploitable by an attacker with 'Basic Attack Potential'. The original flaw hypothesis is disproved.
The evaluator performed Penetrating testing using Nmap for Protocol IPv4, TCP and UDP on TOE, other than that evaluator also performed fuzz testing on the TOE. Output for NMAP and fuzz testing where examined to identify any residual vulnerabilities that can be exploited by the TOE environment.
The evaluator performed Penetrating testing using Test bed used for independent testing. The evaluator configured the NMAP v7.6 on one of the test user's Laptop and conducted the test The output of the Penetrating testing (referring the NMAP guidance published on their public website) did not reveal any residual vulnerabilities which could be exploitable by an attacker with Basic Attack Potential.

B.9 Validator Comments

The Validators have reviewed the Evaluation Technical Report [ETR] along with all relevant evaluation evidences, documents, records, etc. and are in agreement with the conclusion made in it i.e.

- **The [ST] has satisfied all the requirements of the assurance class ASE as mandated in NDcPP, version 2.1 and VPNGW, version 2.1.**
- **The results of evaluation confirm that Cisco ASR900 Series and NCS4200 Series (**hardware chassis: ASR902, ASR903, ASR907, ASR920 and NCS4201, NCS4202, NCS4206, NCS4216**) running IOS-XE 16.9, satisfies all the security requirements and assurance requirements as defined and mandated in NDcPP, version 2.1 and VPNGW, version 2.1, hence is recommended for Certification against the Protection Profiles NDcPP, version 2.1 and VPNGW, version 2.1.**

B.10 List of Acronyms

ACL: Access Control List
CC: Common Criteria
CCTL: Common Criteria Test Laboratory
CEM: Common Evaluation Methodology
DVS: Development security
EAL: Evaluation Assurance Level
ETR: Evaluation Technical Report
FSP: Functional Specification
IC3S: Indian Common Criteria Certification Scheme
IT: Information Technology
PP: Protection Profile
ST: Security Target
TOE: Target of Evaluation
TDS: TOE Design Specification
TSF: TOE Security Function
TSFI: TOE Security Function Interface

B.11 References

1. [CC-I]: Common Criteria for Information Technology Security Evaluation: Part 1: Version 3.1
2. [CC-II]: Common Criteria for Information Technology Security Evaluation: Part 2: Version 3.1
3. [CC-III]: Common Criteria for Information Technology Security Evaluation: Part 3: Version 3.1
4. [CEM]: Common Methodology for Information Methodology: Version 3.1
5. [REF-1]: Collaborative Protection Profile for Network Devices (NDcPP), version 2.1 , 24 Sept. 2018
6. [REF-2]: Network Device collaborative Protection Profile (NDcPP) Extended Package VPN Gateway (VPNGWEP), version 2.1, 8 March, 2017
7. [REF-3]: Supporting Document Mandatory Technical Document Evaluation Activities for Network Device cPP, version 2.1, September-2018
8. [ST] : “Cisco ASR900 Series and NCS4200 Series Switches running IOS-XE 16.9 Common Criteria Security Target ST Version 1.0, October 11, 2019”
9. [ETR]: Evaluation Technical Report No.: Evaluator’s report Cisco ASR900 Series and NCS4200 Series running IOS-XE 16.9 Evaluation Technical Report, ver. 1.0 dated 21-11-2019