National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Cisco Embedded Services Router 5921 (ESR5921) running IOS version 15.9M

Report Number: CCEVS-VR-11275-2022

Dated: 08/05/2022

Version: 0.2

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 George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers

Meredith Martinez

Marybeth S Panock

Seada Mohammed

Fernando L Guzman

Aerospace Corporation

Common Criteria Testing Laboratory

Ken Lasoski

Shaunak Shah

Toan Truong

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) 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 for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 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 the Cisco Embedded Services Router 5921 (ESR5921) Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the 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 documented in the ST.

The evaluation was completed by Acumen Security in August 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e and PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.1.

The TOE identified in this VR 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), as interpreted by the Assurance Activities contained in the Protection Profile (PP). This VR 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 ETR are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, 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 ETR are consistent with the evidence produced.

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). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT 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.

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(s) 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 Embedded Services Router 5921 (ESR5921) running IOS version 15.9M
Protection Profile	• collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e • PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.1.
Security Target	Cisco Embedded Services Router 5921 (ESR5921) running IOS version 15.9M Security Target, , Version 1.0, August 4, 2022
Evaluation Technical Report	Evaluation Technical Report for Cisco Embedded Services Router 5921 (ESR5921) running IOS version 15.9M, Version 1.0, July 29, 2022
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Jerome Myers Meredith Martinez

Item	Identifier
	Marybeth S Panock Seada Mohammed Fernando L Guzman

3 Architectural Information

Product Description

The Cisco Embedded Services Router 5921 (herein after referred to as the ESR5921) is a purpose-built, routing platform that includes VPN functionality.

Cisco IOS 15.9M software is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective switching and routing. Although IOS performs many networking functions, this Security Target only addresses the functions that provide for the security of the TOE itself.

In support of the routing capabilities, the Cisco ESR 5921 provides IPsec connection capabilities to facilitate secure communications with external entities, as required.

The TOE includes the hardware models as defined in the Table 1.

Evaluated Configuration

The TOE is a hardware and software solution that makes up the router models as follows:

- Cisco 5921 ESR virtual router deployed on one of the following compatible platforms:
  - Cisco UCS C-Series M5 Servers with Intel Xeon Scalable 2nd Generation (Cascade Lake)
  - General-purpose computing platforms with Intel Coffee Lake processors: Xeon E-2254ML

The network, on which they reside, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS software image Release 15.9M. In addition, the software image is also downloadable from the Cisco web site. A login id and password is required to download the software image.

The TOE is comprised of the following physical specifications as described in Table 1 below:

Table 1 Hardware Models and Specifications

Hardware	Processor	Features
Cisco ESR 5921(CISCO5921-K9) virtual router compatible Cisco UCS Servers and other general-purpose computing platforms with specified Intel processors	Intel Xeon Scalable 2nd Generation (Cascade Lake)[1] with ESXi 6.7 Intel Coffee Lake processors with ESXi 6.7[2]	**Cisco UCS C-Series M5 Servers Interfaces:** All compatible Cisco UCS C-Series M5 Server models have a dedicated OOB management port, at least two physical ethernet ports, and PCIe expansion slots for additional NICs. **General-purpose computing hardware Interfaces:** • A dedicated management port • Two or more virtual network interface cards that are mapped to physical ethernet ports.

[1] Evaluated on UCS C220 M5 with Intel Xeon Gold 6238R

[2] Evaluated on PacStar 451 with Intel Xeon E-2254ML

4 Security Policy

4.1 Logical Scope of the TOE

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

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all SFRs of the NDcPP v2.2e and MOD_VPNGW v1.1 as necessary to satisfy testing/assurance measures prescribed therein.

4.2 Security Audit

The TOE provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations and manages audit data storage. The TOE provides the administrator with a circular audit trail or a configurable audit trail threshold to track the storage capacity of the audit trail. Audit logs are backed up over an encrypted channel to an external audit server.

4.3 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have CAVP certificates. The TOE leverages the IOS Common Cryptographic Module (IC2M) Rel5.

Table 2 FIPS References

Algorithm	Description	Supported Mode	Module	CAVP Cert. #	SFR
AES	Used for symmetric encryption/decryption	CBC (128, 192 and 256) GCM (128, 192 and 256)	IC2M	A1462	FCS_COP.1/DataEncryption
SHS (SHA-1, SHA-256, SHA-384 and SHA-512)	Cryptographic hashing services	Byte Oriented	IC2M	A1462	FCS_COP.1/Hash
HMAC (HMAC-SHA-1, SHA-256, SHA-512)	Keyed hashing services and digital signature	Byte Oriented	IC2M	A1462	FCS_COP.1/KeyedHash
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	CTR_DRBG (AES 256)	IC2M	A1462	FCS_RBG_EXT.1
RSA	Signature Verification and key transport	PKCS#1 v.1.5, 3072 bit key, FIPS 186-4 Key Gen	IC2M	A1462	FCS_CKM.1 FCS_COP.1/SigGen
ECDSA	Cryptographic Signature services	FIPS 186-4, Digital Signature Standard (DSS)	IC2M	A1462	FCS_CKM.1 FCS_COP.1/SigGen
CVL-KAS-ECC	Key Agreement	NIST Special Publication 800-56A	IC2M	A1462	FCS_CKM.2

The TOE provides cryptography in support of VPN connections and remote administrative management via SSHv2 and IPsec to secure the transmission of audit records to the remote syslog server. In addition, IPsec is used to secure the session between the TOE and the authentication servers.

The cryptographic services provided by the TOE are described in **Table 3** below:

Table 3 TOE Provided Cryptography

Cryptographic Method	Use within the TOE
Internet Key Exchange	Used to establish initial IPsec session.
Secure Shell Establishment	Used to establish initial SSH session.
RSA Signature Services	Used in IPsec session establishment. Used in SSH session establishment. X.509 certificate signing
SP 800-90 RBG	Used in IPsec session establishment. Used in SSH session establishment.
SHS	Used to provide IPsec traffic integrity verification Used to provide SSH traffic integrity verification Used for keyed-hash message authentication
AES	Used to encrypt IPsec session traffic. Used to encrypt SSH session traffic.
RSA	Used in IKE protocols peer authentication Used to provide cryptographic signature services
ECDSA	Used to provide cryptographic signature services Used in Cryptographic Key Generation Used as the Key exchange method for IPsec
FFC DH	Used as the Key exchange method for SSH and IPsec
ECC DH	Used as the Key exchange method for IPsec

4.4 Identification and Authentication

The TOE performs two types of authentication: device-level authentication of the remote device (VPN peers) and user authentication for the Authorized Administrator of the TOE. 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 supports use of IKEv1 (ISAKMP) and IKEv2 pre-shared keys for authentication of IPsec tunnels. The IKE phase authentication for the IPsec communication channel between the TOE and authentication server and between the TOE and syslog server is considered part of the Identification and Authentication security functionality of the TOE.

The TOE provides authentication services for administrative users to connect to the TOE's secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys. The TOE supports the use of a RADIUS AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE's CLI.

The TOE provides an automatic lockout when a user attempts to authenticate and enters invalid information. After a defined number of authentication attempts fail exceeding the configured allowable attempts, the user is locked out until an authorized administrator can enable the user account.

The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec connections.

4.5 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection. The TOE provides the ability to securely manage:

- Administration of the TOE locally and remotely;
- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE;
- Update to the TOE and verification of the updates;
- Configuration of IPsec functionality.

The TOE supports two separate administrator roles: non-privileged administrator and privileged administrator. Only the privileged administrator can perform the above security relevant management functions. Management of the TSF data is restricted to Security Administrators. The ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE is restricted to authorized administrators.

Privileged administrators can create configurable login banners to be displayed at time of login, and can also define an inactivity timeout for each admin interface to terminate sessions after a set period of inactivity.

4.6 Packet Filtering

The TOE provides packet filtering and secure IPsec tunneling. The tunnels can be established between two trusted VPN peers. More accurately, these tunnels are sets of security associations (SAs). The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per the ESP security protocol. An authorized administrator can define the traffic that needs to be protected via IPsec by configuring access lists (permit, deny, log) and applying these access lists to interfaces using crypto map sets.

4.7 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords.

Additionally, Cisco IOS 15.9M is not a general-purpose operating system and access to Cisco IOS 15.9M memory space is restricted to only Cisco IOS 15.9M functions.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually. Finally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

Whenever a failure occurs within the TOE that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE and reloads.

4.8 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. Sessions can also be terminated if an Authorized Administrator enters the "exit" or "logout" command.

The TOE can also display a Security Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

4.9 Trusted path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2, and initiates outbound IPsec tunnels to transmit audit messages to remote syslog servers. In addition, IPsec is used to secure the session between the TOE and the authentication servers. The TOE can also establish trusted paths of peer-to-peer IPsec sessions. The peer-to-peer IPsec sessions can be used for securing the communications between the TOE and authentication server/syslog server, as well as to protect communications with a CA or remote administrative console.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Assumptions drawn from:

- collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e
- PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.1

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

- collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e
- PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.1

5.3 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:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e and PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.1.
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Cisco Embedded Services Router 5921 (ESR5921) running IOS version 15.9M Security Target
- Cisco Embedded Services Router 5921 (ESR5921) CC Configuration guide

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 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE in the evaluated configuration contains the following:

- Cisco UCS C-Series M5 Server or other general-purpose computing platforms with specified Intel processors as described in Table 1
- VMware ESXi 6.7 Hypervisor
- The following minimum technical specs needed on the Cisco UCS Server or general-purpose computing platforms to support a single Cisco ESR 5921 guest Virtual Machine (VM) running Cisco IOS version 15.9M software:
  - Single hard disk
  - 4 GB virtual disk
  - 2 or more virtual network interface cards
  - The following Platform Specifications are recommended:
    - Processor - x86
    - Memory - 512 MB minimum
    - Disk Space - 300 MB minimum
    - Operating System - glibc compiled Linux

The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS 15.9M configuration determines how packets are handled to and from the TOE's network interfaces. The router configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination.

7.2 Excluded Functionality

The following functionality is excluded from the evaluation:

Table 4 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.

These services will be disabled by configuration settings. The exclusion of this functionality does not affect compliance to the NDcPP v2.2e and MOD_VPNGW v1.1.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in ETR for Cisco Embedded Services Router 5921 (ESR5921), which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e and PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.1. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here. The AAR, in section 4.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

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 documents: the Detailed Test Report (DTR) and the ETR. The reader of this document can assume that all 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 TOE Name to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

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 Embedded Services Router 5921 (ESR5921) that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e and PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.1.

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 Development Documentation

The evaluation team applied each EAL 1 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 ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e and PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.1 related to the examination of the information contained in the TOE Summary Specification.

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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 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. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e and PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.1 related to the examination of the information contained in the operational guidance documents.

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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 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 Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e and PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.1 and recorded the results in a Test Report, summarized in the ETR and AAR.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e and PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.1, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

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 addressed the vulnerability analysis Assurance Activities in the collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e and PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.1, 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 test activities 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 performed the Assurance Activities in the collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e and PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.1, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Cisco Embedded Services Router 5921 (ESR5921) CC Configuration guide document.

No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Cisco Embedded Services Router 5921 (ESR5921) running IOS version 15.9M Security Target. Other functionality included in the product was not assessed as part of this evaluation.

All other functionality provided, to include software, firmware, or hardware that was not part of the evaluated configuration needs to be assessed separately and no further conclusions can be drawn about their effectiveness. The excluded functionality is specified in section 7.2 of this report.

All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Annexes

Not applicable.

12 Security Target

Cisco Embedded Services Router 5921 (ESR5921) running IOS version 15.9M Security Target, Version 1.0, August 4, 2022

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.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e
6. PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.1
7. Cisco Embedded Services Router 5921 (ESR5921) CC Configuration Guide, Version 1.0, August 4, 2022
8. Cisco Embedded Services Router 5921 (ESR5921) running IOS version 15.9M Security Target, Version 1.0, August 4, 2022
9. Assurance Activity Report for Cisco Embedded Services Router 5921 (ESR5921) running IOS version 15.9M, Version 1.1, July 29, 2022
10. Evaluation Technical Report for Cisco Embedded Services Router 5921 (ESR5921) running IOS version 15.9M, Version 1.0, July 29, 2022