

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

Cisco Embedded Services Router (ESR) 6300

Report Number: CCEVS-VR-VID11162-2021
Dated: May 21, 2021
Version: 1.0

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

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

ACKNOWLEDGEMENTS

Validation Team

Patrick Mallett, Ph.D. Jim
Donndelinger
Marybeth Panock
Aerospace Corporation

Common Criteria Testing Laboratory

Tammy Compton
Cody Cummins
Wasif Sikder
*Gossamer Security Solutions, Inc. Columbia,
MD*

Table of Contents

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

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Embedded Services Router (ESR) 6300 solution provided by Cisco Systems, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in May 2021. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 with the PP-Module for Virtual Private Network (VPN) Gateways, version 1.1, 18 June 2020.

The Target of Evaluation (TOE) is the Cisco Embedded Services Router (ESR) 6300.

The TOE identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Cisco Embedded Services Router (ESR) 6300 Security Target, version 1.0, April 28, 2021 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product’s evaluation. Upon successful completion of the evaluation, the product is added to NIAP’s Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Cisco Embedded Services Router (ESR) 6300 (Specific models identified in Section 8)
Protection Profile	PP-Configuration for Network Device and Virtual Private Network (VPN) Gateways, version 1.1, 1 July 2020 <ul style="list-style-type: none"> • Base-PP: collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 • PP-Module: PP-Module for Virtual Private Network (VPN) Gateways, version 1.1, 18 June 2020
ST	Cisco Embedded Services Router (ESR) 6300 Security Target, version 1.0, April 28, 2021
Evaluation Technical Report	Evaluation Technical Report for Cisco Embedded Services Router (ESR) 6300, version 0.2, April 28, 2021
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria	Gossamer Security Solutions, Inc.
Testing Lab (CCTL)	Columbia, MD
CCEVS Validators	Patrick Mallett, Jim Donndelinger, Marybeth Panock

3 Architectural Information

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

The TOE is the Cisco Embedded Services Router (ESR) 6300 (herein after referred to as the ESR6300). The TOE is comprised of both software and hardware. The hardware models included in the evaluation are: ESR-6300-NCP-K9 and ESR-6300-CON-K9. The software is comprised of the Cisco IOS-XE 17.3.

The ESR6300 consists of the following architectural features:

- Compact 3” x 3.75” form factor board optimized for custom solutions
- DRAM: 4-GB DDR4 memory capacity
- Flash Memory: 4-GB usable eMMC flash
- Optional router enclosure
- Integrated multi-pin BTB Interface Connector - provides pins dedicated for power input, ethernet ports, and console ports. The following interfaces were used during testing:
 - Console: 1 UART RS232 RJ45 console port
 - WAN Interfaces: 2 Combo Layer 3 GE WAN ports
 - LAN Interfaces: 4 Layer 2 GE LAN ports

The ESR6300 is a purpose-built, routing platform that includes VPN functionality provided by the Cisco IOS-XE software.

The ESR6300 is an embedded router module with a compact form factor of 3.0 by 3.775 inches. Its compact, modular, ruggedized design allows Cisco partners and integrators to build a wide variety of custom embedded solutions. The TOE can be inserted into an enclosure that can accommodate the TOE's size (3.0 x 3.775 in) and provides no compute capabilities. The ESR6300 is available with a custom-designed cooling plate, as well as without the cooling plate. Both versions of the ESR6300 board include an integrated multi-pin Board-to-Board (BTB) interface connector with pins dedicated for power input, ethernet ports, and console ports. The TOE functionality is implemented inside the ESR 6300 physical chassis, as the chassis includes the underlying board (with or without a cooling plate) and all electronic components attached to it; therefore, no computational capabilities outside of the TOE boundary are required to secure the TOE. Refer to Annex A in the Guidance Document (AGD) for hardware technical guidance on the ESR6300 board layout and dimensions and Multi-pin BTB Interface Connector description that includes pinout mapping descriptions for network interfaces and power inputs.

3.1 TOE Evaluated Platforms

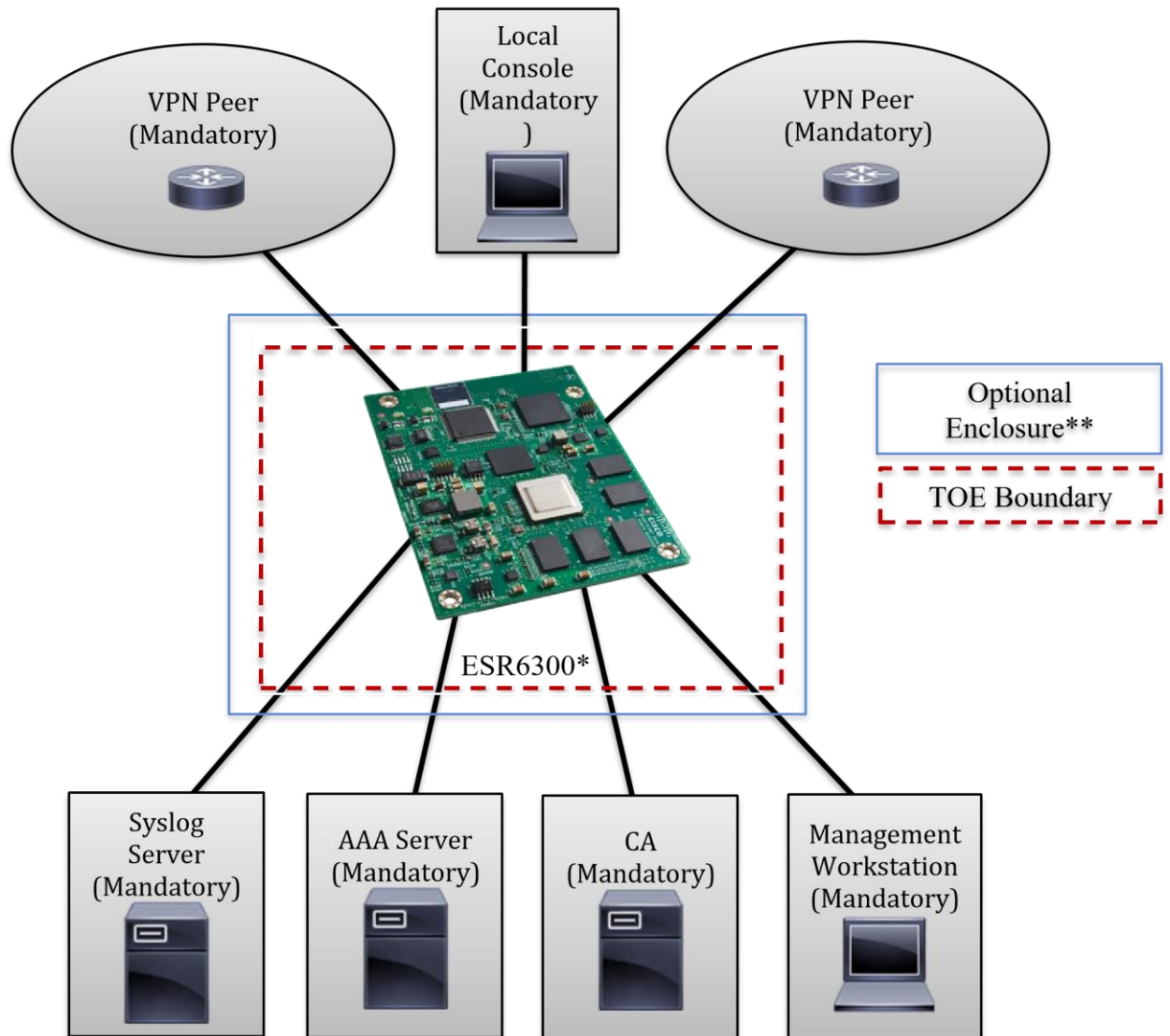
Detail regarding the evaluated configuration is provided in Section 8 below.

3.2 TOE Architecture

The TOE consists of one physical device and includes the Cisco IOS-XE 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 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.

The following figures provide a visual depiction of an example TOE deployment, a LAN/WAN interface diagram, and console port options:

Figure 1 TOE Example Deployment



* The ESR6300 physical chassis pictured includes a multi-pin BTB interface connector on the underside of the board that is fully integrated when purchased.

** The end user can opt to use an enclosure that can accommodate the TOE's size (3.0 x 3.775 in.) and provides no computational services.

The TOE example deployment in figure 1 includes the following:

- The following are considered to be in the IT Environment:
 - VPN Peers
 - Management Workstation
 - RADIUS AAA (Authentication) Server
 - Audit (Syslog) Server
 - Local Console

- Certification Authority (CA)

Figure 2 TOE LAN/WAN Interfaces

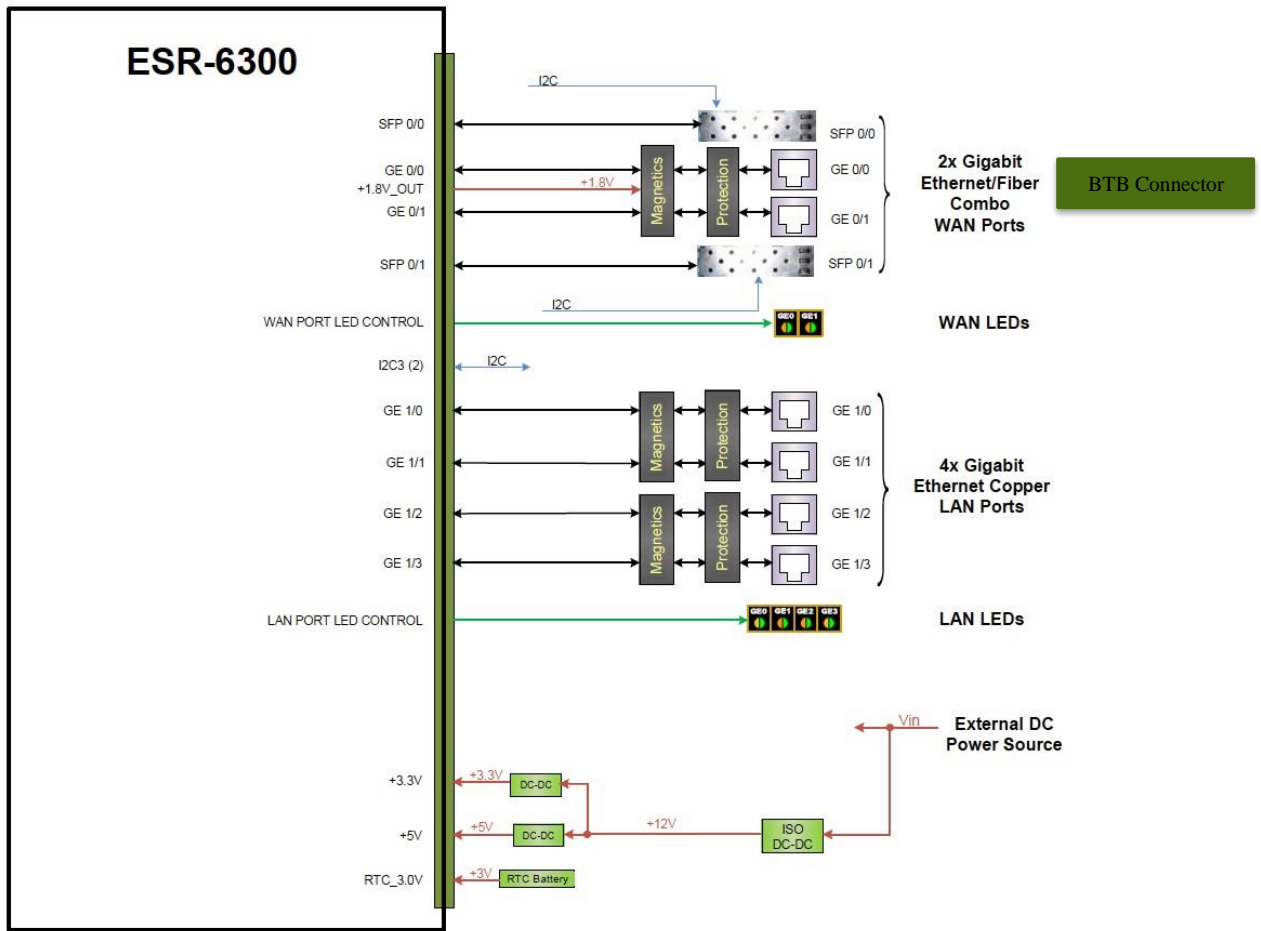
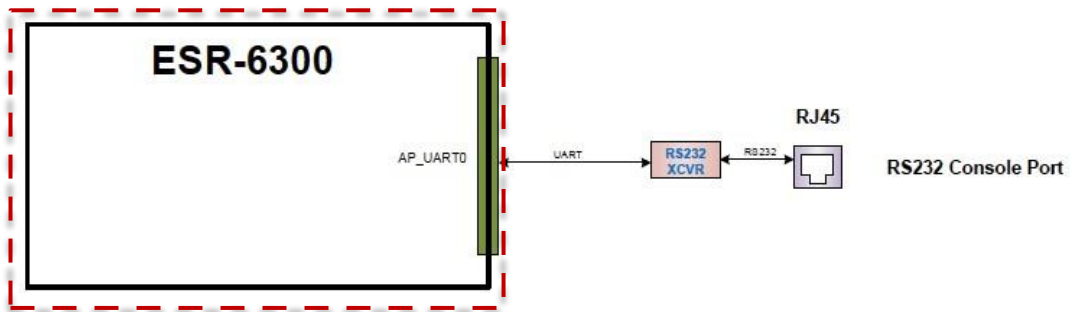


Figure 3 TOE Evaluated RS232 Console Port



- NOTE: While the previous figure includes several non-TOE IT environment devices, the TOE is only the ESR6300 device. Only one TOE device is required for deployment in an evaluated configuration.

3.3 Physical Boundaries

The physical boundary of the TOE is the hardware appliance. The TOE supports the following hardware, software, and firmware in its environment when the TOE is configured in its evaluated configuration:

Table 1 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
RADIUS AAA Server	Yes	This includes any IT environment RADIUS AAA server that provides single-use authentication mechanisms. This can be any RADIUS AAA server that provides single-use authentication. The TOE correctly leverages the services provided by this RADIUS AAA server to provide single-use authentication to administrators.
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Local Console	Yes	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.
Certification Authority (CA)	Yes	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.
Remote VPN Peer	Yes	This includes any VPN Peer (Gateway, Endpoint, another instance of the TOE) with which the TOE participates in VPN communications. Remote VPN Peers may be any device that supports IPsec VPN communications. Another instance of the TOE used as a VPN Peer would be installed in the evaluated configuration, and likely administered by the same personnel.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Also referred to as audit server in the ST.
Router Enclosure	Yes	The end user can opt to use an enclosure that accommodates the TOE's size (3.0 x 3.775 in.) and provides no compute capabilities. The TOE functionality is implemented inside the ESR 6300 physical chassis, as the chassis includes the underlying board (with or without a cooling plate) and all electronic components attached to it; therefore, no computational capabilities outside of the TOE boundary are required to secure the TOE. During testing, the TOE was enclosed within a Cisco developed hardened enclosure. It is a specially designed enclosure used for Cisco internal testing purposes only. It has no compute capabilities and is not a commercially available product. The enclosure passes network connections directly to the TOE interfaces and does not change or modify TSF functionality. In the evaluated configuration, the enclosure used for testing contains the ESR6300 board including the integrated multi-pin BTB interface connector with pins dedicated for power input, ethernet ports, and console ports (two combo Gigabit Ethernet WAN ports, four Gigabit Ethernet LAN ports, and one UART RS232 RJ-45 console port). Refer to Annex A in the Guidance Document (AGD) for hardware technical guidance on the ESR6300 board layout and dimensions and Multi-pin BTB Interface Connector description that includes pinout mapping descriptions for network interfaces and power inputs.

4 Security Policy

This section summarizes the security functionality of the TOE:

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

4.1 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. The TOE is configured to transmit its audit messages to an external syslog server over an encrypted channel.

4.2 Cryptographic support

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have CAVP certificates (Operational Environment – Marvell Armada ARMv8 Cortex A72). The TOE leverages the IOS Common Cryptographic Module (IC2M) Rel5.

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.

4.3 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 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.

4.4 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.

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.

4.5 Packet filtering

The TOE provides packet filtering and secure IPsec tunneling. The tunnels can be established between two trusted VPN peers and the TOE. 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.

4.6 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-XE is not a general-purpose operating system and access to Cisco IOS-XE memory space is restricted to only Cisco IOS-XE 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.

4.7 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.

4.8 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 & Clarification of Scope

Assumptions

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

- collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 with the PP-Module for Virtual Private Network (VPN) Gateways, version 1.1, 18 June 2020

That information has not been reproduced here and the NDcPP22E/MOD_VPNGW11 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22E/MOD_VPNGW11 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

Clarification of scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the collaborative Protection Profile for Network Devices and the VPN Gateway Module and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP22E/MOD_VPNGW11 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- Cisco Embedded Services Router (ESR) 6300 CC Configuration Guide, Version 1.0, March 15, 2021

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Assurance Activity Report for Cisco Embedded Services Router (ESR) 6300, Version 0.2, April 28, 2021 (AAR).

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP22E/MOD_VPNGW11 including the tests associated with optional requirements.

8 Evaluated Configuration

The TOE is comprised of both software and hardware. The hardware models included in the evaluation are: ESR-6300-NCP-K9 and ESR-6300-CON-K9. The software is comprised of the Cisco IOS-XE 17.3.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Embedded Services Router (ESR) 6300 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22E/MOD_VPNGW11.

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 Embedded Services Router (ESR) 6300 product 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 NDcPP22E/MOD_VPNGW11 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 NDcPP22E/MOD_VPNGW11 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 located in the Detailed Test Report (DTR) was prepared by the evaluator on 4/28/2021. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (<https://web.nvd.nist.gov/vuln/search>), Vulnerability Notes Database (<http://www.kb.cert.org/vuls/>), Rapid7 Vulnerability Database (<https://www.rapid7.com/db/vulnerabilities>), Tipping Point Zero Day Initiative (<http://www.zerodayinitiative.com/advisories>), Exploit / Vulnerability Search Engine

(<http://www.exploitsearch.net>), SecurITTeam Exploit Search (<http://www.securiteam.com>), Tenable Network Security (<http://nessus.org/plugins/index.php?view=search>), Offensive Security Exploit Database (<https://www.exploit-db.com/>) on 3/16/2021 with the following search terms: "Cisco IOS XE", "ESR-6300-NCP-K9", "ESR-6300-NCP-K9", "Marvell Armada Cortex A72", "IOS Common Cryptographic Module", "IC2M".

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 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 (ESR) 6300 CC Configuration Guide, Version 1.0, March 15, 2021 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 Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

This product is an embedded device and does not have the physical interface that we normally review in an NDcPP compliant appliance. See Annex A in the Administrator's Guide for information regarding the physical TSF interface and guidance on integration.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Cisco Embedded Services Router (ESR) 6300 Security Target, Version 1.0, April 28, 2021.*

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

- [1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.
- [2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
- [3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
- [4] collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 with the PP-Module for Virtual Private Network (VPN) Gateways, version 1.1, 18 June 2020.

- [5] Cisco Embedded Services Router (ESR) 6300 Security Target, Version 1.0, April 28, 2021 (ST).
- [6] Assurance Activity Report for Cisco Embedded Services Router (ESR) 6300, Version 0.2, April 28, 2021 (AAR).
- [7] Detailed Test Report (NDcPP22E/MOD_VPNGW11) for Cisco Embedded Services Router (ESR) 6300, Version 0.2, April 28, 2021 (DTR).
- [8] Evaluation Technical Report for Cisco Embedded Services Router (ESR) 6300, Version 0.2, April 28, 2021 (ETR).