National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 4000 Series (ISR4K), Cisco Catalyst 8300 and 8500 Series Edge Routers (Cat8300, Cat8500) running IOS XE Version 17.3

Report Number: CCEVS-VR-VID11208-2022

Dated: 18 February 2022

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

DeRon Graves

Patrick Mallett, PhD

Jerome Myers, PhD

The Aerospace Corporation

Common Criteria Testing Laboratory

Kenneth Lasoski

Yogesh Pawar

Sayli Khamkar

Riya Thomas

Supriya Patil

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 Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 4000 Series (ISR4K) and Cisco Catalyst 8300 and 8500 Series Edge Routers (Cat8300, Cat8500) running IOS XE Version 17.3** 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 **February 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 defined in the U.S. Government Protection Profile for Security Requirements for **collaborative Protection Profile for Network Devices Version 2.2e and PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 and Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSECEP) Version 1.2.**

The Target of Evaluation (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), as interpreted by the Assurance Activities contained in **the collaborative Protection Profile for Network Devices Version 2.2e, PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 and Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSECEP) Version 1.2.** 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 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 Security Target (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 evaluation technical report 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 Protection Profile containing Assurance Activities, which are interpretation of 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 information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance 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 Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 4000 Series (ISR4K) and Cisco Catalyst 8300 and 8500 Series Edge Routers (Cat8300, Cat8500) running IOS XE Version 17.3
Protection Profile	PP-Configuration for Network Device and Virtual Private Network (VPN) Gateways, Version 1.1, 01 July 2020 • Base-PP: collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E) • PP-Module: PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1(MOD_VPNGW_V1.1) Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSECEP), Version 1.2, May 10, 2016
Security Target	Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 4000 Series (ISR4K) and Cisco Catalyst 8300 and 8500 Series Edge Routers (Cat8300, Cat8500) running IOS XE Version 17.3 Security Target, Version 1.2, February 15, 2022

Evaluation Technical Report	Evaluation Technical Report for Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 4000 Series (ISR4K), Cisco Catalyst 8300 and 8500 Series Edge Routers (Cat8300, Cat8500) running IOS XE Version 17.3, Version 1.2, February 15, 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 2400 Research Blvd, Suite 395, Rockville, MD 20850.
CCEVS Validators	DeRon Graves, Patrick Mallett, Jerome Myers

3 Architectural Information

The Cisco Aggregation Services Router 1000 Series (herein after referred to as the ASR1K), Cisco Integrated Services Router 4000 Series (herein after referred to as the ISR4K), and the Cisco Catalyst 8300 and 8500 Series Edge Routers (herein after referred to as the Cat8300 and Cat8500 respectively) are purpose-built, routing platforms that includes VPN functionality and MACsec encryption provided by the Cisco IOS-XE software.

Cisco IOS-XE 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.

The TOE includes the hardware models as defined in Table 2.

Table 2 Hardware Models and Specifications

Hardware	Processor	Features

ASR1001-X,
ASR1001-HX, ASR1002-HX, ASR1006-X,
ASR1009-X,
ASR1013
 
 
 
 
	ASR1001-X
	• Intel Xeon E3-1125C (Sandy Bridge)
	• MACsec - Microsemi Intellisec VSC84xx/VSC85xx
	
	ASR1001-HX
	• Intel Xeon E3-1125C v2 (Ivy Bridge)
	• MACsec - Microsemi Intellisec VSC8500xx
	• HW Crypto Module (Required) – Marvell (formerly Cavium) OCTEON II
	
	ASR1002-HX
	• Intel Xeon E3-1125C v2 (Ivy Bridge)
	• MACsec - Microsemi Intellisec VSC84xx/VSC85xx
	• HW Crypto Module (Required) – Marvell (formerly Cavium) OCTEON II
	
	ASR1006-X, ASR1009-X, ASR1013
	• Intel Xeon L5238 (Wolfdale) (RP2)
	• Intel Xeon D-1527 (Broadwell) (RP3)
	• MACsec
	  ○ Microsemi Intellisec VSC84xx/VSC85xx
	  ○ APM SafeXcel-IP-160
		Physical dimensions (H x W x D in.)
		• ASR1001-X - 1.71 x 17.3 x 18.5
		• ASR1001-HX – 1.71 x 17.3 x 18.38
		• ASR1002-HX - 3.5 x 17.3 x 19.25
		• ASR1006-X - 10.5 x 17.2 x 22
		• ASR1009-X - 15.75 x 17.2 x 22
		• ASR1013 - 22.8 x 17.2 x 22
		
		Interfaces
		ASR1001-X
		• Shared Port Adapters: 1
		• Built-in Gigabit Ethernet ports: 8
		• ESP Bandwidth: 2.5 to 20 Gbps
		ASR1001-HX,
		• Shared Port Adapters: 0
		• Built-in Gigabit Ethernet ports: 12+8 optional
		• ESP Bandwidth: 60 Gbps
		ASR1002-HX,
		• Shared Port Adapters: 1
		• Built-in Gigabit Ethernet ports: 16
		• ESP Bandwidth: 100 Gbps
		ASR1006-X,
		• Shared Port Adapters: 12
		• Built-in Gigabit Ethernet ports: 0
		• ESP Bandwidth: 10 to 100 Gbps
		ASR1009-X,
		• Shared Port Adapters: 18

Hardware	Processor	Features
 		• Built-in Gigabit Ethernet ports: 0 • ESP Bandwidth: 40 to 200 Gbps ASR1013 • Shared Port Adapters: 12 • Built-in Gigabit Ethernet ports: 0 • ESP Bandwidth: 40 to 200 Gbps
ISR4321 ISR4331 ISR4351 ISR4431 ISR4451-X ISR4461 NIMs: NIM-1GE-CU-SFP, NIM-2GE-CU-SFP    	ISR4321 • Intel Atom C2558 (Silvermont) • MACsec - Microsemi Intellisec VSC85xx ISR4331 • Intel Atom C2718 (Silvermont) • MACsec - Microsemi Intellisec VSC85xx ISR4351 • Intel Atom C2758 (Silvermont) • MACsec - Microsemi Intellisec VSC85xx ISR4431 • Intel Xeon E3-1105C (Sandy Bridge) • MACsec - Microsemi Intellisec VSC85xx ISR4451-X • Intel Xeon E3-1105C v2 (Ivy Bridge) • MACsec - Microsemi Intellisec VSC85xx ISR4461 • Intel Xeon D-1530 (Broadwell) • MACsec - Microsemi Intellisec VSC85xx	**Physical dimensions** (H x W x D in.) • ISR4321 - 1.75 x 14.55 x 11.60 1RU • ISR4331 - 1.75 x 17.25 x 17.25 1RU • ISR4351 - 3.5 x 17.25 x 18.5 2RU • ISR4431 - 1.73 x 17.25 x 19.97 1RU • ISR4451-X - 3.5 x 17.25 x 18.5 2RU • ISR4461 - 5.2 x 17.25 x 18.5 3RU **Interfaces** • 1 Serial console port RJ45 ISR4321 • 2 10/100/1000 WAN or LAN ports • Aggregate Throughput: 50 to 100 Mbps • 2 RJ-45 ports • 1 SFP-based ports • 2 NIM slots • 1 USB 2.0 (Type A) • 4/8 Default /maximum flash memory GB ISR4331 • 3 10/100/1000 ports • Aggregate Throughput: 100 to 300 Mbps • 2 RJ-45 ports • 2 SFP-based ports • 2 NIM slots • 1 USB 2.0 (Type A) • 4/16Default /maximum flash memory GB ISR4351 • 3 10/100/1000 ports • Aggregate Throughput: 200 to 400 Mbps • 3 RJ-45 ports

Hardware	Processor	Features
		• 3 SFP-based ports • 3 NIM slots • 2 USB 2.0 (Type A) • 4/16 Default /maximum flash memory GB ISR4431 • 4 10/100/1000 ports • Aggregate Throughput: 500 Mbps to 1 Gbps • 4 RJ-45 ports • 4 SFP-based ports • 3 NIM slots • 2 USB 2.0 (Type A) • 8/32 Default /maximum flash memory GB ISR4451-X • 4 10/100/1000 ports • Aggregate Throughput: 2 Gbps • 4 RJ-45 ports • 4 SFP-based ports • 3 NIM slots • 2 USB 2.0 (Type A) • 8/32 Default /maximum flash memory GB ISR4461 • 4 10/100/1000 ports • Aggregate Throuput: 1 to 3 Gbps • 2 RJ-45 ports • 4 SFP-based ports • 3 NIM slots • 2 USB 2.0 (Type A) • 8/32 Default /maximum flash memory GB
C8300-1N1S-6T C8300-1N1S-4T2X C8300-2N2S-6T C8300-2N2S-4T2X NIMs: C-NIM-1X  	C8300-1N1S-6T • Intel Xeon D-1563N (Broadwell) • MACsec - Broadcom BCM8275 C8300-1N1S-4T2X • Intel Xeon D-1573N (Broadwell) • MACsec - Broadcom BCM8275 C8300-2N2S-6T • Intel Xeon D-2148NT (Skylake) • MACsec - Broadcom BCM8275 C8300-2N2S-4T2X • Intel Xeon D-2168NT (Skylake)	**Physical dimensions** (H x W x D in.) • C8300-1N1S-6T - 1.71 x 17.3 x 16.5 1RU • C8300-1N1S-4T2X – 1.71 x 17.3 x 16.5 1RU • C8300-2N2S-6T - 3.5 x 17.25 x 18.52 2RU • C8300-2N2S-4T2X - 3.5 x 17.25 x 18.52 2RU **Interfaces** C8300-1N1S-6T • 1 SM • 1 NIM Slots • 6 x 1-Gigabit Ethernet Ports • 8GB DRAM • 16GB Storage C8300-1N1S-4T2X • 1 SM

Hardware	Processor	Features
 	• MACsec - Broadcom BCM8275	• 1 NIM Slots • 2 x 10-Gigabit Ethernet • 4 x 1-Gigabit Ethernet Ports • 8GB DRAM • 16GB Storage C8300-2N2S-6T • 2 SM • 2 NIM Slots • 6 x 1-Gigabit Ethernet Ports • 8GB DRAM • 16GB Storage C8300-2N2S-4T2X • 2 SM • 2 NIM Slots • 2 x 10-Gigabit Ethernet • 4 x 1-Gigabit Ethernet Ports • 8GB DRAM • 16GB Storage
C8500-12X4QC C8500-12X  	C8500-12X • Intel Xeon D-1563N (Broadwell) • MACsec - Broadcom BCM8275 • (embedded) C8500-12X4QC • Intel Xeon D-1563N (Broadwell) • MACsec - Broadcom BCM8275 • MACsec - CoMIRA Mentor Questa Sim 10.7	**Physical dimensions** (H x W x D in.) • 1.73 x 17.50 x 18.46 1RU **Interfaces** C8300-12X4QC • 12 1/10GE ports • 40GE ports • 40/100GE ports (max 240G) C8300-12X • 12x 1/10GE ports

4 Security Policy

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
- Packet Filtering
- 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 RFCs of the NDcPP v2.2e, MOD_VPNGW v1.1 and MACSECEPv1.2 as necessary to satisfy testing/assurance measures prescribed therein.

4.1.1 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 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.

4.1.2 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. The TOE leverages the IOS Common Cryptographic Module (IC2M) Rel5 (see Table 3 for certificate references).

Table 3 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) AES Key Wrap and CMAC (128, 256)	IC2M	A1462	FCS_COP.1/DataEncryption FCS_COP.1(1) FCS_COP.1(2)
			Crypto HW Module (ASR1000HX)	2346	

Algorithm	Description	Supported Mode	Module	CAVP Cert. #	SFR
		GCM (128, 256)	MACSec	3504 3505 3160 4550 C1668	
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 software integrity test	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
KAS-FFC-SSC	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 4 below:

Table 4 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. Used for random number generation, key generation and seeds to asymmetric key generation
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. Used to encrypt MACsec traffic
HMAC	Used for keyed hash, integrity services in IPsec and SSH session establishment.
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

Cryptographic Method	Use within the TOE
ECC DH	Used as the Key exchange method for IPsec

The TOE authenticates and encrypts packets between itself and a MACsec peer. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys to protect data exchanged by the peers.

4.1.3 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 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.

4.1.4 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.

4.1.5 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.

The TOE is also capable of rejecting any MACsec PDUs in a given session that contain a SCI that is different from the one that is used to establish that session. The SCI is derived from the MACsec peer's MAC address and port to uniquely identify the originator of the MACsec PDU. Only EAPOL (PAE EtherType 88-8E) and MACsec frames (EtherType 88-E5) are permitted in the MACsec communication between peers and others are discarded.

4.1.6 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 is also able to detect replay of information received via secure channels (MACsec). The detection applied to network packets that terminate at the TOE, such as trusted communications between the TOE and an IT entity (e.g., MACsec peer). If replay is detected, the packets are discarded.

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.

4.1.7 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" 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.

4.1.8 Trusted path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 which has the ability to be encrypted further using IPsec, 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.

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.

Table 5 TOE 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 or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does 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. For vNDs, this assumption applies to the physical platform on which the VM runs.
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 computing platform for general purpose applications (unrelated to networking functionality). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
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 ND cPP and PP-Modules. 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

Assumption	Assumption Definition
	expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
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.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.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. This assumption defines the TOE's placement in a network such that it is able to perform its required security functionality. The Base-PP does not define any assumptions about the TOE's architectural deployment so there is no conflict here. The operational environment objective OE.CONNECTIONS is realized through A.CONNECTIONS.

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.

Table 6 Threats

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the Network Device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its

Threat	Threat Definition
	entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself. An attacker may acquire sensitive TOE or user data that is transmitted to or from the TOE because an untrusted communication channel causes a disclosure of data in transit.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

Threat	Threat Definition
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.NETWORK_DISCLOSURE	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If known malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of a phishing episode or by inadvertent responses to email messages), then those internal devices may be susceptible to the unauthorized disclosure of information. From an infiltration perspective, VPN gateways serve not only to limit access to only specific destination network addresses and ports within a protected network, but whether network traffic will be encrypted or transmitted in plaintext. With these limits, general network port scanning can be prevented from reaching protected networks or machines, and access to information on a protected network can be limited to that obtainable from specifically configured ports on identified network nodes (e.g., web pages from a designated corporate web server). Additionally, access can be limited to only specific source addresses and ports so that specific networks or network nodes can be blocked from accessing a protected

Threat	Threat Definition
	network thereby further limiting the potential disclosure of information. From an exfiltration perspective, VPN gateways serve to limit how network nodes operating on a protected network can connect to and communicate with other networks limiting how and where they can disseminate information. Specific external networks can be blocked altogether or egress could be limited to specific addresses and/or ports. Alternately, egress options available to network nodes on a protected network can be carefully managed in order to, for example, ensure that outgoing connections are encrypted to further mitigate inappropriate disclosure of data through packet sniffing.
T.NETWORK_MISUSE	Devices located outside the protected network, while permitted to access particular public services offered inside the protected network, may attempt to conduct inappropriate activities while communicating with those allowed public services. Certain services offered from within a protected network may also represent a risk when accessed from outside the protected network. From an ingress perspective, it is generally assumed that entities operating on external networks are not bound by the use policies for a given protected network. Nonetheless, VPN gateways can log policy violations that might indicate violation of publicized usage statements for publicly available services. From an egress perspective, VPN gateways can be configured to help enforce and monitor protected network use policies. As explained in the other threats, a VPN gateway can serve to limit dissemination of data, access to external servers, and even disruption of services – all of these could be related to the use policies of a protected network and as such are subject in some regards to enforcement. Additionally, VPN gateways can be configured to log network usages that cross between protected and external networks and as a result can serve to identify potential usage policy violations.
T.REPLAY_ATTACK	If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a "replay" attack. This method of attack allows the individual to capture packets traversing throughout the network and send the packets at a later time, possibly unknown by the intended receiver. Traffic is subject to replay if it meets the following conditions: • Cleartext: an attacker with the ability to view unencrypted traffic can identify an appropriate segment of the communications to replay as well in order to cause the desired outcome. • No integrity: alongside cleartext traffic, an attacker can make arbitrary modifications to captured traffic and replay it to cause the desired outcome if the recipient has no means to detect these.

Threat	Threat Definition
T.DATA_INTEGRITY	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external devices are able to communicate with devices on the protected network or if devices on the protected network can communicate with those external devices then the data contained within the communications may be susceptible to a loss of integrity. An attacker may modify data transmitted over the MACsec channel in a way that is not detected by the recipient.
T.NETWORK_ACCESS	Devices located outside the protected network may seek to exercise services located on the protected network that are intended to only be accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network. Devices located outside the protected network may, likewise, offer services that are inappropriate for access from within the protected network. From an ingress perspective, VPN gateways can be configured so that only those network servers intended for external consumption by entities operating on a trusted network (e.g., machines operating on a network where the peer VPN gateways are supporting the connection) are accessible and only via the intended ports. This serves to mitigate the potential for network entities outside a protected network to access network servers or services intended only for consumption or access inside a protected network. From an egress perspective, VPN gateways can be configured so that only specific external services (e.g., based on destination port) can be accessed from within a protected network, or moreover are accessed via an encrypted channel. For example, access to external mail services can be blocked to enforce corporate policies against accessing uncontrolled e-mail servers, or, that access to the mail server must be done over an encrypted link. An attacker may send traffic through the TOE that enables them to access devices in the TOE's Operational Environment without authorization.

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 Version 2.2e, PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 and Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSECEP) Version 1.2.

- Consistent with the expectations of the Protection Profile, 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.
- Section 7.2 describes features explicitly excluded from the evaluation.
- As clarified in Section 1.6 of the ST, the evaluated devices were tested with a dedicated LAN/MGMT port, WAN port, and an RJ45 serial port for local console connectivity.

6 Documentation

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

- Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 4000 Series (ISR4K) and Cisco Catalyst 8300 and 8500 Series Edge Routers (Cat8300, Cat8500) running IOS XE Version 1.3 CC Configuration Guide, Version 1.0.

Only the CC Configuration Guide and the sections explicitly referenced by the Guide in the following table should be trusted to configure, administer, or use the TOE in its evaluated configuration:

#	Title	Link
[1]	Loading and Managing System Images Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sys-image-mgmt/configuration/xe-17-1/sysimgmgmt-xe-17-1-book.html
[2]	Cisco ASR 1000 Series Router Hardware Installation Guide Hardware Installation Guide for the Cisco 4000 Series Integrated Services Router Hardware Installation Guide for Cisco Catalyst 8300 Series Edge Platforms Cisco Catalyst 8500 Series Edge Platforms Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/routers/asr1000/install/guide/asr1routers/asr-1000-series-hig.html https://www.cisco.com/c/en/us/td/docs/routers/access/4400/hardware/installation/guide4400-4300/C4400_isr.html https://www.cisco.com/c/en/us/td/docs/routers/cloud_edge/c8300/hardware_installation/b-catalyst-8300-series-edge-platforms-hig/m-overview.html https://www.cisco.com/c/en/us/td/docs/routers/cloud_edge/c8500/hardware-installation-guide/b_C8500_HIG/m_Router_Overview.html
[3]	Configuration Fundamentals Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/xe-17/fundamentals-xe-17-book.html
[4]	Basic System Management Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/configuration/xe-17/bsm-xe-17-book.html
[5]	RADIUS Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_rad/configuration/xe-17/sec-usr-rad-xe-17-book.html

[6]	Using Setup Mode to Configure a Cisco Networking Device	http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/15-s/fundamentals-15-s- book.html
[7]	FlexVPN and Internet Key Exchange Version 2 Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/xe-17/sec-flex-vpn-xe-17-book/sec-intro-ikev2-flex.html
[8]	Cisco IOS Security Command Reference: Commands A to C	http://www.cisco.com/en/US/docs/ios-xml/ios/security/a1/sa1-cr-book.html
	Cisco IOS Security Command Reference: Commands D to L	http://www.cisco.com/en/US/docs/ios-xml/ios/security/d1/sd1-cr-book.html
	Cisco IOS Security Command Reference: Commands M to R	http://www.cisco.com/en/US/docs/ios-xml/ios/security/m1/sm1-cr-book.html
	Cisco IOS Security Command Reference: Commands S to Z	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-cr-book.html
[9]	Public Key Infrastructure Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-17/sec-pki-xe-17-book.html
[10]	Security Configuration Guide: Zone-Based Policy Firewall	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_zbf/configuration/xe-16/sec-data-zbf-xe-16-book.html#GUID-BAA34ACF-595E-473D-B82C-605E93D954D1
[11]	SSL VPN Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_sslvpn/configuration/15-mt/sec-conn-sslvpn-15-mt-book/sec-conn-sslvpn-ssl-vpn.html
[12]	Cisco IOS Configuration Fundamentals Command Reference	http://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/command/Cisco_IOS_Configuration_Fu ndamentals_Command_Reference.html

[13]	Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide Cisco 4000 Series ISRs Software Configuration Guide Cisco Catalyst 8300 Series Edge Platforms Software Configuration Guide Cisco Catalyst 8500 Series Edge Platforms Software Configuration Guide	https://www.cisco.com/c/en/us/td/docs/routers/asr1000/configuration/guide/chassis/asr1000-software-config-guide.html https://www.cisco.com/c/en/us/td/docs/routers/access/4400/software/configuration/guide/isr4400swcfg.html https://www.cisco.com/c/en/us/td/docs/routers/cloud_edge/c8300/software_config/cat8300swcfg-xe-17-book.html https://www.cisco.com/c/en/us/td/docs/routers/cloud_edge/c8500/software-configuration-guide/c8500-software-config-guide.html
[14]	IP Addressing: NAT Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-17-1/nat-xe-17-x-book.html
[15]	Secure Shell Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_ssh/configuration/xe-17/sec-usr-ssh-xe-17-book.html
[16]	MACsec and MKA Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-17/macsec-xe-17-book.html

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The evaluated configuration consists of the hardware, software, and firmware described in this section when configured in accordance with the documentation identified in Section 6.

The exact tested configuration is explained in full detail in Section 4 of the Assurance Activity Report.

7.1.1 Cisco Aggregation Services Router 1000 Series (ASR1K)

The TOE consists of one or more physical devices and includes Cisco IOS-XE version 17.3 software. The ASR1K hardware models included in this evaluation are the ASR1001-X, ASR1001-HX, ASR1002-HX, ASR1006-X, ASR1009-X, and ASR1013 with supporting MACsec hardware ASR1000-MIP100, EPA-18X1GE, EPA-10X10GE, EPA-1X100GE, EPA-CPAK-2X40GE, EPA-1X100GE QSFP+, EPA-2X40GE QSFP+, and EPA-1X40GE QSFP+. Table adds additional details on the physical characteristics of the models. 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.

7.1.2 Cisco Integrated Services Router 4000 Series (ISR4K)

The TOE consists of one or more physical devices and includes Cisco IOS-XE version 17.3 software. The hardware models included in the evaluation are the ISR4321, ISR4331, ISR4351, ISR4431, ISR4451-X, ISR4461 with MACsec network interface modules (NIM): NIM-1GE-CU-SFP and NIM-2GE-CU-SFP. 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.

7.1.3 Cisco Catalyst 8300 Series Edge Routers (Cat8300)

The TOE consists of one or more physical devices and includes Cisco IOS-XE version 17.3 software. The Cat8300 hardware models included in this evaluation are the CAT8300-1N1S-6T (1-RU), CAT8300-1N1S-4T2X (1-RU), CAT8300-2N2S-6T (2-RU), CAT8300-2N2S-4T2X (2-RU).

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.

7.1.4 Cisco Catalyst 8500 Series Edge Routers (Cat8500)

The TOE consists of one physical device and includes Cisco IOS-XE version 17.3 software. The hardware models included in the evaluation are the C8500-12X4QC, C8500-12X. 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 devices are considered to be in the TOE's Environment:

- VPN Peer
- MACSec Peer
- Management Workstation
- Radius AAA (Authentication) Server
- Audit (Syslog) Server
- Local Console
- Certificate Authority (CA)

7.2 Excluded Functionality

The following functionality is excluded from the evaluation:

Table 7 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.
USB console port	The USB console port is not associated with the Security Functional Requirements claimed in [NDcPP].

These services will be disabled by configuration settings. The exclusion of this functionality does not affect compliance to the NDcPP v2.2e, MOD_VPNGW v1.1 and MACSECEP v1.2. Note that while the evaluated RJ-45 console interface is in use, USB console port functionality (if present on the device) is disabled.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 4000 Series (ISR4K) and Cisco Catalyst 8300 and 8500 Series Edge Routers (Cat8300, Cat8500) running IOS XE Version 17.3 Target of Evaluation (TOE). which is not publicly available. The Assurance Activities Report 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 the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Devices Version 2.2e, PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 and Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSECEP) Version 1.2. The Independent Testing activity, Test Configurations and associated Test Tools are identified in Section 4.1 and 4.2 of the Assurance Activity Report.

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 Evaluation Technical Report (ETR). The reader of this document can assume that 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 4 and CEM version 3.1 rev 4. The evaluation determined the Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 4000 Series (ISR4K) and Cisco Catalyst 8300 and 8500 Series Edge Routers (Cat8300, Cat8500) running IOS XE Version 17.3 to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP, VPNGW, and MACSECEP.

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 Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 4000 Series (ISR4K) and Cisco Catalyst 8300 and 8500 Series Edge Routers (Cat8300, Cat8500) 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 Version 2.2e, PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 and Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSECEP) Version 1.2.

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 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's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices Version 2.2e, PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 and Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSECEP) Version 1.2 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 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 Version 2.2e, PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 and Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSECEP) Version 1.2 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 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 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 Version 2.2e, PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 and Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSECEP) Version 1.2 and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

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 Version 2.2e, PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 and Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSECEP) Version 1.2 and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and uncovered three vulnerabilities and their mitigation which is summarized in section 7.6 of the AAR which includes the search terms, databases, and search dates. The mitigations for the three vulnerabilities are summarized as follows:

- CVE-2021-1621 requires an adjacent physical attacker to create the DoS conditioned as explained in the CVE details. The TOE is not remotely exploitable by adversaries. This is further supported by A.PHYSICAL_PROTECTION and A.TRUSTED_ADMINISTRATOR as the only entities assumed to be able to carry out a physical attack on the TOE are also assumed to be trusted.
- CVE-2021-1616 is mitigated by a workaround which has been published in the AGD.
- CVE-2021-1446 is mitigated by a workaround which has been published in the AGD.

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 Version 2.2e and PP-Module for Virtual Private Network (VPN) Gateways 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 Version 2.2e, PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 and Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSECEP) Version 1.2, 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 Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 4000 Series (ISR4K) and Cisco Catalyst 8300 and 8500 Series Edge Routers (Cat8300, Cat8500) running IOS XE Version 1.3 CC Configuration Guide, Version 1.0 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.

11 Annexes

Not applicable.

12 Security Target

Cisco Aggregation Services Router 1000 Series (ASR1K), Cisco Integrated Services Router 4000 Series (ISR4K) and Cisco Catalyst 8300 and 8500 Series Edge Routers (Cat8300, Cat8500) running IOS XE Version 17.3 Security Target, Version 1.2.

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.