

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report for the
**Cisco Catalyst 8200 and 8500 Series Edge Routers (Cat8200,
Cat8500)**

Report Number: CCEVS-VR-VID11331-2023

Dated: 3/29/2023

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, Ph. D.
Jerome Myers, Ph. D.

The Aerospace Corporation

Common Criteria Testing Laboratory

Rahul Joshi
Snehal Raghunath Gaonkar

Acumen Security, LLC

Table of Contents

1 Executive Summary 5

2 Identification 7

3 Architectural Information 8

4 Security Policy..... 9

4.1 Security Audit9

4.2 Cryptographic Support9

4.3 Identification and Authentication12

4.4 Security Management13

4.5 Packet Filtering.....13

4.6 Protection of TSF14

4.7 TOE Access14

4.8 Trusted path/Channels.....14

5 Assumptions, Threats & Clarification of Scope 15

5.1 Assumptions15

5.2 Threats.....16

5.3 Clarification of Scope21

6 Documentation 22

7 Evaluated Configuration..... 23

7.1 Evaluated Configuration.....23

7.1.1 Cisco Catalyst 8200 Series Edge Routers (Cat8200)23

7.1.2 Cisco Catalyst 8500 Series Edge Routers (Cat8500)23

7.2 Excluded Functionality25

8 Product Testing..... 26

8.1 Developer Testing26

8.2 Evaluation Team Independent Testing.....26

9 Results of the Evaluation 27

9.1 Evaluation of Security Target27

9.2 Evaluation of Development Documentation27

9.3 Evaluation of Guidance Documents28

9.4 Evaluation of Life Cycle Support Activities28

9.5 Evaluation of Test Documentation and the Test Activity28

9.6 Vulnerability Assessment Activity29

9.7 Summary of Evaluation Results30

10 Validator Comments & Recommendations 31

11 Annexes..... 32

12 Security Target 33

13 Glossary 34

14 Bibliography..... 35

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 Catalyst 8200 and 8500 Series Edge Routers running IOS-XE 17.6 Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in March 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of:

- Collaborative Protection Profile for Network Devices (CPP_ND_V2.2E)
- Network Device Protection Profile Extended Package MACsec Ethernet Encryption (PP_NDCPP_MACSEC_EP_V1.2)
- Virtual Private Network (VPN) Gateways (MOD_VPNGW_v1.1).

The following NIAP Technical Decisions are applicable to the claimed Protection Profile and Modules:

- TD0652: MACsec CAK Lifetime in FMT_SMF.1
- TD0638: NIT Technical Decision for Key Pair Generation for Authentication
- TD0632: NIT Technical Decision for Consistency with Time Data for vNDs
- TD0631: NIT Technical Decision for Clarification of public key authentication for SSH Server
- TD0618: MACsec Key Agreement and conditional support for group CAK
- TD0597: VPN GW IPv6 Protocol Support
- TD0592: NIT Technical Decision for Local Storage of Audit Records
- TD0590: Mapping of operational environment objectives
- TD0581: NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3
- TD0580: NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e
- TD0572: NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers
- TD0571: NiT Technical Decision for Guidance on how to handle FIA_AFL.1

- TD0570: NiT Technical Decision for Clarification about FIA_AFL.1
- TD0564: NiT Technical Decision for Vulnerability Analysis Search Criteria
- TD0563: NiT Technical Decision for Clarification of audit date information
- TD0553: FCS_MACSEC_EXT.1.4 and MAC control frames
- TD0549: Consistency of Security Problem Definition update for MOD_VPNGW_v1.0 and MOD_VPNGW_v1.1
- TD0547: NIT Technical Decision for Clarification on developer disclosure of AVA_VAN
- TD0538: The NIT has issued a technical decision for Outdated link to allowed-with list
- TD0536: The NIT has issued a technical decision for Update Verification Inconsistency
- TD0527: Updates to Certificate Revocation Testing (FIA_X509_EXT.1)
- TD0509: Correction to MACsec Audit
- TD0487: Correction to Typo in FCS_MACSEC_EXT.4
- TD0466: Selectable Key Sizes for AES Data Encryption/Decryption
- TD0273: Rekey after CAK expiration
- TD0190: FPT_FLS.1(2)/SelfTest Failure with Preservation of Secure State and Modular Network Devices

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory (CCTL) using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the Protection Profile (PP). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

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

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

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

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Cisco Catalyst 8200 and 8500 Series Edge Routers (Cat8200, Cat8500) IOS-XE 17.6
Protection Profile	Collaborative Protection Profile for Network Devices (CPP_NDV2.2E), Network Device Protection Profile Extended Package MACsec Ethernet Encryption (PP_NDCPP_MACSecEP V1.2), Virtual Private Network (VPN) Gateways (MOD_VPNGW_V1.1)
Security Target	Cisco Catalyst 8200 and 8500 Series Edge Routers (Cat8200, Cat8500) Security Target Version 0.6, February 2, 2023
Evaluation Technical Report	Evaluation Technical Report for Cisco Catalyst 8200 and 8500 Series Edge Routers (Cat8200, Cat8500) IOS-XE 17.6 Version 1.1, March 21, 2023
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	DeRon Graves Patrick Mallett Jerome Myers



3 Architectural Information

The Cisco Catalyst 8200 and 8500 Series Edge Routers are purpose-built, routing platforms that includes VPN functionality and MACsec encryption provided by the Cisco IOS-XE software. The Cat8200 and Cat8500 provide IPsec connection capabilities to facilitate secure communications with external entities as required. The TOE is comprised of both software and hardware. The Cisco IOS-XE version 17.6 software is used to meet all the requirements as specified in this document regardless of the hardware platform.

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 TOE includes the hardware models as defined in Table 2.

Table 2: Hardware Models and Specifications

Hardware	Processor	Features
C8200-1N-4T C8200L-1N-4T NIM: C-NIM-2T 	C8200-1N-4T <ul style="list-style-type: none"> Intel Xeon D-1563N (Broadwell) C8200L-1N-4T <ul style="list-style-type: none"> Intel Xeon D-1573N (Broadwell) C-NIM-2T <ul style="list-style-type: none"> MACsec - Broadcom BCM54194 	Physical dimensions (H x W x D in.) <ul style="list-style-type: none"> 1.71 x 17.3 x 16.5 1RU Interfaces C8200-1N-4T <ul style="list-style-type: none"> 1 NIM Slot 4x 1-Gigabit Ethernet Ports (2x SFP, 2x RJ45) C8200L-1N-4T <ul style="list-style-type: none"> 1 NIM Slot 4x 1-Gigabit Ethernet Ports (2x SFP, 2x RJ45) C-NIM-2T <ul style="list-style-type: none"> 2x 1-Gigabit Ethernet Ports
C8500L-8S4X 	<ul style="list-style-type: none"> Intel Xeon D-2168NT (Skylake) MACsec - Broadcom BCM82757/BCM54194 	Physical dimensions (H x W x D in.) <ul style="list-style-type: none"> 1.73 x 17.50 x 18.46 1RU Interfaces <ul style="list-style-type: none"> 4x 1/10GE ports 8x 1GE ports

4 Security Policy

The TOE is comprised of the following security features:

- 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 CPP_ND_V2.2E, MOD_VPNGW_V1.1 and PP_NDCPP_MACSEC_EP_V1.2 as necessary to satisfy testing/assurance measures prescribed therein.

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. Audit logs are backed up over an encrypted channel to an external audit server.

4.2 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have Cryptographic Algorithm Validation Program (CAVP) certificates for all processors listed in ST. The TOE leverages the IOS Common Cryptographic Module (IC2M) Rel5a (see Table 3 for certificate references).

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.

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.

Table 3. FIPS References

Algorithm	Description	Supported Mode	Module	CAVP Cert. #	SFR
AES	Used for symmetric encryption/decryption	CBC (128, 192 and 256)	IC2M	A1462	FCS_COP.1/DataEncryption FCS_COP.1(1)/KeyedHashCMAC FCS_COP.1(2)
		GCM (128, 192 and 256)			
		AES Key Wrap and CMAC (128, 256)			
		GCM (128, 256)	MACSec	4544 4550	
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

Algorithm	Description	Supported Mode	Module	CAVP Cert. #	SFR
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

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.

Cryptographic Method	Use within the TOE
RSA	Used in IKE protocols peer authentication Used to provide cryptographic signature services
ECDSA	Used to provide cryptographic signature services Used in Cryptographic Key Generation Used as the Key exchange method for IPsec
FFC DH	Used as the Key exchange method for SSH and IPsec
ECC DH	Used as the Key exchange method for IPsec

4.3 Identification and Authentication

The TOE performs two types of authentications: 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 TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec connections. 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.

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. 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.

4.6 Protection of 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 are 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" 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 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 4. TOE Assumptions

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	<p>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.</p>
A.LIMITED_FUNCTIONALITY	<p>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).</p> <p>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.</p>
A.NO_THRU_TRAFFIC_PROTECTION	<p>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).</p>
A.TRUSTED_ADMINISTRATOR	<p>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</p>

Assumption	Assumption Definition
	<p>entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.</p> <p>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).</p>
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	<p>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.</p> <p>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.</p> <p>The operational environment objective OE.CONNECTIONS is realized through A.CONNECTIONS.</p>

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 5. 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 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	<p>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.</p> <p>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.</p>
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.

Threat	Threat Definition
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.
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 includes 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	<p>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.</p> <p>From an infiltration perspective, VPN gateways serve</p>

Threat	Threat Definition
	<p>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 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.</p>
T.NETWORK_MISUSE	<p>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.</p>

Threat	Threat Definition
T.REPLAY_ATTACK	<p>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:</p> <ul style="list-style-type: none"> • 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.
T.DATA_INTEGRITY	<p>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.</p> <p>An attacker may modify data transmitted over the MACsec channel in a way that is not detected by the recipient.</p>
T.NETWORK_ACCESS	<p>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.</p> <p>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.</p> <p>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</p>

Threat	Threat Definition
	<p>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.</p> <p>An attacker may send traffic through the TOE that enables them to access devices in the TOE's Operational Environment without authorization.</p>

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 (CPP_ND_V2.2e), Network Device Protection Profile Extended Package MACsec Ethernet Encryption (PP_NDCPP_MACSEC_EP_V1.2), Virtual Private Network (VPN) Gateways (MOD_VPNGW_V1.1).
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security-related functional capabilities included in the product were not covered by this evaluation.

Non-FIPS 140-2 mode of operation functionality is excluded from the evaluation This mode of operation includes non-FIPS allowed operations. This service 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.

6 Documentation

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

- Cisco Catalyst 8200 and 8500 Series Edge Routers (Cat8200, Cat8500) CC Configuration Guide, Version 1.0. March 28, 2023
- MACSEC and MKA Configuration Guide, Cisco IOS XE 17, 2/17/2023.

Note: Only the Guides listed above, and the specific sections of the other documents referenced by that guide should be trusted for the installation, administration, and use of this product in its evaluated configuration.

7 Evaluated Configuration

7.1 Evaluated Configuration

The evaluated configuration consists of the following hardware and software described in the following sections when configured in accordance with the documentation specified in Section 6.

7.1.1 Cisco Catalyst 8200 Series Edge Routers (Cat8200)

The TOE consists of one or more physical device as specified in Figure 1 below and includes Cisco IOS-XE version 17.6 software. The Cat8200 hardware models included in this evaluation are the C8200-1N-4T, C8200L-1N-4T. Table 2 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 Catalyst 8500 Series Edge Routers (Cat8500)

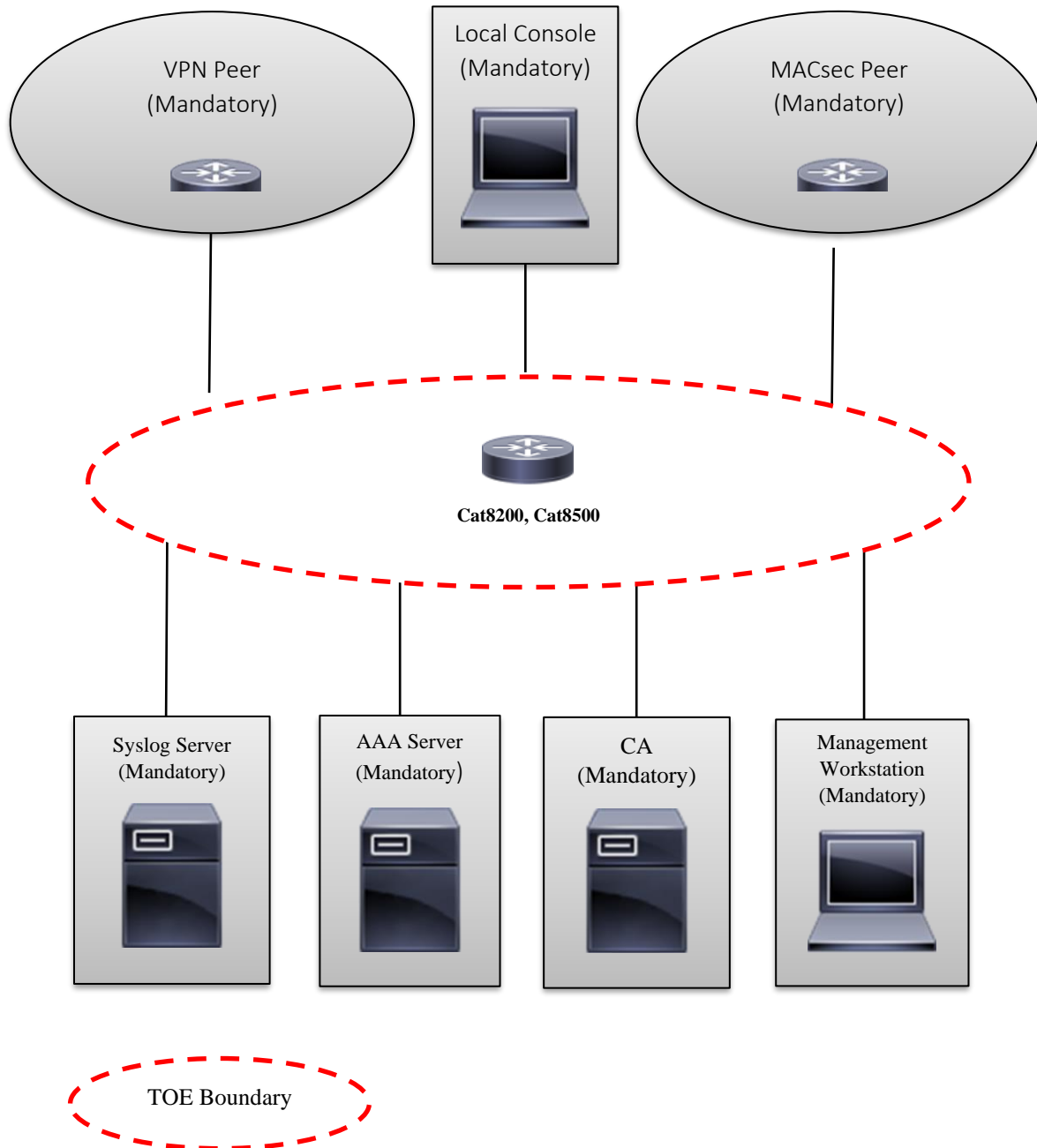
The TOE consists of one physical device as specified in Figure 1 below and includes Cisco IOS-XE version 17.6 software. The hardware model included in the evaluation is the C8500L-8S4X. Table 2 adds additional details on the physical characteristics of the two models. The TOE has two or more network 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.

Note: The interfaces tested include a dedicated LAN/MGMT connection, a dedicated WAN connection, and an RJ45 serial console connection.

The Figure 1 includes the following:

- Examples of TOE models
- The following are considered to be in the IT Environment:
 - VPN Peer
 - MACSec Peer
 - Management Workstation
 - Radius AAA (Authentication) Server
 - Audit (Syslog) Server
 - Local Console
 - Certificate Authority (CA)

Figure 1 TOE Example Deployment for Cat8200, Cat8500



NOTE: While the previous figure includes several non-TOE IT environment devices, the TOE is only the Cat8200 and Cat8500 devices. Only one TOE device is required for deployment of the TOE in the evaluated configuration.

7.2 Excluded Functionality

The following functionality is excluded from the evaluation:

Table 6. Excluded Functionality

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

These services will be disabled by configuration settings. The exclusion of this functionality does not affect compliance to the CPP_ND_V2.2e, MOD_VPNGW_v1.1 and PP_NDCPP_MACSEC_EP_V1.2.

8 Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in ETR for Cisco Catalyst 8200 and 8500 Series Edge Routers running IOS-XE 17.6, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the Collaborative Protection Profile for Network Devices (CPP_ND_V2.2e), Network Device Protection Profile Extended Package MACsec Ethernet Encryption (PP_NDCPP_MACSec_EP_V1.2), Virtual Private Network (VPN) Gateways (MOD_VPNGW_V1.1). The specific Independent Testing activity, configurations, and test tools are documented in the AAR Section 3, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the ETR. The reader of this document can assume that all activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 Rev. 5 and CEM version 3.1 Rev.5. The evaluation determined the TOE Name to be Part 2 extended, and meets the SFRs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco Catalyst 8200 and 8500 Series Edge Routers running IOS-XE 17.6 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 (CPP_ND_V2.2e), Network Device Protection Profile Extended Package MACsec Ethernet Encryption (PP_NDCPP_MACSec_EP_V1.2), Virtual Private Network (VPN) Gateways (MOD_VPNGW_V1.1).

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the Collaborative Protection Profile for Network Devices (CPP_ND_V2.2e), Network Device Protection Profile Extended Package MACsec Ethernet Encryption (PP_NDCPP_MACSec_EP_V1.2), Virtual Private Network (VPN) Gateways (MOD_VPNGW_V1.1) related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each AGD_OPE.1 and AGD_PRE.1 CEM work units. 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 (CPP_ND_V2.2e), Network Device Protection Profile Extended Package MACsec Ethernet Encryption (PP_NDCPP_MACSec_EP_V1.2), Virtual Private Network (VPN) Gateways (MOD_VPNGW_V1.1) related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each ALC_CMC.1 and ALC_CMS.1 CEM work units. 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_IND.1 CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the Collaborative Protection Profile for Network Devices (CPP_ND_V2.2e), Network Device Protection Profile Extended Package MACsec Ethernet Encryption (PP_NDCPP_MACSec_EP_V1.2), Virtual Private Network (VPN) Gateways (MOD_VPNGW_V1.1) and recorded the results in a Test Report, summarized in the ETR and AAR.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the Collaborative Protection Profile for Network Devices (CPP_ND_V2.2e), Network Device Protection Profile Extended Package MACsec Ethernet Encryption (PP_NDCPP_MACSec_EP_V1.2), Virtual Private Network (VPN) Gateways (MOD_VPNGW_V1.1, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

In compliance with AVA_VAN.1, the evaluator examined sources of publicly available information to identify potential vulnerabilities in the product. The following vulnerability databases were searched:

- <https://nvd.nist.gov/vuln/search>
- <https://www.cisco.com/>
- <https://tools.cisco.com/security/center/softwarechecker.x>
- <http://nvd.nist.gov/>
- <http://www.securityfocus.com/>
- <https://www.cvedetails.com/>

The following search terms were used.

- Cisco Router
- Cisco IOS XE 17.6.1
- Cisco Network Interface Module
- Broadwell
- Skylake
- Intel Xeon D-1573N
- Intel Xeon D-1563N
- Intel Xeon D-2168NT
- C-NIM-2T
- Broadcom BCM54194
- Broadcom BCM82757
- Catalyst Series Edge Routers
- Cisco Catalyst 8200
- Cisco Catalyst 8500
- C8200-1N-4T
- C8200L-1N-4T
- C8500L-8S4X
- IOS XE MACsec

- IOS XE SSH
- IOS XE VPN
- IOS XE IPsec
- IC2M
- IOS Common Cryptographic Module
- TCP
- UDP

The vulnerability search was performed on March 20, 2023.

The evaluation did not discover any known vulnerabilities with the product.

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 (CPP_ND_V2.2e), Network Device Protection Profile Extended Package MACsec Ethernet Encryption (PP_NDCPP_MACSec_EP_V1.2), Virtual Private Network (VPN) Gateways (MOD_VPNGW_V1.1, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the guidance documents listed in Section 6. 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 Catalyst 8200 and 8500 Series Edge Routers (Cat8200, Cat8500) Security Target, Version 1.0, March 28, 2023.

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. Assurance Activity Report for Cisco Catalyst 8200 and 8500 Series Edge Routers (Cat8200, Cat8500)
2. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
4. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
5. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
6. Evaluation Technical Report for Cisco Catalyst 8200 and 8500 Series Edge Routers (Cat8200, Cat8500), Version 1.1, March 21, 2023.
7. Cisco Catalyst 8200 and 8500 Series Edge Routers (Cat8200, Cat8500) CC Configuration Guide Version 1.0, March 28, 2023.
8. Collaborative Protection Profile for Network Devices (NDcPPv2.2e), Network Device Protection Profile Extended Package MACsec Ethernet Encryption (MACSecEP V1.2), Virtual Private Network (VPN) Gateways (MOD_VPNGW_V1.1).
9. Cisco Catalyst 8200 and 8500 Series Edge Routers (Cat8200, Cat8500) Security Target, Version 1.0, March 28, 2023.