National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15

Report Number:	**CCEVS-VR-VID11637-2025**
Dated:	**29 August 2025**
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

Doug Dull

DeRon Graves

Patrick Mallett, Ph. D.

Jerome Myers, Ph. D.

The Aerospace Corporation

Jade Stewart, Ph. D.

National Information Assurance Partnership

Common Criteria Testing Laboratory

Greg McLearn

Joon Sim

Kevin Steiner

Kenji Yoshino

Lightship Security, USA

Table of Contents

List of Tables

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 solution provided by Cisco Systems, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in August 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the collaborative Protection Profile for Network Devices, Version 3.0e, PP-Module for MACsec Ethernet Encryption, Version 1.0, PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3 and Functional Package for Secure Shell, Version 1.0.

The TOE is the Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15. The TOE identified in this VR has been evaluated at a NIAP approved 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). 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 (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

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

The technical information included in this report was obtained from the Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 Security Target, Version 1.1, August 21, 2025, and analysis performed by the Validation Team.

2. Identification

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

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

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluated Product	Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15
Sponsor and Developer	Cisco Systems, Inc.
CCTL	Lightship Security USA 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.
CEM	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Item	Identifier
Protection Profile	collaborative Protection Profile for Network Devices, Version 3.0e PP-Module for MACsec Ethernet Encryption, Version 1.0 PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3 Functional Package for Secure Shell (SSH), Version 1.0
ST	Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 Security Target, Version 1.1, August 21, 2025
Evaluation Technical Report	Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 Evaluation Technical Report, v1.1, August 27, 2025
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Lightship USA: Greg McLearn, Joon Sim, Kevin Steiner, Kenji Yoshino
CCEVS Validators	Aerospace: Doug Dull, DeRon Graves, Patrick Mallett, Jerome Myers NIAP: Jade Stewart

3. Architectural Information

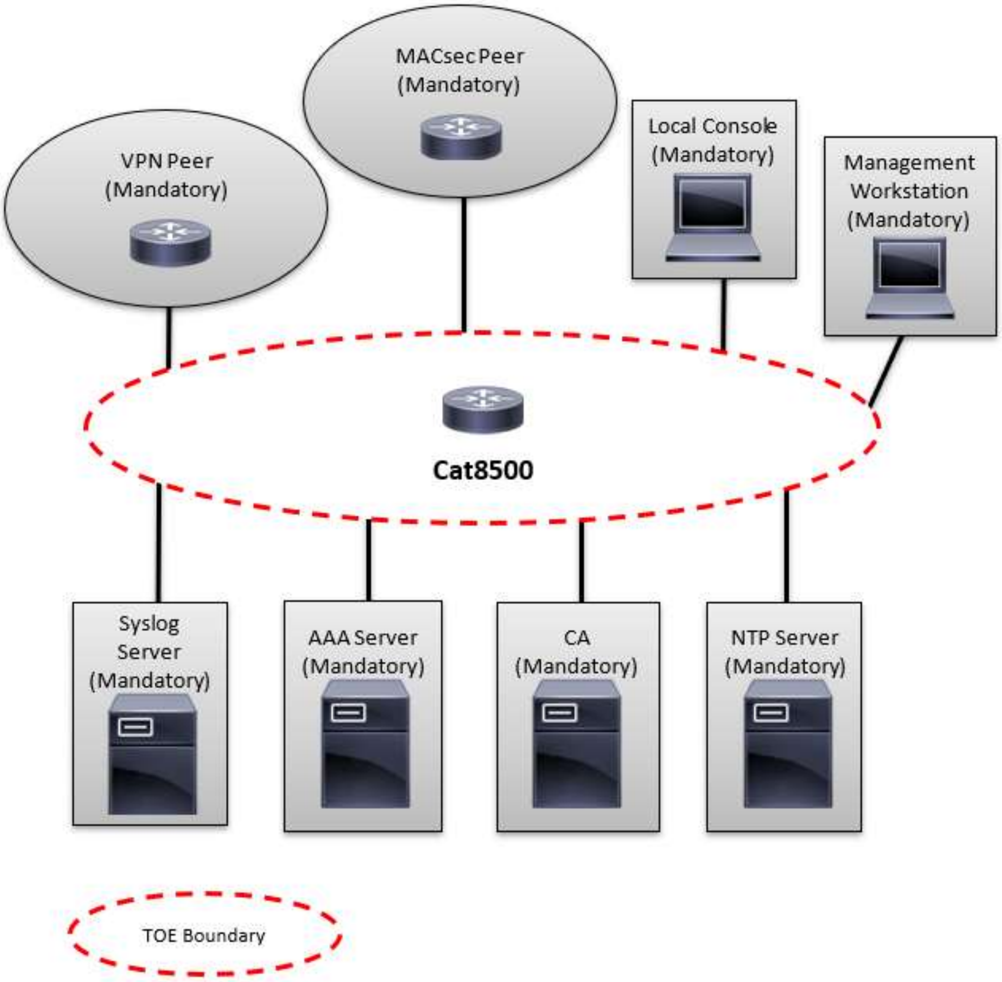
Note: The following architectural description is based on the description presented in the Security Target.

The Cat8500 Series Edge routers are purpose built for high performance and integrated services. The Cat8500 provides higher WAN port density, redundant power supply capability and have options to choose from lower and higher module density. The Cat8500 provides IPsec connection capabilities to facilitate secure communications with external entities as required. The Cat8500 is a purpose-built, routing platform that includes VPN functionality and MACsec encryption.

3.1. TOE Evaluated Configuration

The TOE consists of one physical device as specified in section 1.7 of the *Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 Security Target* and includes Cisco IOS-XE version 17.15 software. The hardware model included in the evaluation is the C8500-20X6C. Table 4 adds additional details on the physical characteristics. 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 figure provides a visual depiction of an example Cat8500 TOE deployment:



The figure above 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)
  - NTP Server

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

3.2. Physical Boundary

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

- Cat8500
  - C8500-20X6C

The network, on which they reside, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS-XE software image Release 17.15. In addition, the software image is downloadable from the Cisco web site. A login ID and password are required to download the software image. The TOE is comprised of the following physical specifications as described in the table below:

Hardware	Processor	Features
C8500-20X6C 	• Intel Xeon D-1573N (Broadwell) **MACsec** • Broadcom BCM82757 (1/10GE) • Comira MV88EC808 (40/100GE)	**Physical dimensions** 26.85” L x 17.25” W x 5.22” H 3RU **Interfaces** • 1x Serial console port RJ45 or micro USB • 2x Type A USB • 1x 1GE Management port • 20x 1/10GE SFP ports with MACsec • 6x 40/100GE SFP ports with MACsec

3.3. Supported non-TOE Hardware/ Software/ Firmware

The TOE supports the following hardware, software, and firmware in its environment when the TOE is configured in its evaluated configuration:

Component	Required	Usage/Purpose Description for TOE performance
RADIUS AAA Server	Yes	This includes any IT environment RADIUS AAA server that provides single-use authentication mechanisms. This can be any RADIUS AAA server that provides single-use authentication. The TOE correctly leverages the services provided by this RADIUS AAA server to provide single-use authentication to administrators.
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with an SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Management Workstation with IPSec Client	Yes	This includes any IT Environment Management workstation with an IPSec client installed that is used by the TOE administrator to support TOE administration over IPSec protected channels. Any IPSec client that supports IKEv2 or the appropriate IPSec protocols may be used.
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
Certificate Authority (CA)	Yes	This includes any IT Environment Certification Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.
MACsec Peer	Yes	This includes any MACsec peer with which the TOE participates in MACsec communications. It may be any device that supports MACsec communications.
Remote VPN Gateway/Peer	Yes	This includes any VPN Peer (Gateway, Endpoint, another instance of the TOE) with which the TOE participates in VPN communications. Remote VPN Peers may be any device that supports IPsec VPN communications. Another instance of the TOE used as a VPN Peer would be installed in the evaluated configuration and likely administered by the same personnel.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Also referred to as audit server in the ST.
NTP Server	Yes	The TOE supports communications with an NTP Server in order to synchronize the date and time for a reliable timestamp on the TOE.

4. Security Policy

This section summarizes the security functionality of the TOE:

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 stored in persistent memory, with a configurable maximum size. When the log reaches the configured threshold, the TOE overwrites the oldest records. 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. All the algorithms claimed have CAVP certificates for all processors listed in Table 4 in the *Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 Security Target*. The TOE leverages the IOS Common Cryptographic Module (IC2M) Rel5a (see the table below for certificate references). These cryptographic modules, including the MACsec cryptographic module, are implemented in a combination of hardware (such as the AES 4550 hardware implementation for MACsec) and firmware (such as the IC2M A1462 and C1668 implementations). The cryptographic operational environment for each of these modules is:

- Intel Xeon D-1573N (Broadwell) processor for the IOS Common Cryptographic Module (IC2M) Rel5a (A1462)
- Comira MV88EC808 for the GCM-AES Crypto Core (C1668)
- Broadcom BCM82757 for the AES ECB 128bit & 256bit Encryption/Decryption Engine (AES 4550)

SFR	Algorithm	Description	Mode	Module	Certificate
FCS_COP.1/DataEncryption	AES	Symmetric Encryption/Decryption	AES-CBC-128 AES-CBC-192 AES-CBC-256 AES-GCM-128 AES-GCM-192 AES-GCM-256	IC2M	A1462

SFR	Algorithm	Description	Mode	Module	Certificate
FCS_COP.1/Hash	SHA	Cryptographic Hashing Service	SHA-1 SHA-256 SHA-384 SHA-512	IC2M	A1462
FCS_COP.1/KeyedHash	HMAC	Keyed Hashing Service	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512 implicit	IC2M	A1462
FCS_COP.1/CMAC	AES-CMAC	Keyed-Hash Message Authentication	AES-CMAC-128 AES-CMAC-256	IC2M	A1462
FCS_COP.1/MACSEC	AES-KW	Key Wrap	AES-KW-128 AES-KW-256	IC2M	A1462
FCS_COP.1/MACSEC	AES-GCM	AEAD Symmetric Encryption/Decryption	AES-GCM-128 AES-GCM-256	MACsec	4550 C1668
FCS_COP.1/SigGen	RSA	RSA Signature Generation and Verification	PKCS #1v1.5 (2048, 3072)	IC2M	A1462
FCS_COP.1/SigGen	ECDSA	Elliptic Curve Signature Generation and Verification	P-256 P-384 P-521	IC2M	A1462
FCS_CKM.1 – Cryptographic Key Generation FCS_CKM.1/IKE – Cryptographic Key Generation	RSA	RSA Key Generation	2048 3072	IC2M	A1462
FCS_CKM.1 – Cryptographic Key Generation FCS_CKM.1/IKE – Cryptographic Key Generation	ECDSA	Elliptic Curve Key Generation	P-256 P-384	IC2M	A1462
FCS_CKM.1 – Cryptographic Key Generation FCS_CKM.1/IKE – Cryptographic Key Generation	FFC	FFC Key Generation	DH-14, DH-15, DH-16, DH-19, DH-20	IC2M	Tested by CCTL

SFR	Algorithm	Description	Mode	Module	Certificate
FCS_CKM.2 – Cryptographic Key Establishment	KAS-ECC-SSC	ECC Key Establishment	P-256 P-384	IC2M	A1462
FCS_CKM.2 – Cryptographic Key Establishment	KAS-FFC-SSC	FFC Key Establishment	DH-14, DH-15, DH-16, DH-19, DH-20	IC2M	Tested by CCTL
FCS_RBG_EXT.1– Random Bit Generation	DRBG	Deterministic Random Bit Generation Services	CTR_DRBG (AES 256)	IC2M	A1462

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 the table below:

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.
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

Cryptographic Method	**Use within the TOE**
AES	Used to encrypt IPsec session traffic. Used to encrypt SSH session traffic. Used to encrypt MACsec traffic Used to generate subkeys for CMAC
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 Used in Cryptographic Key Generation
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 IPsec
ECC DH	Used as the Key exchange method for SSH and 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 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.

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;
- NTP configurations;
- Update to the TOE and verification of the updates;
- Configuration of IPsec functionality.

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.

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), MACsec frames (EtherType 88-E5), MAC control frames EtherType 0x876F 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 has an internal clock; however, the TOE synchronizes time with an NTP server and then 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.

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.

Finally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module.

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” or “logout” command.

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

4.1.8. 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. 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. In addition, IPsec is used to secure communications between the TOE and external entities, including remote authentication servers and NTP servers (via NTPv4 over IPsec).

5. Assumptions and Clarification of Scope

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

- *collaborative Protection Profile for Network Devices, Version 3.0e*
- *PP-Module for MACsec Ethernet Encryption, Version 1.0*
- *PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3*
- *Functional Package for Secure Shell, Version 1.0*

That information has not been reproduced here and the documents referenced above should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in CPP_ND_V3.0E, MOD_MACSEC_V1.0, MOD_VPNGW_v1.3, and PKG_SSH_V1.0 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

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 in accordance with the assurance activities specified in the CPP_ND_V3.0E, MOD_MACSEC_V1.0, MOD_VPNGW_v1.3, and PKG_SSH_V1.0 and performed by the Evaluation team
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the CPP_ND_V3.0E, MOD_MACSEC_V1.0, MOD_VPNGW_v1.3, and PKG_SSH_V1.0 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

The following functionality is excluded from the evaluation:

Excluded Functionality	Exclusion Rationale

Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.
USB ports	USB ports are not used for TOE functionality

These services will be disabled by configuration settings. The exclusion of this functionality does not affect compliance to the NDcPP v3.0e, MOD_VPNGW v1.3 and MOD_MACSEC_V1.0.

6. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 Operational User Guidance and Preparative Procedures*, 1.0, August 14, 2025

Only the Administrator Guide 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. IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 Detailed Test Report*, which is not publicly available. The *Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 Assurance Activity Report,* v1.1, August 25, 2025, provides an overview of testing and the prescribed assurance activities.

7.1. Developer Testing

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

7.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing at Lightship Security USA lab in Baltimore, MD from May 2025 through August 2025. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Assurance Activities.

Each Assurance Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed. The specific test configurations and test tools utilized may be found in AAR section 24.5.

7.3. Evaluated Configuration

The evaluated configuration of the TOE consists of the following hardware and software. Hardware is the C8599-20X6C Intel Xeon D-1573N (Broadwell) processor, MACsec Broadcom BCM82757 (1/10GE) and Comira MV88EC808. Software is IOS-XE 17.15.

Devices in the test environment are listed in the Table 2.

Table 2: Devices in the Testing Environment

Name / HW / SW	Description / Functions	Test Tools
C8500-20X6C HW: C8500-20X6C SW: IOS-XE 17.15	Fully tested TOE model IPsec SSH Server MACsec Peer VPN Peer	N/A
Services VM HW: Test Hypervisor SW: Debian GNU/Linux 10 (buster)	Logging Server (UDP & IPsec) Radius Server NTP Server CRL Server IPsec Server Perform Packet Captures	syslog-ng 4.8.1 ntpd ntpsec 1.2.3 tcpdump 4.99.5 strongSwan 6.0.1 swanctl Custom build of Strongswan: strongSwan 6.0.1-Lightship freeradius 3.2.7 python 3.13.2
MACsec Node A HW: MACsec Hypervisor SW: Debian 12 with Linux kernel 6.1	MACsec Manual packet construction using Python3 and Scapy Packet captures	Custom MACsec MKPDU controller: v2.10-lightship-1.0 Custom Linux kernel modules for MPDU manipulation for FCS_MACSEC_EXT.1 Test 5 (v1.0), FCS_MACSEC_EXT.2 Test 8 (v1.0), and FCS_MKA_EXT.1 Test 12 (v1.0). Linux tc utility: iproute2-6.1.0, libbpf 1.1.0 Python 3.11.2 Scapy 2.5.0 Packet captures: tcpdump 4.99.3 Ethernet packet flooding: Lightship eth-flood v1.0
MACsec Node B HW: MACsec Hypervisor SW: Debian 12 with Linux kernel 6.1	MACsec (third peer only) Packet captures	Custom MACsec MKPDU controller: v2.10-lightship-1.0 Packet captures: tcpdump 4.99.3

Name / HW / SW	Description / Functions	Test Tools
LAN VM HW: Test Hypervisor SW: Debian GNU/Linux 10 (buster)	Packet recipient captures	Packet captures: tcpdump 4.9.3
WAN VM HW: Test Hypervisor SW: Debian GNU/Linux 10 (buster)	Packet generation Packet capture	Packet captures: tcpdump 4.9.3 scapy 2.6.1 Python2 2.7.16 Python3 3.7.3 hping3 version 3.0.0-alpha-2 sendip provided by Debian package send-ip-2.5-7+b1 OpenSSH 7.9p1 nslookup 9.11.5-P4-5.1+deb10u9-Debian netcat provided by Debian package netcat-openbsd-1.195-2
Router VM HW: Test Hypervisor SW: Debian 10	Provides NAT'ing for specific IPsec test cases.	NAT services: iptables 1.8.2 (nf_tables)
NAT'd node HW: Test Hypervisor SW: Debian 10	Provides an IPsec instance behind a NAT.	IPsec: Custom build of Strongswan: strongSwan 6.0.1-Lightship
Test Hypervisor HW: Dell PowerEdge R440 SW: ESXi, 6.7.0	Hypervisor for the various virtual machines.	None
MACsec Hypervisor HW: Dell PowerEdge R540 SW: ESXi 6.7.0	Hypervisor for the MACsec nodes	BCM57412 10G capable network card
Aruba Switch HW: Instant On 1830	Port mirrors used for physical disconnect packet captures	N/A

Name / HW / SW	Description / Functions	Test Tools
GL VM HW: Test Hypervisor SW: Kali GNU/Linux 2023.2	SSH Client (SSH) Protocol Test Host (SSH) Certification Authority Perform Packet Captures	Greenlight 3.0.35 Python 3.11.2 OpenSSL 3.0.8 OpenSSH 9.2p1 tcpdump 4.99.3
Packet Capture Laptop HW: Lenovo ThinkPad T15 SW: Windows 11 Pro	Physical disconnect packet captures for FTP_ITC.1	Wireshark 4.0.3
Serial Server HW: Raritan Dominion SX32	Serial console access over SSH	N/A

8. 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 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 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined the Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in CPP_ND_V3.0E, MOD_MACSEC_V1.0, MOD_VPNGW_v1.3, and PKG_SSH_V1.0.

8.1. Evaluation of Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team 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.

8.2. Evaluation of Development Documentation (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the CPP_ND_V3.0E, MOD_MACSEC_V1.0, MOD_VPNGW_v1.3, and PKG_SSH_V1.0 related to the examination of the information contained in the TSS.

The Validation 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.

8.3. Evaluation of Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation team 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.

8.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

The Validation team 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.

8.5. Evaluation of Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the assurance activities in the CPP_ND_V3.0E, MOD_MACSEC_V1.0, MOD_VPNGW_v1.3, and PKG_SSH_V1.0 and recorded the results in a Test Report, summarized in the AAR.

The Validation team 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.

8.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15, Vulnerability Assessment*, v1.1, August 2025, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on August 4, 2025, did not uncover any residual vulnerability.

The Evaluation team searched:

- Cisco security advisories (https://www.cisco.com/security/)
- CVEs
  - NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
  - Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/
  - Common Vulnerabilities and Exposures: https://www.cvedetails.com/vulnerability-search.php
- CISA Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

The Evaluation team performed a search using the following keywords:

- Cisco Catalyst 8500 Series Edge Routers
- C8500-20X6C
- Intel Xeon D-1573N (Broadwell)
- Broadcom BCM82757
- Comira MV88EC808
- Cisco IOS-XE 17.15
- OpenSSH 9.2p1
- IC2M Rel5a
- CiscoSSL
- CiscoSSH

The Validation team 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.

8.7. 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 followed the procedures defined in the CEM and performed the Assurance Activities in the CPP_ND_V3.0E, MOD_MACSEC_V1.0, MOD_VPNGW_v1.3, and PKG_SSH_V1.0 and correctly verified that the product meets the claims in the ST.

9. Validator Comments

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 6 of this Validation Report. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. Any additional customer documentation that was not included in the scope of the evaluation should not be relied upon when configuring or operating the device as evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. No versions of the TOE and software, either earlier or later, were evaluated.

10. Annexes

Not applicable.

11. Security Target

Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 Security Target, 1.1, August 21, 2025.

12. GLOSSARY

- **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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **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.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

13. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership

NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

14. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001*, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002*, Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003*, Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
5. *collaborative Protection Profile for Network Devices, Version: 3.0e, Date: 06-December-2023*
6. *Evaluation Activities for Network Device cPP, December-2019, Version 3.0e, Date: 06-December-2023*
7. *PP-Module for MACsec Ethernet Encryption, Version 1.0, 2023-03-02*
8. *Supporting Document Mandatory Technical Document PP-Module for MACsec Ethernet Encryption, Version 1.0, 2023-03-02*
9. *PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3, August-16-2023*
10. *Supporting Document Mandatory Technical Document PP-Module for VPN Gateways, Version 1.3, 16-August-2023*
11. *Functional Package for Secure Shell, Version 1.0, 13-May-2021*

12. *Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE Security Target, 1.1, August 21, 2025*
13. *Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 Operational User Guidance and Preparative Procedures, Version 1.0, August 14, 2025*
14. *Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 Assurance Activity Report, Version 1.1, August 2025*
15. *Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15, Vulnerability Assessment, Version 1.1, August 2025*
16. *Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 Evaluation Technical Report, Version 1.1, August 2025*
17. *Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 Detailed Test Report, Version 1.1, August 2025*
18. *Cisco Catalyst 8500 Series Edge Routers (Cat8500) running IOS-XE 17.15 Detailed Test Report Evidence, Version 1.1, August 2025*