Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.15

Version 1.0, 28 October 2025

Document reference: AISEP-CC-CR-2025-EFT-T059-CR-V1.0
(Certification expires five years from certification report date)

Table of contents

Executive Summary

This report describes the findings of the IT security evaluation of Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.15 against Common Criteria approved Protection Profiles (PPs).

The Target of Evaluation (TOE) is a purpose-built, virtual routing platform that includes VPN functionality provided by the Cisco IOS-XE software operating within a virtual machine (VM). The TOE consists solely of the Cisco IOS-XE software image running in the VM.

This report concludes that the Target of Evaluation (TOE) has complied with the following PPs [4]:

- Collaborative Protection Profile for Network Devices, Version 3.0e, 6 December 2023. (CPP_ND_V3.0E)
- PP-Module for Virtual Private Network (VPN) Gateways, Version: 1.3, 16 August 2023. (MOD_VPNGW_V1.3)
- Functional Package for SSH Version 1.0, 13 May 2021. (PKG_SSH_V1.0).

Additionally, the above PPs are grouped together using a certified PP-Configuration. This evaluation used the following PP-Configuration [4]:

- PP-Configuration for Network Devices and VPN Gateways, Version 2.0, 25 April 2024. (CFG_NDcPP-VPNGW_V2.0)

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australian Information Security Evaluation Program (AISEP). The evaluation was performed by Teron Labs with the final Evaluation Technical Report (ETR) submitted on 02 October 2025.

With regard to the secure operation of the TOE, the Australian Certification Authority recommends that administrators:

- ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are understood
- configure and operate the TOE according to the vendor's product administrator guidance and pay attention to all security warnings
- verify the hash of any downloaded software, as advised in configuration guide for the TOE
- the system auditor should review the audit trail generated and exported by the TOE periodically.

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target [8] and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

Purpose

The purpose of this Certification Report is to:

- Report the certification of results of the IT security evaluation of the TOE against the requirements of the Common Criteria [1,2,3] and Protection Profiles [4]
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target [8] which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.15.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.15
Software version	17.15
Hardware platforms	C8000V virtual with UCS C Series M7
Security Target	Security Target Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.15, Version 1.1, 29 September 2025
Evaluation Technical Report	Evaluation Technical Report 1.0, dated 02 October 2025 Document reference EFT-T059-ETR 1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, April 2017, Version 3.1 Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5
Conformance	Collaborative Protection Profile for Network Devices, Version 3.0e, 6 December 2023. (CPP_ND_V3.0E)

	PP-Module for Virtual Private Network (VPN) Gateways, Version: 1.3, 16 August 2023. (MOD_VPNGW_V1.3) Functional Package for SSH Version 1.0, 13 May 2021. (PKG_SSH_V1.0)
Developer	Cisco Systems, Inc. 170 West Tasman Dr. San Jose, CA 95134
Evaluation facility	Teron Labs Level 2, 14 Moore St, Canberra ACT 2601 Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

The TOE is the Cisco Catalyst 8000V Edge (C8000V), a virtual router that functions as a virtual Network Device (vND) in accordance with the evaluated configuration Case 1 of the NDcPP v3.0e. The TOE consists solely of the Cisco IOS-XE software, version 17.15, and running as a Virtual Machine (VM) on a hypervisor. The underlying hardware platform (Cisco UCS C-Series M7 server) and the ESXi 8.0 hypervisor are part of the Virtual System but are explicitly outside the TOE boundary. The TOE includes a virtual Route Processor and a virtual Forwarding Processor, both implemented in software within the VM.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.6 of the Security Target [8].

TOE Physical Boundary

The TOE consists solely of the Cisco IOS-XE software image Release 17.15 running in a VM. The underlying hardware and hypervisor (e.g., ESXi 8.0 on Cisco UCS C-Series M7) are part of the Virtual System and Evaluated Configuration but are not part of the TOE.

The software is pre-installed in the VM and is also available for download from the Cisco website (login required). The following table describes the underlying hardware and virtual configuration that supports the evaluated configuration; this information is provided for completeness and clarity about the evaluated environment, but this hardware is not part of the TOE.

The install image provided for the TOE is:

- c8000v-universalk9.17.15.x86_64.iso

The software version reflects the detail reported for the Cisco IOS-XE when the “show version” command is executed on the device.

Architecture

The TOE is the Cisco Catalyst 8000V Edge (C8000V), a virtual network device (vND) that operates as a virtual router with integrated VPN capabilities. It runs the Cisco IOS-XE 17.15 software image within a virtual machine (VM) hosted on a Cisco UCS C-Series M7 server using the VMware ESXi 8.0 hypervisor.

The TOE requires the following:

- Cisco UCS C-Series M7 Server with Intel Xeon Scalable 2nd Generation processors
- VMware ESXi 8.0 Hypervisor
- Virtual Machine (VM) Requirements: The following minimum technical specs are required on the Cisco UCS Server to support the C8000V guest VM running Cisco IOS-XE version 17.15 software:
    - A single virtual hard disk – 8 GB minimum
    - One dedicated management port
    - Two or more virtual network interfaces with adapter type VMXNET3 that are mapped to physical Ethernet ports on the host server via ESXi
    - The following virtual CPU/RAM configurations are supported:
        - 1 virtual CPU, requiring 4 GB minimum of RAM
        - 2 virtual CPUs, requiring 4 GB minimum of RAM
        - 4 virtual CPUs, requiring 4 GB minimum of RAM
        - 8 virtual CPUs, requiring 8 GB minimum of RAM
        - 16 virtual CPUs, requiring 8 GB minimum of RAM

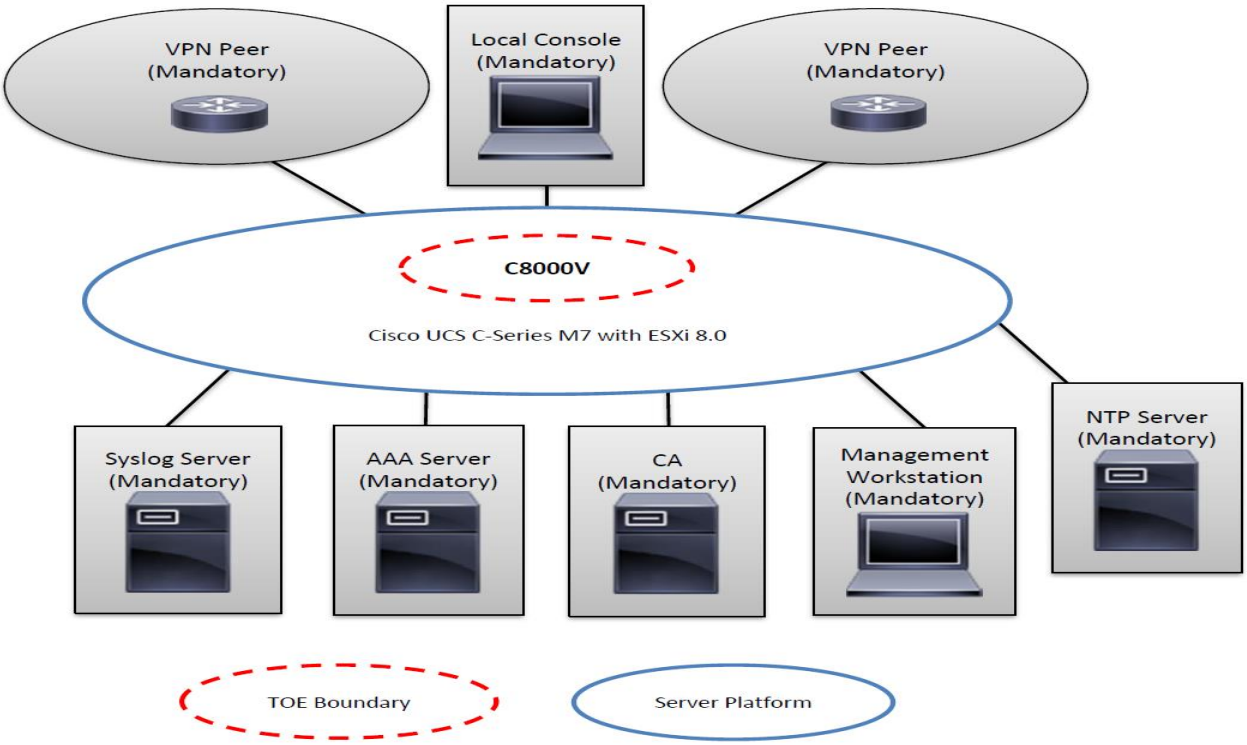
The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XE configuration determines how packets are handled to and from the TOE’s network interfaces. The router configuration will determine how traffic flows received on an interface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

Evaluated configuration for the UCS C-Series M7 Servers with Intel Scalable 4th Generation processors include the following:

- Intel Xeon Platinum 8452Y (Sapphire Rapids)
- VMware ESXi 8.0
- VMXNET3 NIC (3 physical GbE port mapped to 3 virtual NICs (Mgmt, WAN, LAN)
- The Packet Forwarding Engine is incorporated in the TOE software to perform packet forwarding functons on top of hardware-based link layer and routing engine capabilities.

- 1vCPU
- 4GB RAM (virtual) / 64GB (physical)
- 8GB HDD (virtual) / 2TB (physical)

The following figure provides a visual depiction of an example C8000V TOE:



NOTE: While the above image includes several non-TOE IT environment devices, the TOE is only the C8000V devices.

Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the Security Target [8].

Evaluated Functionality

Functional tests performed during the evaluation were taken from the Protection Profiles [4] and Supporting Documents [12] and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

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 a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
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 enrolment.
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.

C8000V hardware platform	Yes	This includes the Cisco UCS C-Series M7 platform with Intel Xeon Scalable 4th Generation processors running ESXi 8.0. Hardware specifications are described in Section, 1.7, Table 4 of the ST.

Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Australian Government users should refer to the *Australian Government Information Security Manual* [5] for policy relating to using an evaluated product in an unevaluated configuration.

Security

The TOE Security Policy is a set of rules that defines the required security behaviour of the TOE; how information within the TOE is managed and protected. The Security Target [8] contains a summary of the functionality that is evaluated.

Secure Delivery

The TOE delivery procedure is described the guidance documentation [6].

The following components are delivered to the consumer as part of the TOE:

- Cisco C8000V IOS-XE Software Image
- Common Criteria Operational User Guidance and Preparative Procedures

Software delivery procedures

To obtain the evaluated image, submit a request to Cisco Technical Assistance Centre (TAC) (http://www.cisco.com/techsupport) specifying that the request be for the evaluated IOS XE 17.15.3a Special Image CSCWO73590. Once approved, Cisco TAC will provide access to download the evaluated image.

The following file types are available in the Cisco Catalyst 8000V Edge software image package and are used to install the Cisco Catalyst 8000V Edge software on a hypervisor.

- .OVA - Used for deploying the OVA template on a VM (in TAR format)
- .ISO - Used for installing the software image on a VM (requires manually creating the VM)

Hardware delivery procedures

There are several mechanisms provided in the delivery process to ensure that a customer receives a product that has not been tampered with. In addition to the above procedures for the TOE software, the TOE requires hardware to run

on, despite the hardware being out of scope of the TOE boundary, the customer should still perform the following checks upon receipt of any hardware to verify the integrity of the platform:

- Shipping label—ensure that the shipping label correctly identifies the correct customer name and address as well as the device.
- Outside packaging—Inspect the outside shipping box and tape. Ensure that the shipping tape has not been cut or otherwise compromised. Ensure that the box has not been cut or damaged to allow access to the device.
- Inside packaging—inspect the plastic bag and seal. Ensure that the bag is not cut or removed. Ensure that the seal remains intact.

If the customer identifies a problem during the inspection, he or she should immediately contact the supplier. Provide the order number, tracking number, and a description of the identified problem to the supplier.

Installation of the TOE

The Configuration Guides [6] contains all relevant information for the secure configuration of the TOE.

Version Verification

The verification of the TOE is largely automatic, including the verification using hashes. The TOE cannot load a modified image. Valid software images can be downloaded from http://www.cisco.com/techsupport by submitting a request to Cisco TAC. The TOE will automatically display the hash verification on boot or by using the reload command. The successful hash verification message will display on the successful verification of the boot image. If the image was tampered with in any way, an error would display, and the image will not boot. The TOE confirms that the C8000V loads the image correctly, completes internal self-checks and displays any cryptographic export warning on the console.

Once the image is loaded into bootflash, to display information related to software authenticity for a specific image file, use the verify command.

Security Administrators are able to query the current version of the TOE firmware using the CLI command ‘show version’.

Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased.

All Common Criteria guidance material is available at https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/common-criteria.html

For the latest version of The *Australian Government Information Security Manual,* Please refer to the following link: https://www.cyber.gov.au/ism [5].

Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

The network device is assumed to be physically secured within its operational environment, protected from physical attacks that could compromise its security or interfere with its physical connections and correct operation. This level of protection is expected to be sufficient to safeguard the device and the sensitive data it handles.

The TOE is expected to provide networking functionality as its primary purpose and should not offer any general-purpose computing capabilities, such as running compilers or user applications unrelated to its networking functions. This ensures that the device remains focused solely on its intended security and networking roles.

The network device's administrator(s) are assumed to be trustworthy, acting in the best interests of the organization's security. This includes being well-trained, adhering to established policies, and following all guidance documentation. Administrators are responsible for ensuring that passwords and credentials used within the TOE are strong and secure. The TOE is not expected to protect against a malicious administrator who deliberately seeks to bypass or compromise its security features.

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).

The TOE's firmware and software are assumed to be regularly updated by an administrator, particularly in response to newly discovered vulnerabilities. This ensures that the TOE remains protected against emerging threats.

The credentials (such as private keys) used by administrators to access the TOE must be securely protected on any platform where they are stored. Administrators must also ensure that sensitive residual information, including cryptographic keys, keying material, PINs, and passwords, is not accessible to unauthorised individuals when networking equipment is discarded or removed from service.

The TOE is assumed to be connected to distinct networks in a way that ensures its security policies are enforced on all relevant network traffic flowing between these networks.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the relevant Protection Profiles [4] and Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3 [1, 2].

Testing methodology was drawn from Common Methodology for Information Technology Security, April 2017 Version 3.1 Revision 5 [3] and relevant Supporting Documents [12].

The evaluation was carried out in accordance with the operational procedures of the Australian Information Security Evaluation Program [10].

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security [9] and the document *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs* [13] were also upheld.

Functional Testing

All functional tests performed by the evaluators were taken from the Protection Profiles [4] and Supporting Documents [12]. The tests were designed to provide the required testing coverage for the security functions claimed by the TOE.

Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report [11].

Penetration Testing

The evaluators performed the evaluation activities for vulnerability assessment specified by the NDcPP Supporting Document [12] that follow a flaw hypothesis methodology. Accordingly, four types of flaw hypotheses have been considered:

- Type 1 - public vulnerabilities
- Type 2 - ND-iTC (Network international Technical Community) sourced
- Type 3 - evaluation team generated
- Type 4 - tool generated.

The evaluators conducted a review of public vulnerability databases and technical community sources to determine potential flaw hypotheses using searches that include TOE device name and components, protocols supported by the TOE and terms relating to the device type of the TOE. These searches were conducted up to the 29 Aug 2025. Coinciding with the conclusion of the evaluation. There was no identifiable Type 2 hypotheses for this evaluation.

The evaluation team devised one test to check a potential vulnerability within the TOE's firmware for hard-coded credentials or other sensitive information. Additional analysis concluded the TOE returned no sensitive values. The evaluation team also conducted tool-generated vulnerability testing of the TOE as per the Supporting Document [12]

Based on the results of this testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

This certification focused on the evaluation of product compliance with Protection Profiles that cover the technology area of network devices with added security functionality including VPN gateway functions and SSH. Organisations can have confidence that the scope of an evaluation against an ASD-approved Protection Profiles cover the necessary security functionality expected of the evaluated product and known threats will have been addressed.

The analysis is supported by testing as outlined in the PP Supporting Documents and Protection Profile Module activities, and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures. Certification is not a guarantee of freedom from security vulnerabilities.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with the Protection Profiles (PPs). PPs provide assurance by providing a full Security Target, and an analysis of the Security Functional Requirements in that Security Target, guidance documentation, and a basic description of the architecture of the TOE.

Certification Result

Teron Labs **has determined** that the TOE upholds the claims made in the Security Target [8] and **has met** the requirements of the Protection Profiles CPP_ND_V3.0E [4.a], PKG_SSH_V1. [4.b], MOD_VPNGW_V1.3 [4.c] and PP configuration for Network device and VPN Gateway [4.d].

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the Evaluation Technical Report [7], the Australian Certification Authority **certifies** the evaluation of the Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.15 performed by the Australian Information Security Evaluation Facility, Teron Labs.

The Australian Certification Authority certifies that the Security Target [8] have met the requirements of the Network Device Protection Profiles [4].

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian Government users. For further guidance, Australian Government users should refer to the Australian Government Information Security Manual [5].

In addition to ensuring that the assumptions concerning the operational environment are fulfilled, and the guidance document is followed, the Australian Certification Authority also recommends that users and administrators:

- ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
- configure and operate the TOE according to the vendor's product administrator guidance and pay attention to all security warnings
- maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
- the system auditor should review the audit trail generated and exported by the TOE periodically

These points ensure that the TOE remains in a CC compliant state throughout usage.

Annex – References and Abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5*

2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*

3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*

4. Protection Profiles:

    a) Collaborative Protection Profile for Network Devices, Version 3.0e, 6 December 2023 *(CPP_ND_V3.0E)*

    b) *Functional Package for SSH Version 1.0, 13 May 2021 (PKG_SSH_V1.0)*

    c) *PP-Module for Virtual Private Network (VPN) Gateways, Version: 1.3, 16 August 2023 (MOD_VPNGW_V1.3)*

    d) *PP-Configuration for Network Devices and VPN Gateways, Version 2.0, 25 April 2024 (CFG_NDcPP-VPNGW_V2.0)*

5. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism,

6. Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.15, Operational User Guidance and Preparative Procedures, Version 1.0, Published 26 September 2025.

7. *Evaluation Technical Report Cisco Catalyst 8000V Edge (C8000V) running IOS-XE, Version 1.0, Dated 02 October 2025* (Document reference EFT-T059-ETR 1.0)

8. *Security Target Cisco Catalyst 8000V Edge (C8000V) running IOS-XE 17.15, Version 1.1, 29 September 2025.*

9. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014*

10. *AISEP Policy Manual (APM):* https://www.cyber.gov.au/sites/default/files/2023-03/2022_AUG_REL_AISEP_Policy_Manual_6.3.pdf , Version 6.3, release August 2022.

11. Entropy Documentation:

    a) *Entropy Information, Cisco Catalyst 8000V Edge (C8000V) running IOS-XE running IOS-XE 17.15, Version 1.0, dated 26 September, 2025*

12. Protection Profile Supporting Documents

    a) *Supporting Document, Evaluation Activities for Network Device cPP, Version 3.0e, 6 December 2023 (CPP_ND_V3.0E_SD)*

    b) *Supporting Document, Mandatory Technical Document, PP-Module for Virtual Private Network (VPN) Gateways, version 1.3, 16 August 2023 (MOD_VPNGW_V1.3_SD)*

13. *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs 30 September 2021, Version 2.0, CCDB-013-v2.0*

Abbreviations

AAA	Authentication, Authorization, and Accounting
AISEP	Australian Information Security Evaluation Program
CA	Certificate Authority
CCRA	Common Criteria Recognition Arrangement
CPU	Central Processing Unit
GB	Gigabyte
HDD	Hard Disk Drive
IPsec	Internet Protocol Security
NDcPP	CCRA-approved collaborative Protection Profile for Network Devices
ND-iTC	Network international Technical Community
NIC	Network Interface Card
NTP	Network Time Protocol
LAN	Local Area Network
Mgmt	Management (shorthand)
PP	Protection Profile
RAM	Random Access Memory
SSH	Secure Shell
TAC	Cisco Technical Assistance Centre
TOE	Target of Evaluation
UCS	Cisco Unified Computing System
vND	virtual Network Device
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate