

**National Information Assurance Partnership**



**Common Criteria Evaluation and Validation Scheme**

**Validation Report**

**Cisco Catalyst 8000V Edge (C8000V), Cisco 1000 Series Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800), Cisco Catalyst 8300 Rugged Series Routers (IR8300)**

**Version 1.0**

**Report Number: CCEVS-VR-VID11332-2023**

**Dated: 05/04/2023**

**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**

**Ft. Meade, MD 20755-6982**

# **ACKNOWLEDGEMENTS**

## **Validation Team**

Jerome Myers

*Aerospace Corporation*

Farid Ahmed

Anne Gugel

Michael Smeltzer

Richard Toren

*Johns Hopkins University - Applied Physics Laboratory*

## **Common Criteria Testing Laboratory**

Rahul Joshi

Manohar Negi

Ranjeet Kumar

Rupendra Kadtan

Shivani Birwadkar

Snehal Raghunath Gaonkar

*Acumen Security, LLC*

## Table of Contents

<b>1</b>	<b>Executive Summary</b> .....	<b>5</b>
<b>2</b>	<b>Identification</b> .....	<b>6</b>
<b>3</b>	<b>Architectural Information</b> .....	<b>8</b>
3.1	TOE Overview .....	8
3.2	TOE Description.....	8
3.3	Physical Scope of the TOE.....	9
<b>4</b>	<b>Security Policy</b> .....	<b>12</b>
4.1	Security Audit .....	12
4.2	Cryptographic Support.....	12
4.3	Identification and authentication .....	14
4.4	Security Management .....	15
4.5	Packet Filtering.....	15
4.6	Protection of the TSF .....	16
4.7	TOE Access .....	16
4.8	Trusted path/Channels.....	16
<b>5</b>	<b>Assumptions, Threats &amp; Clarification of Scope</b> .....	<b>17</b>
5.1	Assumptions .....	17
5.2	Threats.....	19
5.3	Clarification of Scope .....	23
<b>6</b>	<b>Documentation</b> .....	<b>24</b>
<b>7</b>	<b>TOE Evaluated Configuration</b> .....	<b>25</b>
7.1	Evaluated Configuration.....	25
7.1.1	Cisco Catalyst 8000V Edge (C8000V) .....	25
7.1.2	Cisco 1000 Series Integrated Services Router (ISR1000).....	26
7.1.3	Cisco Catalyst 1800 Rugged Series Routers (IR1800).....	26
7.1.4	Cisco Catalyst 8300 Rugged Series Routers (IR8300).....	26
7.2	Excluded Functionality .....	28
<b>8</b>	<b>IT Product Testing</b> .....	<b>29</b>
8.1	Developer Testing .....	29
8.2	Evaluation Team Independent Testing.....	29
<b>9</b>	<b>Results of the Evaluation</b> .....	<b>30</b>
9.1	Evaluation of Security Target .....	30
9.2	Evaluation of Development Documentation.....	30
9.3	Evaluation of Guidance Documents.....	30
9.4	Evaluation of Life Cycle Support Activities .....	31
9.5	Evaluation of Test Documentation and the Test Activity .....	31
9.6	Vulnerability Assessment Activity .....	31
9.7	Summary of Evaluation Results .....	31

<b>10</b>	<b>Validator Comments &amp; Recommendations .....</b>	<b>33</b>
<b>11</b>	<b>Annexes.....</b>	<b>34</b>
<b>12</b>	<b>Security Target .....</b>	<b>35</b>
<b>13</b>	<b>Glossary .....</b>	<b>36</b>
<b>14</b>	<b>Bibliography.....</b>	<b>37</b>

# 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 8000V Edge (C8000V), Cisco 1000 Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800), Cisco Catalyst 8300 Rugged Series Routers (IR8300) 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 April 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 the Protection Profile Configuration for Network Devices and Virtual Private Network (VPN) Gateways Version 1.1. Those requirements include the requirements from the Collaborative Protection Profile for Network Devices (NDcPPv2.2e), Virtual Private Network (VPN) Gateways (MOD\_VPNGW\_V1.1).

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 Activity 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 Common Criteria Evaluation and Validation Scheme (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**

<b>Item</b>	<b>Identifier</b>
<b>Evaluation Scheme</b>	United States NIAP Common Criteria Evaluation and Validation Scheme
<b>TOE</b>	Cisco Catalyst 8000V Edge (C8000V), Cisco 1000 Series Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800), Cisco Catalyst 8300 Rugged Series Routers (IR8300)
<b>Protection Profile</b>	PP-Configuration for Network Device and Virtual Private Network (VPN) Gateways (CFG_NDcPP-VPNGW_V1.1), version 1.1, 1 July 2020 <ul style="list-style-type: none"> <li>• Base-PP: collaborative Protection Profile for Network Devices (CPP_ND_V2.2E), version 2.2e, 23 March 2020</li> <li>• PP-Module: PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW_V1.1), version 1.1, 18 June 2020</li> </ul>
<b>Security Target</b>	Cisco Catalyst 8000V Edge (C8000V), Cisco 1000 Series Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800), Cisco Catalyst 8300 Rugged Series Routers (IR8300) Security Target Version 1.0, May 2, 2023
<b>Evaluation Technical Report</b>	Evaluation Technical Report for Cisco Catalyst 8000V Edge (C8000V), Cisco 1000 Series Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800), Cisco Catalyst 8300 Rugged Series Routers (IR8300) Version 0.3, May 2, 2023
<b>CC Version</b>	Common Criteria Version 3.1, Revision 5
<b>Conformance Result</b>	CC Part 2 Extended and CC Part 3 Conformant
<b>Sponsor</b>	Cisco Systems, Inc.

<b>Item</b>	<b>Identifier</b>
<b>Developer</b>	Cisco Systems, Inc.
<b>Common Criteria Testing Lab (CCTL)</b>	Acumen Security Rockville, MD
<b>CCEVS Validators</b>	Jerome Myers Farid Ahmed Anne Gugel Michael Smeltzer Richard Toren

## 3 Architectural Information

### 3.1 TOE Overview

The Cisco Catalyst 8000V Edge (herein after referred to as the C8000V), Cisco 1000 Series Integrated Services Routers (herein after referred to as the ISR1000), Cisco Catalyst 1800 Rugged Series Routers (herein after referred to as the IR1800), and Cisco Catalyst 8300 Rugged Series Routers (herein after referred to as the IR8300) are purpose-built, routing platforms that include VPN functionality.

Cisco IOS-XE software is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective switching and routing. Although IOS performs many networking functions, this Security Target only addresses the functions that provide for the security of the TOE itself as described in Logical Scope of the TOE

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

### 3.2 TOE Description

The TOE software for each platform is comprised of Cisco IOS-XE version 17.9. Cisco IOS-XE is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS-XE performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself. The Cisco IOS-XE version 17.9 software is used to meet all of the requirements as specified in this document regardless of the hardware platform.

#### **Cisco Catalyst 8000V Edge (C8000V)**

This section provides an overview of the C8000V virtual router Target of Evaluation (TOE) as a virtual Network Device (vND) using the evaluated configuration Case 1 specified in NDcPPv2.2e. The C8000V provides a router deployed on a virtual machine (VM) instance on x86 server hardware. The C8000V includes a virtual Route Processor and a virtual Forwarding Processor (FP) as part of its architecture. The C8000V is deployed as a virtual machine running on ESXi 6.7 hypervisor on a Cisco UCS C-Series M5 Server (Intel Xeon Scalable 2<sup>nd</sup> Generation (Cascade Lake) processor) or other general-purpose computing platforms running Intel Broadwell, Goldmont, and Coffee Lake processors. Compatible hardware is described in Section 3.3, Table 2 of this document. The software is comprised of Cisco IOS-XE version 17.9.

#### **Cisco 1000 Series Integrated Services Routers (ISR1000)**

This section provides an overview of the ISR1000 Target of Evaluation (TOE). This section also defines the TOE components included in the evaluated configuration of the TOE. The TOE is comprised of both software and hardware. The software is comprised of Cisco IOS-XE version 17.9. The C1131 is the hardware model included in the evaluation.

The ISR1000 consists of the following architectural features:

- Chassis: The TOE is housed in a 1RU form factor chassis.
- Multicore Processors: Multicore processors that support high-speed WAN connections.
- Integrated Gigabit Ethernet ports: Provides up to 10 built-in 10/100/1000 Ethernet ports for WAN or LAN. All platforms have one 10/100/1000 Ethernet port that can support Small Form-Factor Pluggable (SFP)-based connectivity in addition to RJ-45 connections, enabling fiber or copper connectivity. An additional dedicated Gigabit Ethernet port is provided for device management.



- Flash memory support: The TOE has a fixed 8 GB flash memory. Two USB type A 2.0 ports.
- DRAM: The TOE has 8 GB fixed DRAM.

### **Cisco Catalyst 1800 Rugged Series Routers (IR1800)**

This section provides an overview of the IR1800 TOE. This section also defines the TOE components included in the evaluated configuration of the TOE. The TOE is comprised of both software and hardware. The software is comprised of Cisco IOS-XE version 17.9. The IR1821-K9, IR1831-K9, IR1833-K9, and IR1835-K9 are the hardware models included in the evaluation.

The Cisco IR1800 primary features include the following:

- DRAM: 4 GB (IR1821-K9, IR1831-K9, IR1833-K9), 8 GB (IR1835-K9)
- Flash memory: 4 GB (IR1821-K9, IR1831-K9, IR1833-K9), 8 GB (IR1835-K9)
- One micro USB console port
- One USB type A 2.0 port
- WAN Interfaces
  - One combo 10/100/1000 Mbps Gigabit Ethernet port (RJ-45 and SFP)
- LAN Interfaces
  - Four 10/100/1000 Mbps Gigabit Ethernet ports (RJ-45)

### **Cisco Catalyst 8300 Rugged Series Routers (IR8300)**

This section provides an overview of the IR8300 TOE. This section also defines the TOE components included in the evaluated configuration of the TOE. The TOE is comprised of both software and hardware. The software is comprised of Cisco IOS-XE version 17.9. The IR8340-K9 is the hardware model included in the evaluation.

The IR8300 consists of the following architectural features:

- DRAM: 8 GB
- Flash memory: 16 GB
- One RJ-45 console port
- One USB type A 2.0 port
- WAN Interfaces
  - Two combo 10/100/1000 Mbps Gigabit Ethernet port (RJ-45 and SFP)
- LAN Interfaces
  - Four 10/100/1000 Mbps Gigabit Ethernet ports (RJ-45)
  - Four 10/100/1000 Mbps Gigabit Ethernet ports (SFP)
  - Four combo 10/100/1000 Mbps Gigabit Ethernet ports (RJ-45 and SFP)

## **3.3 Physical Scope of the TOE**


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

- C8000V virtual router deployed on one of the following compatible platforms:
  - Cisco UCS C-Series M5 Servers with Intel Xeon Scalable 2<sup>nd</sup> Generation (Cascade Lake)
  - General-purpose computing platforms with Intel Broadwell processors: Xeon D-1559
  - General-purpose computing platforms with Intel Goldmont processors: Atom E3950
  - General-purpose computing platforms with Intel Coffee Lake processors: Xeon E-2254ML
- IR1800
  - IR1821-K9

- IR1831-K9
- IR1833-K9
- IR1835-K9
- ISR1000
  - C1131
- IR8300
  - IR8340-K9



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 17.9. In addition, the software image is downloadable from the Cisco web site. A login ID and password is required to download the software image. The TOE is comprised of the following physical specifications as described in Table 2 below:

**Table 2 Hardware Models and Specifications**

Hardware	Processor	Features
C8000V virtual router compatible Cisco UCS Servers and other general-purpose computing platforms with specified Intel processors	Intel Xeon Scalable 2 <sup>nd</sup> Generation (Cascade Lake) <sup>1</sup> with ESXi 6.7 Intel Broadwell processors with ESXi 6.7 Intel Goldmont processors with ESXi 6.7 Intel Coffee Lake processors with ESXi 6.7	<p><b>Cisco UCS C-Series M5 Servers and General-purpose computing hardware Interfaces:</b></p> <p>All compatible hardware platforms have a dedicated OOB management port and at least two physical Gigabit ethernet interfaces.</p> <p><b>VM Interfaces:</b></p> <ul style="list-style-type: none"> <li>● One dedicated management port<sup>2</sup></li> <li>● Two or more virtual network interfaces with adaptor type VMXNET3 that are mapped to physical ethernet ports on the host server via ESXi</li> </ul>
1000 Series Integrated Services Routers C1131 	Marvell Armada (Cortex-A72)	<p><b>Physical dimensions (H x W x D in.)</b></p> <ul style="list-style-type: none"> <li>● 1.75 x 12.7 x 9.6 in. (LTE)</li> <li>● 1.75 x 12.7 x 9.03 in. (Non-LTE)</li> <li>● 1.73 x 9.75 x 6.6 in. (C1101 LTE)</li> <li>● 1.1 x 7.5 x 6.0 in. (C1101 Non-LTE)</li> </ul> <p><b>Interfaces</b></p> <ul style="list-style-type: none"> <li>● Up to 10 built-in 10/100/1000 Ethernet ports for WAN or LAN.</li> <li>● One 10/100/1000 Ethernet port that can support (SFP)-based or RJ-45 connections.</li> <li>● PoE/PoE+ on Gigabit Ethernet interfaces (enabled on specific platforms).</li> </ul>

<sup>1</sup> Evaluated on UCS C220 M5 with Intel Xeon Gold 6244

<sup>2</sup> VMware remote local console

Hardware	Processor	Features
		<ul style="list-style-type: none"> <li>One Gigabit Ethernet port is provided for device management.</li> </ul>
<p>Catalyst 1800 Rugged Series Routers</p> <p>IR1821-K9, IR1831-K9, IR1833-K9, IR1835-K9</p> 	<p>Marvell Armada (Cortex-A72)</p>	<p><b>Physical dimensions (H x W x D)</b></p> <ul style="list-style-type: none"> <li>2.20 x 11.04 x 8.06 in. (55.9 x 280.4 x 204.7 mm)</li> </ul> <p><b>Interfaces</b></p> <ul style="list-style-type: none"> <li>One micro-USB console port</li> <li>One USB type A 2.0 port</li> <li>WAN <ul style="list-style-type: none"> <li>One combo 10/100/1000 Mbps Gigabit Ethernet port (RJ-45 and SFP)</li> </ul> </li> <li>LAN <ul style="list-style-type: none"> <li>Four 10/100/1000 Mbps Gigabit Ethernet ports (RJ-45)</li> </ul> </li> </ul>
<p>Cisco Catalyst 8300 Rugged Series Routers</p> <p>IR8340-K9</p> 	<p>Intel Atom C3708 (Goldmont)</p>	<p><b>Physical dimensions (H x W x D)</b></p> <ul style="list-style-type: none"> <li>3.5 x 17.25 x 15 in.</li> </ul> <p><b>Interfaces</b></p> <ul style="list-style-type: none"> <li>One RJ-45 console port</li> <li>One USB type A 2.0 port</li> <li>WAN <ul style="list-style-type: none"> <li>Two combo 10/100/1000 Mbps Gigabit Ethernet port (RJ-45 and SFP)</li> </ul> </li> <li>LAN <ul style="list-style-type: none"> <li>Four 10/100/1000 Mbps Gigabit Ethernet ports (RJ-45)</li> <li>Four 10/100/1000 Mbps Gigabit Ethernet ports (SFP)</li> <li>Four combo 10/100/1000 Mbps Gigabit Ethernet ports (RJ-45 and SFP)</li> </ul> </li> </ul>

## 4 Security Policy

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Packet Filtering
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all SFRs of the NDcPP v2.2e and MOD\_VPNGW v1.1 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. The administrator configures auditable events, performs back-up operations and manages audit data storage. The TOE provides the administrator with a circular audit trail or a configurable audit trail threshold to track the storage capacity of the audit trail. Audit logs are backed up over an encrypted channel to an external audit server.

### 4.2 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 2. The TOE leverages the IOS Common Cryptographic Module (IC2M) Rel5a (see Table 3 for certificate references).

**Table 3 FIPS References**

Algorithm	Description	Supported Mode	Module	CAVP Cert. #	SFR
AES	Used for symmetric encryption/decryption	CBC (128, 192 and 256)  GCM (128, 192 and 256)	IC2M	A1462	FCS_COP.1/DataEncryption
SHS (SHA-1, SHA-256, SHA-384 and SHA-512)	Cryptographic hashing services	Byte Oriented	IC2M	A1462	FCS_COP.1/Hash

Algorithm	Description	Supported Mode	Module	CAVP Cert. #	SFR
HMAC (HMAC-SHA-1, SHA-256, SHA-512)	Keyed hashing services and digital signature	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
KAS-ECC-SSC	Key Agreement	NIST Special Publication 800-56A	IC2M	A1462	FCS_CKM.2
KAS-FFC-SSC	Key Agreement	NIST Special Publication 800-56A	IC2M	A1462	FCS_CKM.2

The TOE provides cryptography in support of VPN connections and remote administrative management via SSHv2 and IPsec to secure the transmission of audit records to the remote syslog server. In addition, IPsec is used to secure the session between the TOE and the authentication servers.

The cryptographic services provided by the TOE are described in Table 3 below:

**Table 4 TOE Provided Cryptography**

Cryptographic Method	Use within the TOE
Internet Key Exchange	Used to establish initial IPsec session.

Cryptographic Method	Use within the TOE
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.
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.
HMAC	Used for keyed hash, integrity services in IPsec and SSH session establishment.
RSA	Used in IKE protocols peer authentication Used to provide cryptographic signature services
ECDSA	Used to provide cryptographic signature services Used in Cryptographic Key Generation Used as the Key exchange method for IPsec
FFC DH	Used as the Key exchange method for SSH and IPsec
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 also 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 Command Line Interface (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 TOE Security Functionality (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.

#### **4.6 Protection of the TSF**

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords.

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

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually. Finally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

Whenever a failure occurs within the TOE that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE and reloads.

#### **4.7 TOE Access**

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. Sessions can also be terminated if an Authorized Administrator enters the "exit" or "logout" command.

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

#### **4.8 Trusted path/Channels**

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 which has the ability to be encrypted further using IPsec and initiates outbound IPsec tunnels to transmit audit messages to remote syslog servers. In addition, IPsec is used to secure the session between the TOE and the authentication servers. The TOE can also establish trusted paths of peer-to-peer IPsec sessions. The peer-to-peer IPsec sessions can be used for securing the communications between the TOE and authentication server/syslog server, as well as to protect communications with a CA.



## 5 Assumptions, Threats & Clarification of Scope

### 5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

**Table 5 TOE Assumptions**

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	<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. It is assumed that this protection will be covered by cPPs and PP-Modules 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 entropy and to lack</p>

Assumption	Assumption Definition
	<p>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.VS_TRUSTED_ADMINISTRATOR <sup>3</sup>	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
A.VS_REGULAR_UPDATES <sup>4</sup>	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_ISOLATON	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.

---

<sup>3</sup> Applies to C8000V only

<sup>4</sup> Applies to C8000V only

Assumption	Assumption Definition
A.VS_CORRECT_CONFIGURATION <sup>4</sup>	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

## 5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

**Table 6 Threats**

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the Network Device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.

Threat	Threat Definition
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials include replacing existing credentials with an attacker’s credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

Threat	Threat Definition
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 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.</p> <p>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.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>
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</p>

Threat	Threat Definition
	<p>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 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>
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.</p> <p>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.</p> <p>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>
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"> <li>• 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.</li> <li>• 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.</li> </ul>

### 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 (NDcPPv2.2e), 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.
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process. In particular, only the C1131 model is evaluated in the ISR1000 series. Likewise, the IR1821-K9, IR1831-K9, IR1833-K9, and IR1835-K9 are the hardware models included in the evaluation of IR1800 series. And finally only IR8340-K9 is the hardware model included in the evaluation of IR8300 series. The software is comprised of Cisco IOS-XE version 17.9 for all hardware models.
- Apart from the Admin Guide, additional customer documentation for the specific routers and VPN Gateway models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- 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. In particular, the use of the USB ports for supplemental storage or additional network ports is not covered by this evaluation. Those USB ports should not be used in those other manners when the TOE is in its evaluated configuration without further analysis and potentially additional security measures being put in place.

## 6 Documentation

The following documents were provided by the vendor with the TOE for evaluation, however, The CC Configuration Guides are the only documents that should be trusted for the installation, administration, and use of these products in their evaluated configurations.

- Cisco Catalyst 8000V Edge (C8000V), Cisco 1000 Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800), Cisco Catalyst 8300 Rugged Series Routers (IR8300), Security Target Version: 1.0.
- Assurance Activity Report for Cisco Catalyst 8000V Edge (C8000V), Cisco 1000 Series Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800), Cisco Catalyst 8300 Rugged Series Routers (IR8300) Version: 0.2.
- Evaluation Technical Report for Cisco Catalyst 8000V Edge (C8000V), Cisco 1000 Series Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800), Cisco Catalyst 8300 Rugged Series Routers (IR8300) Version: 0.3.
- Cisco Catalyst 8000V Edge (C8000V), CC Configuration Guide Version: 1.0.
- Cisco 1000 Series Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800), Cisco Catalyst 8300 Rugged Series Routers (IR8300), CC Configuration Guide, Version: 1.0

**Table 7 Cisco Documentation C8000V**

#	Title	Link
[1]	Cisco Catalyst 8000V Edge Software Installation And Configuration Guide	<a href="https://www.cisco.com/c/en/us/td/docs/routers/C8000V/Configuration/c8000v-installation-configuration-guide/m_installation_overview.html">https://www.cisco.com/c/en/us/td/docs/routers/C8000V/Configuration/c8000v-installation-configuration-guide/m_installation_overview.html</a>



## 7 TOE Evaluated Configuration

### 7.1 Evaluated Configuration

#### 7.1.1 Cisco Catalyst 8000V Edge (C8000V)

The TOE in the evaluated configuration contains the C8000V software image. The C8000V TOE requires the following:

- Cisco UCS C-Series M5 Server with Intel Xeon Scalable 2nd Generation processors or other general-purpose computing platforms with specified Intel processors as described in Section, 3.3, Table 2
- VMware ESXi 6.7 Hypervisor
- Virtual Machine (VM) Requirements: The following minimum technical specs are required on the Cisco UCS Server or general-purpose computing platforms to support the C8000V guest VM running Cisco IOS-XE version 17.9 software:
  - A single virtual hard disk – 8 GB minimum
  - One dedicated management port<sup>5</sup>
  - 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 4 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 M5 Servers with Intel Scalable 2nd Generation processors includes the following:**

- Intel Xeon Gold 6244 (Cascade Lake)
- VMware ESXi 6.7
- VMXNET3 NIC (3 physical GbE port mapped to 3 virtual NICs (Mgmt, WAN, LAN))
- 1vCPU
- 4GB RAM (virtual) / 64GB (physical)
- 8GB HDD (virtual) / 2TB (physical)

**Evaluated configuration for the general-purpose computing platforms with Intel Broadwell processors: includes the following:**

- Intel Xeon D-1559 (Broadwell)
- VMware ESXi 6.7
- VMXNET3 NIC (3 physical GbE port mapped to 3 virtual NICs (Mgmt, WAN, LAN))
- 1vCPU
- 4GB RAM (Virtual) / 64GB RAM (Physical)

---

<sup>5</sup> VMware remote local console

- 8GB HDD (virtual) / 500GB (physical)

**Evaluated configuration for the general-purpose computing platforms with Intel Coffee Lake processors includes the following:**

- Intel Xeon E-2254ML (Coffee Lake)
- VMware ESXi 6.7
- VMXNET3 NIC (3 physical GbE port mapped to 3 virtual NICs (Mgmt, WAN, LAN))
- 1vCPU
- 4GB RAM (virtual) / 64GB (physical)
- 8GB HDD (virtual) / 2TB (physical)

**Evaluated configuration for the general-purpose computing platforms with Intel Goldmont processors includes the following:**

- Intel Atom E3950 (Goldmont)
- VMware ESXi 6.7
- VMXNET3 NIC (3 physical GbE port mapped to 3 virtual NICs (Mgmt, WAN, LAN))
- 1vCPU
- 4GB RAM (virtual) / 8GB (physical)
- 8GB HDD (virtual) / 500GB (physical)

#### 7.1.2 Cisco 1000 Series Integrated Services Router (ISR1000)

The TOE consists of one physical device as specified in Section 3.3 and includes Cisco IOS-XE version 17.9 software. The hardware model included in the evaluation is the C1131. Table adds additional details on the physical characteristics of the model. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XE configuration determines how packets are handled to and from the TOE's network interfaces. The router configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination.

#### 7.1.3 Cisco Catalyst 1800 Rugged Series Routers (IR1800)

The TOE consists of one physical device as specified in Section 3.3 below and includes Cisco IOS-XE version 17.9 software. The IR1800 hardware models included in this evaluation are the IR1821-K9, IR1831-K9, IR1833-K9, and IR1835-K9. Table adds additional details on the physical characteristics of these 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.

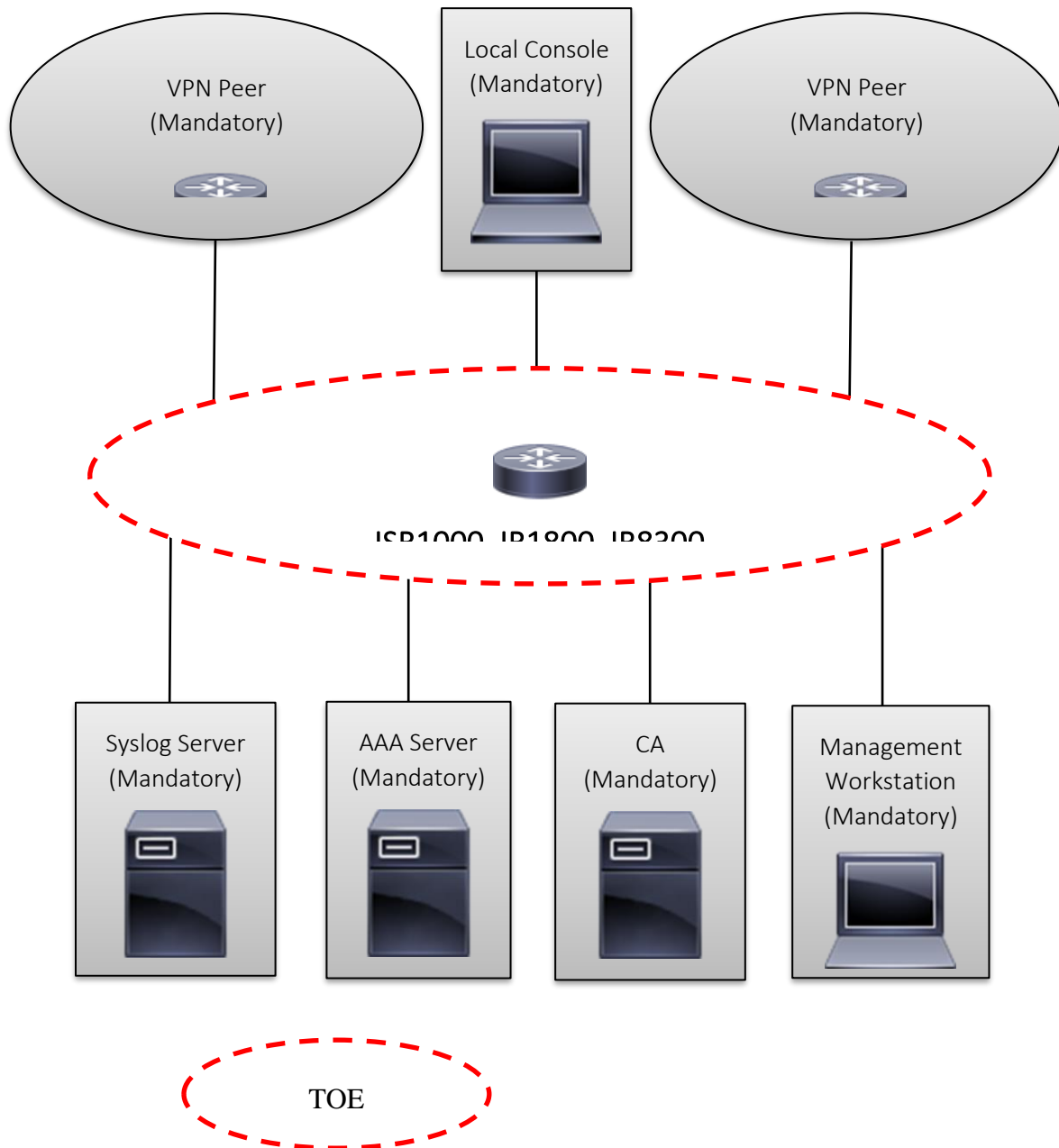
#### 7.1.4 Cisco Catalyst 8300 Rugged Series Routers (IR8300)

The TOE consists of one physical device as specified in Section 3.3 and includes Cisco IOS-XE version 17.9 software. The IR8300 hardware models included in this evaluation is the IR8340-K9. Table 2 adds additional details on the physical characteristics of these 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.

The following two figures provide a visual depiction of an example TOE deployment for the ISR1000, IR1800, IR8300 and the C8000V.

**Figure 1 TOE Example Deployment for ISR1000, IR1800, and IR8300**



## 7.2 Excluded Functionality

The following functionality is excluded from the evaluation:

**Table 8 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 as described in the Guidance documents (AGD). The exclusion of this functionality does not affect compliance to the NDcPP v2.2e and MOD\_VPNGW\_v1.1.

## **8 IT 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 8000V Edge (C8000V), Cisco 1000 Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800), Cisco Catalyst 8300 Rugged Series Routers (IR8300) IOS-XE 17.9, 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 (NDcPPv2.2e), Virtual Private Network (VPN) Gateways (MOD\_VPNGW\_V1.1). The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here. In particular, the test configurations and test tools are identified in Section 4 of the AAR.

## **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 Detailed Test Report (DTR) and 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 Common Criteria (CC) version 3.1 Rev. 5 and CEM version 3.1 Rev. 5. The evaluation determined the TOE to be Part 2 extended, and meets the SARs 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 8000V Edge (C8000V), Cisco 1000 Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800), Cisco Catalyst 8300 Rugged Series Routers (IR8300) IOS-XE 17.9 that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Network Devices Version 2. (NDcPPv2.2e) and PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 (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 EAL 1 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's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices Version 2. (NDcPPv2.2e) and PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 (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 EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were

complete. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices Version 2. (NDcPPv2.2e) and PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 (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 EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

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

#### **9.5 Evaluation of Test Documentation and the Test Activity**

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the collaborative Protection Profile for Network Devices Version 2.2 (NDcPPv2.2e) and PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 (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 (NDcPPv2.2e), 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**

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE. A list of databases searched, the search terms, and the date of the search can be found in Section 7.6.1 of the AAR.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the Collaborative Protection Profile for collaborative Protection Profile for Network Devices Version 2.2 (NDcPPv2.2e) and PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 (MOD\_VPNGW\_V1.1), and that the conclusion reached by the evaluation team was justified.

#### **9.7 Summary of Evaluation Results**

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the collaborative Protection Profile for Network Devices Version 2. (NDcPPv2.2e) and PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 (MOD\_VPNGW\_V1.1), and correctly verified that the product meets the claims in the ST.



## **10 Validator Comments & Recommendations**

All of the validators concerns are adequately captured in Section 5, Assumptions, Threats, and Clarification of Scope.

## **11 Annexes**

Not applicable.

## **12 Security Target**

**Cisco Catalyst 8000V Edge (C8000V), Cisco 1000 Series Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800), Cisco Catalyst 8300 Rugged Series Routers (IR8300), Security Target Version: 0.4.**

## 13 Glossary

The following definitions are used throughout this document:

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

## 14 Bibliography

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

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. collaborative Protection Profile for Network Devices Version 2. (NDcPPv2.2e)
6. PP-Module for Virtual Private Network (VPN) Gateways Version 1.1 (MOD\_VPNGW\_V1.1).
7. Assurance Activity Report for Cisco Catalyst 8000V Edge (C8000V), Cisco 1000 Series Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800), Cisco Catalyst 8300 Rugged Series Routers (IR8300) Version: 0.2.
8. Evaluation Technical Report for Cisco Catalyst 8000V Edge (C8000V), Cisco 1000 Series Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800), Cisco Catalyst 8300 Rugged Series Routers (IR8300) Version: 0.2.
9. Cisco Catalyst 8000V Edge (C8000V), CC Configuration Guide Version: 0.2.
10. Cisco 1000 Series Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800), Cisco Catalyst 8300 Rugged Series Routers (IR8300), CC Configuration Guide, Version: 0.2
11. Cisco Catalyst 8000V Edge (C8000V), Cisco 1000 Integrated Services Routers (ISR1000), Cisco Catalyst 1800 Rugged Series Routers (IR1800), Cisco Catalyst 8300 Rugged Series Routers (IR8300), Security Target Version: 0.4.