

National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



Validation Report

for

Cisco Expressway X12.5

Report Number: CCEVS-VR-VID11015-2020

Dated: February 24, 2020

Version: 1.0

**National Institute of Standards and
Technology**

**Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899**

National Security Agency

**Information Assurance Directorate
9800 Savage Road STE 6940
Fort Meade, MD 20755-6940**

ACKNOWLEDGEMENTS

Validation Team

Harry Beddo

Marybeth Panock

Jerome Myers

Common Criteria Testing Laboratory

Acumen Security, LLC

Table of Contents

1	Executive Summary	4
2	Identification	5
3	Architectural Information	6
4	Security Features	7
5	Assumptions, Threats & Clarification of Scope	12
5.1	Assumptions	12
5.2	Threats.....	13
5.3	Clarification of Scope	15
6	Documentation	16
7	TOE Evaluated Configuration	17
7.1	Evaluated Configuration.....	17
7.2	Physical Scope of the TOE	20
7.3	Excluded Functionality	23
8	IT Product Testing	24
8.1	Developer Testing	24
8.2	Evaluation Team Independent Testing.....	24
9	Results of the Evaluation	25
9.1	Evaluation of Security Target	25
9.2	Evaluation of Development Documentation	25
9.3	Evaluation of Guidance Documents	25
9.4	Evaluation of Life Cycle Support Activities	26
9.5	Evaluation of Test Documentation and the Test Activity	26
9.6	Vulnerability Assessment Activity	26
9.7	Summary of Evaluation Results	27
10	Validator Comments & Recommendations	28
11	Annexes	29
12	Security Target	30
13	Glossary	31
14	Bibliography	32

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 Expressway X12.5 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in February 2020. The information in this report is largely derived from the proprietary Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security and summarized in the publicly available Assurance Activity Report (AAR) for this evaluation. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for the collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314 (CPP_ND_V2.0E).

The Target of Evaluation identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1, Rev. 4, for conformance to the Common Criteria for Information Technology Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the NDcPP 2.0e Supporting Document. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

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

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profiles containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

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

Product Compliance List.

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

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

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Cisco Expressway X12.5
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314 (CPP_ND_V2.0E)
Security Target	Cisco Expressway X12.5 System Common Criteria Security Target
Evaluation Technical Report	Cisco Expressway X12.5 Evaluation Technical Report
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security
CCEVS Validators	Harry Beddo, Marybeth Panock, Jerome Myers

3 Architectural Information

The TOE is a hardware and software solution that makes up the Cisco Expressway. The TOE hardware platform is at least one of the following Cisco UCS platforms, UCS C220 M4, UCS C240 M4, UCS C220 M5 or the UCS C240 M5. The TOE software is the Cisco Expressway X12.5 software. The network, on which the TOE resides is considered part of the environment. The TOE guidance documentation, the Cisco Expressway Common Criteria Configuration Guide that is also considered to be part of the TOE can be found listed and is downloadable from the NIAP portal <https://www.niap-ccevs.org/>.

4 Security Features

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

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the NDcPP v2.0e to satisfy testing/assurance measures prescribed therein.

Security Audit

The Cisco Expressway provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco Expressway 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 audit event logging is centralized and enabled by default. Audit logs can be sent to an external audit server over a secure TLS channel

Communications

The TOE provides the configuration options for the Authorized Administrator to enable the persistent, dedicated secure connections using SSHv2.0 between the two components, Expressway-C and Expressway-E. This connection forms a highly secure traversal link to provide a collaboration gateway solution that extends the services and access to users inside and outside of the organization's firewall.

Cryptographic Support

The TOE provides cryptography in support of other Cisco Expressway security functionality. The Expressway software calls the CiscoSSL FIPS Object Module (FOM) v6.2 that has been validated in accordance with the specified standards to meet the requirements listed below and all the algorithms claimed have CAVP certificates.

Refer to Table 2 for algorithm certificate references.

Table 2 FIPS References

Algorithm	Description	Supported Mode	CAVP Cert. #	Module	SFR
RSA	Signature Verification and key transport	FIPS PUB 186-4 Key Generation, PKCS#1 v.1.5, 2048 bit key	C905 (UCS M5) C924 (UCS M4)	CiscoSSL FIPS Object Module (FOM) v6.2	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/SigGen
ECDSA	Cryptographic Signature services	FIPS 186-4, Digital Signature Standard (DSS)	C905 (UCS M5) C924 (UCS M4)	CiscoSSL FIPS Object Module (FOM) v6.2	FCS_CKM.1 FCS_COP.1/SigGen
AES	Used for symmetric encryption/decryption	AES Key Wrap in CBC, CTR and GCM (128 and 256 bits)	C905 (UCS M5) C924 (UCS M4)	CiscoSSL FIPS Object Module (FOM) v6.2	FCS_COP.1/DataEncryption
SHS (SHA-1, 256, 384, 512)	Cryptographic hashing services	Byte Oriented	C905 (UCS M5) C924 (UCS M4)	CiscoSSL FIPS Object Module (FOM) v6.2	FCS_COP.1//Hash
HMAC SHA-1, SHA-256, SHA-384, SHA-512	Keyed hashing services and software integrity test	Byte Oriented	C905 (UCS M5) C924 (UCS M4)	CiscoSSL FIPS Object Module (FOM) v6.2	FCS_COP.1/KeyedHash
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	CTR_DRBG (AES 256)	C905 (UCS M5) C924 (UCS M4)	CiscoSSL FIPS Object Module (FOM) v6.2	FCS_RBG_EXT.1
CVL SSH/TLS	Key Agreement	NIST Special Publication 800-56A	C905 (UCS M5)	CiscoSSL FIPS Object	FCS_CKM.2

Algorithm	Description	Supported Mode	CAVP Cert. #	Module	SFR
			C924 (UCS M4)	Module (FOM) v6.2	
CVL – KAS-ECC	Key Agreement	NIST Special Publication 800-56A	C905 (UCS M5) C924 (UCS M4)	CiscoSSL FIPS Object Module (FOM) v6.2	FCS_CKM.2

The TOE provides cryptography in support of remote administrative management via HTTPS/TLS, the secure connection to an external audit server using TLS and a dedicated SSHv2 secure connection between the Expressway C and E components. The TOE uses the X.509v3 certificate for securing the SSH, and TLS connections.

The TOE also authenticates software updates to the TOE using a published SHA512 hash.

Identification and Authentication

The TOE provides authentication services for administrative users to connect to the TOEs GUI administrator interface. The TOE requires Authorized Administrators to be successfully identified and authenticated 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 using the GUI interface accessed via secure HTTPS connection.

The TOE also provides an automatic lockout when a user attempts to authenticate and enters invalid information. When the threshold for a defined number of authentication attempts fail has exceeded the configured allowable attempts, the user is locked out until an authorized administrator can enable the user account.

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 HTTPS session or via a local console connection. The TOE provides the ability to securely manage:

- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using published hash capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- Ability to configure audit behavior;
- Ability to configure the cryptographic functionality;

- Ability to configure the interaction between TOE components;
- Ability to re-enable an Administrator account;
- Change a user's password;
- Require a user's password to be changed upon next login;
- Configure NTP

The TOE supports the security administrator role. Only the Authorized Administrator can perform the above security relevant management functions.

Authorized Administrators can create configurable login banners to be displayed at time of login and can define an inactivity timeout threshold for each admin interface to terminate sessions after a set period of inactivity has been reached.

Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification and authentication to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally, Cisco Expressway is not a general-purpose operating system and access to Cisco Expressway memory space is restricted to only Cisco Expressway functions.

The TOE initially synchronizes time with an NTP server and then 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.

The TOE performs testing to verify correct operation of the system itself and that of the cryptographic module.

Finally, the TOE can verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software via a published hash

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.

The TOE can also display an Authorized Administrator specified banner on the GUI management interface prior to allowing any administrative access to the TOE.

Trusted Path/Channels

The TOE allows trusted channels to be established to itself from remote Authorized Administrators using HTTPS, initiates outbound TLS secure connection to transmit audit messages to remote syslog servers and uses NTPv4 to secure the connection to the NTP server.

The TOE can also establish trusted paths between the Expressway C and Expressway E components using SSHv2 when configured in Mobile and Remote Access (MRA) mode. In MRA mode, the TOE provides secure a highly secure traversal link to provide a collaboration gateway solution that extends the services and access to users inside and outside of the organization's firewall

In MRA mode, SSHv2 is used to secure the persistent, dedicated connection where Expressway C acts as the SSH server and the Expressway E acts as the SSH client, therefore creating a distributed TOE.

If any of the established trusted channels/paths are unintentionally broken, the connection will need to be re-established as described in this document and the referenced Cisco Expressway X12.5 System Common Criteria Configuration Guide.

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 3: TOE Assumptions

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/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 will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will 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.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the

Assumption	Assumption Definition
	security of the device.
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.COMPONENTS_RUNNING	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
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.

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 4: 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.

Threat	Threat Definition
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.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

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.

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 NDcPP 2.0e
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality referenced below in Section 7.3 of this report is outside the scope of the evaluation.

6 Documentation

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

- Cisco Expressway X12.5 System Common Criteria Security Target, Version 1.5, February 19, 2020
- Cisco Expressway X12.5 System Common Criteria Configuration Guide Version 1.4 February 19, 2020
 - Section 1.3 “Document References” of the CC Guide lists the Cisco Systems documentation, in Table 3, that is also the Common Criteria Configuration Item (CI) List. A hard copy of the hardware installation guides, item 2 from this table, is received with the delivered hardware.

Any additional customer documentation delivered with the product or that may be available through download was not included in the scope of the evaluation and hence should not be relied upon when configuring or using the products in the evaluated configuration.

Consumers are encouraged to download the configuration documentation from the NIAP website to ensure the device(s) are configured as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

This section provides an overview of the Cisco Expressway Target of Evaluation (TOE). Cisco Expressway is an advanced gateway that extends services to users inside and outside the organization firewall, such as desktop share, instant messaging, and presence.

The evaluated configuration consists of the hardware and software, specified below, when configured in accordance with the documentation identified in Section 6 of this report.

The TOE is comprised of both software and hardware. The TOE deployment is the Cisco Expressway instance running X12.5 software installed on one of four different models of the Cisco Unified Computing System™ (Cisco UCS), all of which are described below. The Cisco UCS boxes are administered through a single management entity called the Cisco UCS Manager (Cisco Unified Computing System (UCS) Manager 2.2(3a)). It is assumed the Cisco UCS is setup, configured in their evaluated configurations and ready for use.

The Cisco Unified Computing System™ (Cisco UCS) C220 M4 Rack Server (one rack unit [1RU]) offers up to two Intel® Xeon® E5 Series processors, 24 DIMM slots, eight small form-factor (SFF) disk drives or four large form-factor (LFF) drives, and two 1 Gigabit Ethernet LAN-on-motherboard (LOM) ports. Refer to Table 5 Hardware Models and Specifications for the primary features of the Cisco UCS C220 M4.



Figure 1 Cisco UCS C220 M4 Server

The Cisco Unified Computing System™ (Cisco UCS) C240 M4 Rack Server (two rack unit [2RU]) offers up to two Intel® Xeon® E5 Series processors, 24 DIMM slots, 24 small form-factor (SFF) disk drives or 12 large form-factor (LFF) drives, and two 1 Gigabit Ethernet LAN-on-motherboard (LOM) ports. Refer to Table 5 Hardware Models and Specifications for the primary features of the Cisco UCS C240 M4.



Figure 2 Cisco UCS C240 M4 Server

The Cisco UCS C220 M5 Rack Server is a two-socket 1 Rack Unit (1RU) rack-mount server offers up to two Intel® Xeon® Scalable Series processors. The UCS C220 M5 supports:

- up to 24 DDR4 DIMMs
- up to 10 Small-Form-Factor (SFF) 2.5-inch drives or 4 Large-Form-Factor (LFF) 3.5-inch drives (77 TB storage capacity with all NVMe PCIe SSDs)

- support for 12-Gbps SAS modular RAID controller in a dedicated slot, leaving the remaining PCIe Generation 3.0 slots available for other expansion cards
- Modular LAN-On-Motherboard (mLOM) slot that can be used to install a Cisco UCS Virtual Interface Card (VIC) without consuming a PCIe slot
- dual embedded Intel x550 10GBASE-T LAN-On-Motherboard (LOM) ports

Refer to Table 5 Hardware Models and Specifications for the primary features of the Cisco UCS C220 M5.



Figure 3 Cisco UCS C220 M5 Server

The Cisco Unified Computing System™ (Cisco UCS) C240 M5 2 Rack Unit (2RU) offers up to two Intel® Xeon® Scalable series processors. The C240 M5 supports:

- up to 24 DDR4 DIMM slots
- up to 26 hot-swappable Small-Form-Factor (SFF) 2.5-inch drives, including 2 rear hot-swappable SFF drives
- support for 12-Gbps SAS modular RAID controller in a dedicated slot Modular LAN-On-Motherboard (mLOM) slot that can be used to install a Cisco UCS Virtual Interface Card (VIC) without consuming a PCIe slot.

Also supporting dual 10- or 40-Gbps network connectivity, Dual embedded Intel x550 10GBASE-T LAN-On-Motherboard (LOM) ports and modular M.2 or Secure Digital (SD) cards that can be used for boot.

Refer to Table 1 Hardware Models and Specifications for the primary features of the Cisco UCS C240 M5.



Figure 4 Cisco UCS C240 M5 Server

The TOE includes a web-browsable interface for the system configuration for administrators. Cisco Expressway supports the following operating system browsers:

- Internet Explorer 8, 9, 10, and 11
- Firefox 3 or later
- Chrome

HTTPS is used to secure the connection between Cisco Expressway and the browser.

The TOE will be configured to only use x.509v3-ssh-rsa public key algorithm for secure connection between Expressway-C and Expressway-E in MRA mode. This is a dedicated SSHv2 connection between the two components. The Expressway-C component is configured as the SSH Client and the Expressway-E is configured as the SSH Server. For the outbound port from Expressway-C (private) it is an ephemeral port to Expressway-E (DMZ) port 2222, a listening port. The Expressway-E listens on port 222 for SSH tunnel traffic and the only legitimate sender of SSH traffic is the Expressway-C. Refer to the Cisco Expressway X12.5 System Common Criteria Configuration Guide for details and configuration settings for the evaluated configuration.

TLS is used to secure the connection between Cisco Expressway and the syslog server. This includes any syslog server to which the TOE would transmit syslog messages using TLSv1.1 or TLSv1.2 to secure the connection.

Cisco Expressway X12.5 software is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective services to users inside and outside the organization. Although X12.5 software performs many functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 1.7 Logical Scope of the TOE.

The following figure provides a visual depiction of a TOE deployment. The TOE boundary are the blue boxes.

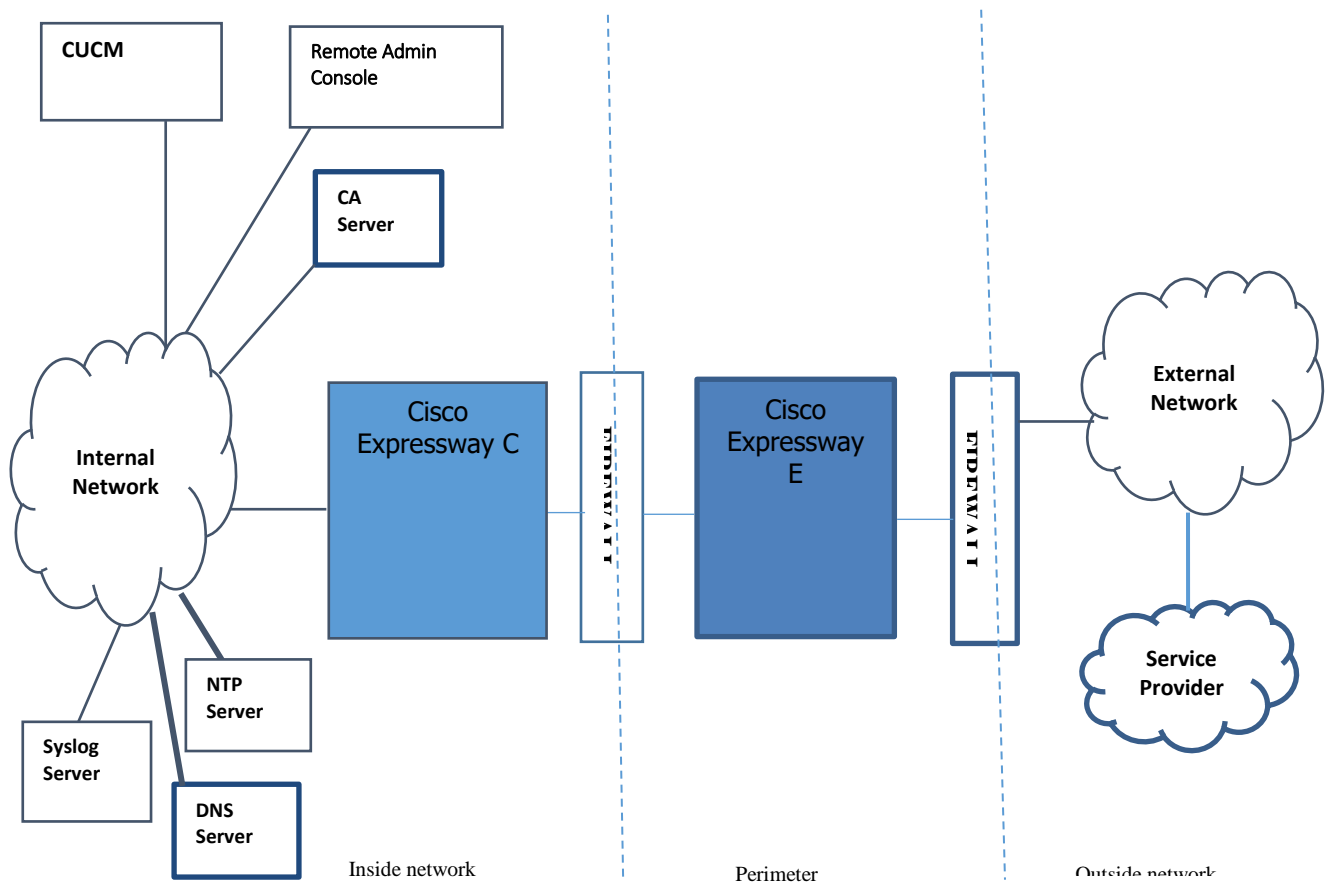



Figure 5 TOE Example Deployment


7.2 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the Cisco Expressway. The TOE hardware platform is at least one of the following Cisco UCS platforms, UCS C220 M4, UCS C240 M4, UCS C220 M5 or the UCS C240 M5. The TOE software is the Cisco Expressway X12.5 software. The network, on which the TOE resides is considered part of the environment. The TOE guidance documentation, the Cisco Expressway Common Criteria Configuration Guide that is also considered to be part of the TOE can be found listed and are downloadable from the NIAP portal <https://www.niap-ccevs.org/>. The TOE hardware is comprised of the following physical specifications as described in Table 5 below:


Table 1 Hardware Models and Specifications

Hardware/Processor/Software	Picture	Size	Power	Interfaces
<p>UCS C220 M4</p> <p>While tested on the specific processor model listed¹, any Intel® Xeon® E526xx v4, processor may be used as part of the evaluated configuration with VMware ESXi 6.0</p> <p>Expressway X12.5 software</p>		<p>1RU: 1.7 x 16.9 x 29.8 in. (4.32 x 43 x 75.6 cm)</p>	<p>Up to two 770 W (AC) hot swappable power supplies or two 1050 W (DC) power supplies. One is mandatory; one more can be added for 1 + 1 redundancy.</p>	<ul style="list-style-type: none"> • Up to 4 LFF or 8 SFF front-accessible, hot-swappable, internal SAS, SATA, or SSD drives, providing redundancy options and ease of serviceability • Various PCIe card ports (dependent on which cards are installed), • Virtual Interface Card (VIC) ports, Converged Network Adapter (CNA) ports, Network Interface Card (NIC) ports, Host Bus Adapter (HBA) ports • I/O performance and flexibility with one x8 half-height and half-length slot, and one x16 full-height and half-length slot • Up to two internal 32GB or two 64GB Cisco FlexFlash drives (SD cards) • One internal USB flash drive <p>Front panel - One KVM console connector (supplies two USB 2.0 connectors, one GA DB15 connector, and one serial port (RS232) RJ45 connector)</p>


¹ Intel® Xeon® E5 2660 v4 Series processor

				<p>Rear panel - One DB15 VGA connector, One RJ45 serial port connector, Two USB 3.0 port connectors, One RJ-45 10/100/1000 Ethernet management port, using Cisco Integrated Management Controller (CIMC) firmware, two Intel i350 embedded (on the motherboard) GbE LOM ports, One flexible modular LAN on motherboard (mLOM) slot that can accommodate various interface cards</p>
<p>UCS C240 M4</p> <p>While tested on the specific processor model listed², any Intel® Xeon® E526xx v4, processor may be used as part of the evaluated configuration with VMWare ESXi 6.0</p> <p>Expressway X12.5 software</p>		<p>2RU: 3.43 x 17.65 x 29.0 in. (8.7 x 44.8 x 73.8 cm)</p>	<p>The server is available with four types of power supplies:</p> <ul style="list-style-type: none"> • 650 W (AC) • 930 W (DC) • 1200 W (AC) • 1400 W (AC) 	<ul style="list-style-type: none"> • Up to 12 LFF or 24 SFF front-accessible, hot-swappable, SAS, SATA, or SSD drives for local storage, providing redundancy options and ease of serviceability <p>Rear panel</p> <ul style="list-style-type: none"> • One DB15 VGA connector • One RJ45 serial port connector • Two USB 3.0 port connectors • One RJ-45 10/100/1000 Ethernet management port, using Cisco Integrated Management Controller (CIMC) firmware • Two Intel i350 embedded (on the motherboard) GbE LOM ports • One flexible modular LAN on motherboard (mLOM) slot that can accommodate various interface cards, Various PCIe card ports (dependent on which cards are installed) • Virtual Interface Card (VIC) ports • Converged Network Adapter (CNA) ports • Network Interface Card (NIC) ports • Host Bus Adapter (HBA) ports

² Intel® Xeon® E5 2660 v4 Series processor

				<p>Front panel</p> <ul style="list-style-type: none"> • One KVM console connector (supplies two USB 2.0 connectors, one VGA, DB15 video connector, and one serial port (RS232) RJ45 connector) support the InfiniBand architecture. <p>A front panel controller provides status indications and control buttons</p>
<p>UCS C220 M5</p> <p>While tested on the specific processor model listed³, any Intel® Xeon® Scalable processor with the Skylake-SP microarchitecture may be used as part of the evaluated configuration with VMware ESXi 6.0</p> <p>Expressway X12.5 software</p>		<p>Height 1.7 in. (4.32 cm)</p> <p>Width 16.89 in. (43.0 cm) including handles: 18.98 in. (48.2 cm)</p> <p>Depth 29.8 in. (75.6 cm) including handles: 30.98 in. (78.7 cm)</p>	<p>Up to two of the following hot-swappable power supplies:</p> <ul style="list-style-type: none"> • 770 W (AC) • 1050 W (AC) • 1050 W V2 (DC) 	<p>Rear panel</p> <ul style="list-style-type: none"> • One 1-Gbps RJ-45 management port (Marvell 88E6176) • Two 10GBase-T LOM ports (Intel X550 controller embedded on the motherboard) • One RS-232 serial port (RJ45 connector) • One DB15 VGA connector • Two USB 3.0 port connectors • One flexible modular LAN on motherboard (mLOM) slot that can accommodate various interface cards <p>Front panel</p> <ul style="list-style-type: none"> • One KVM console connector (supplies two USB 2.0 connectors, one VGA DB15 video connector, and one serial port (RS232) RJ45 connector) <p>Modular LAN on Motherboard (mLOM) slot</p> <p>The dedicated mLOM slot on the motherboard can flexibly accommodate the following cards:</p> <ul style="list-style-type: none"> ☑ Cisco Virtual Interface Cards ☑ Quad Port Intel i350 1GbE RJ45 Network Interface Card (NIC)

³ Intel® Xeon® Scalable Platinum 8160M Series processors

<p>UCS C240 M5</p> <p>While tested on the specific processor model listed⁴, any Intel® Xeon® Scalable processor with the Skylake-SP microarchitecture may be used as part of the evaluated configuration with VMware ESXi 6.0</p> <p>Expressway X12.5 software</p>		<p>Height 3.43 in. (8.70 cm)</p> <p>Width (including slam latches) 17.65 in. (44.8 cm)</p> <p>Including handles: 18.96 in. (48.2 cm)</p> <p>Depth 29.0 in. (73.8 cm)</p> <p>Including handles: 30.18 in. (76.6 cm)</p>	<p>Up to two of the following hot-swappable power supplies:</p> <ul style="list-style-type: none"> • 1050 W (AC) power supply • 1050 W V2 (DC) power supply • 1600 W (AC) power supply 	<p>Rear panel</p> <ul style="list-style-type: none"> • One 1-Gbps RJ-45 management port (Marvell 88E6176) • Two 10GBase-T LOM ports (Intel X550 controller embedded on the motherboard) • One RS-232 serial port (RJ45 connector) • One DB15 VGA connector • Two USB 3.0 port connectors • One flexible modular LAN on motherboard (mLOM) slot that can accommodate various interface cards <p>Front panel</p> <ul style="list-style-type: none"> • One KVM console connector (supplies two USB 2.0 connectors, one VGA DB15 video connector, and one serial port (RS232)) <p>Modular LAN on Motherboard (mLOM) slot</p> <p>The dedicated mLOM slot on the motherboard can flexibly accommodate the following cards:</p> <ul style="list-style-type: none"> • Cisco Virtual Interface Cards • Quad Port Intel i350 1GbE RJ45 mLOM Network Interface Card (NIC)
---	---	---	---	--

7.3 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 6 Excluded Functionality

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

These services can be disabled by configuration settings as described in the Guidance documents (AGD). The exclusion of this functionality does not affect the compliance to the NDcPPv2.0e.

Each platform model (UCS 220 M4, UCS240 M4, UCS 220 M5, UCS 240 M5) includes a serial interface and USB interfaces. The serial port found on each TOE hardware is only used during installation. No USB interfaces are allowed to be used in conjunction with the TOE.

⁴Intel® Xeon® Scalable Platinum 8160M Series processors

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Cisco Expressway X12.5, which is not publicly available. The publicly available Assurance Activities Report provides an overview of testing and the prescribed assurance activities. See Section 3 Test Diagram, p. 29, for the Test Configuration and Test Tools.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the NDcPP 2.0e. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

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

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Cisco Expressway X12.5 to be Part 2 extended and meets the Security Assurance Requirements (SARs) contained in the protection profile (PP). Additionally the evaluator performed the Assurance Activities specified in the NDcPP 2.0e.

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 Expressway X12.5 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 NDcPP 2.0e.

The validators 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 assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP 2.0e related to the examination of the information contained in the TOE Summary Specification.

The validators 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 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 NDcPP 2.0e related to the examination of the information contained in the operational guidance documents.

The validators 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 found that the TOE was identified.

The validators 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 ran the set of tests specified by the Assurance Activities in the NDcPP 2.0e recorded the results in a Test Report, summarized in both the Evaluation Technical Report and Assurance Activities Report.

The validators 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 NDcPP 2.0e and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluator examined sources of information publicly available to identify potential vulnerabilities in the TOE. The sources of the publicly available information are provided below.

The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.

- <http://nvd.nist.gov/>

The evaluator performed the public domain vulnerability searches using the following key words.

- Cisco Systems
- Expressway X12.5 System
- PKIX-SSH 10.1.1
- CiscoSSL 1.0.2n.6.1.368-fips
- UCS C220 M4
- UCS C240 M4
- UCS C220 M5
- UCS C240 M5
- Cisco UCS platforms
- VMware ESXi 6.0
- Intel Xeon E526xx v4
- Intel Xeon Scalable Processors

The evaluator selected the search key words based upon the following criteria.

- The vendor name was searched,
- The product name was searched,

- Key platform features the product leverages were searched

The vulnerability searches were performed on February 12, 2020 .

The TOE was evaluated against the NDcPP version 2.0e. The objective of this analysis and testing is to determine whether the TOE, in its operational environment, has vulnerabilities exploitable by attackers possessing Basic attack potential.

TOE Vulnerability Analysis

Vulnerabilities: National Vulnerability Database
Search Term: Cisco Systems Total Matches: 52 Potential Matches for TOE: 0
Search Term: Expressway X12.5 System Total Matches: 3 Potential Matches for TOE: 3
Search Term: SSH-2.0-X FIPS Total Matches: 0 Potential Matches for TOE: 0
Search Term: CiscoSSL 1.0.2n.6.1.368-fips Total Matches: 0 Potential Matches for TOE: 0
Search Term: UCS C220 M4 Total Matches: 1 Potential Matches for TOE: 0
Search Term: UCS C240 M4 Total Matches: 1 Potential Matches for TOE: 0
Search Term: UCS C220 M5 Total Matches: 0 Potential Matches for TOE: 0
Search Term: UCS C240 M5 Total Matches: 0 Potential Matches for TOE: 0
Search Term: Cisco UCS Platforms Total Matches: 6 Potential Matches for TOE: 1
Search Term: VMWare ESXi 6.0 Total Matches: 24 Potential Matches for TOE: 2
Search Term: Intel Xeon E526xx v4 Total Matches: 0 Potential Matches for TOE: 0
Search Term: Intel Xeon Scalable Processors Total Matches: 1 Potential Matches for TOE: 0
Search Term: TLS Total Matches: 44 Potential Matches for TOE: 0
Search Term: TCP Total Matches: 72 Potential Matches for TOE: 0
Search Term: UDP Total Matches: 21 Potential Matches for TOE: 0
Search Term: SSH Total Matches: 35 Potential Matches for TOE: 0

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 NDcPP 2.0e, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

Although the documents for this evaluation, the ST, this VR, etc., identify 4 models, UCS C220 M4, UCS C240 M4, UCS C220 M5, and UCS C240 M5, only one was tested, UCS 220 M4. The M4 and M5 series have different processors and hence, two different CAVP certificates. M4 models use the VMware ESXi 6.0 on Intel® Xeon® E5 2660 v4 Series processor and have the Cisco Systems, Inc CiscoSSL FIPS Object Module CAVP C924. M5 models use the VMware ESXi 6.0 on Intel® Xeon® Scalable Platinum 8160M Series processor and have the Cisco Systems, Inc CiscoSSL FIPS Object Module CAVP C905. The equivalency analysis required for this testing is explained in section 2 of the AAR.

Table 1 in the AAR (Table 5 in the ST) show the serial ports, e.g., RS-232, RJ-45, USB, VGA, for each of the models. The ST and other documents specify that “All TOE administration occurs either through a secure HTTPS session or via a local console connection.” However, only the remote connection was tested, not the local console connection. This is not explained in the equivalency analysis or elsewhere in the evaluation documentation.

Also note that the AGD “Cisco Expressway X12.5 System Common Criteria Configuration Guide Version 1.3 February 19, 2020” is part of the TOE and can be found on the NIAP portal. The AGD, in section 1.3 Document References, Table 3 Cisco Documentation, lists about a dozen other documents. These have not been reviewed and are not part of the TOE. Their utility in maintaining the evaluated configuration is unknown. The AGD is the only document specifically intended to ensure the product is in the evaluated configuration.

Each platform model (UCS 220 M4, UCS240 M4, UCS 220 M5, UCS 240 M5) includes a serial interface and USB interfaces. The serial port found on each TOE hardware is only used during installation. No USB interfaces are allowed to be used in conjunction with the TOE.

All other concerns and issues are adequately addressed in other parts of this document.

11 Annexes

Not applicable.

12 Security Target

Cisco Expressway X12.5 System Common Criteria Security Target Version 1.5 February 19, 2020

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 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4
5. Cisco Expressway X12.5 System Common Criteria Security Target Version 1.5 February 19, 2020
6. Cisco Expressway X12.5 System Common Criteria Configuration Guide Version 1.4, February 19, 2020
7. Assurance Activity Report for Cisco Expressway X12.5 Version 1.7 February 19, 2020
8. Cisco Expressway X12.5 Evaluation Technical Report Version 2.5 February 12, 2020
9. Vulnerability Assessment for Cisco Expressway X12.5 Version 1.6 February 12, 2020
10. Test Plan for Cisco Expressway X12.5 Version 2.2 February 17, 2020

End of Document