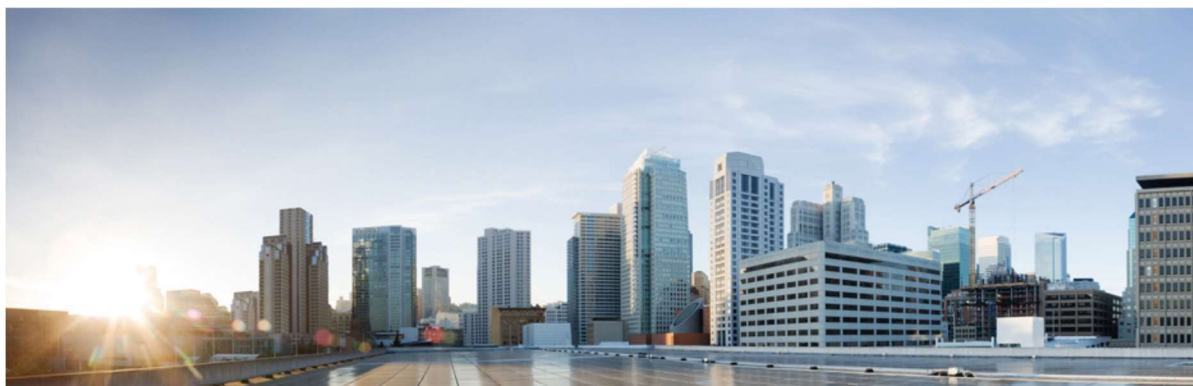




Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12

Security Target

Version: 1.2

Date: December 16 2024



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2024 Cisco Systems, Inc. and/or its affiliates. All rights reserved. This document is Cisco Systems, Inc. Public.

Table of Contents

Document Introduction	9
1 Security Target Introduction	10
1.1 ST and TOE Reference.....	10
1.2 TOE Overview	11
1.3 TOE Product Type	12
1.4 Supported non-TOE Hardware/ Software/ Firmware	12
1.5 TOE Description	13
1.6 TOE Evaluated Configuration	14
1.7 Physical Scope of the TOE.....	15
1.8 Logical Scope of the TOE.....	20
1.8.1 Security Audit.....	20
1.8.2 User Data Protection.....	21
1.8.3 Cryptographic support	21
1.8.4 Identification and authentication.....	21
1.8.5 Security Management.....	21
1.8.6 Firewall	22
1.8.7 Protection of the TSF	22
1.8.8 TOE Access	23
1.8.9 Trusted path/Channels	23
1.9 Excluded Functionality	23
2 Conformance Claims	24
2.1 Common Criteria Conformance Claim.....	24
2.2 Protection Profile Conformance Claim.....	24
3 Security Problem Definition	25
3.1 Assumptions	25
3.2 Threats.....	25
3.3 Organizational Security Policies	26
4 Security Objectives	27
4.1 Security Objectives for the TOE	28
4.2 Security Objectives for the Environment	29
5 Extended Components Definition	30
5.1 Cryptographic Support (FCS).....	30
5.1.1 Random Bit Generation (FCS_RBG_EXT.1)	30

5.2	Firewall (FFW)	31
5.2.1	Stateful Traffic Filtering (FFW_RUL_EXT).....	31
5.3	Identification and Authentication (FIA).....	33
5.3.1	Password Managment (FIA_PMG_EXT)	33
5.4	Protection of the TSF (FPT)	34
5.4.1	Protection of Administrator Passwords (FPT_APW_EXT)	34
5.5	Extended Components Rationale	35
6	Security Requirements	36
6.1	Conventions	36
6.2	TOE Security Functional Requirements	36
6.2.1	Security audit (FAU).....	37
6.2.2	Cryptographic Support (FCS).....	40
6.2.3	User Data Protection (FDP).....	41
6.2.4	Firewall (FFW)	42
6.2.5	Identification and authentication (FIA).....	44
6.2.6	Security management (FMT).....	45
6.2.7	Protection of the TSF (FPT).....	46
6.2.8	TOE Access (FTA)	47
6.2.9	Trusted Path/Channels (FTP)	48
6.3	TOE SFR Dependencies Rationale for SFRs.....	48
6.4	Security Assurance Requirements	51
6.4.1	Security Assurance Requirements	51
6.4.2	Security Assurance Requirements Rationale	52
6.5	Assurance Measures	52
7	TOE Summary Specification	54
7.1	TOE Security Functional Requirement Measures.....	54
8	Rationale	66
8.1	Rationale for TOE Security Objectives	66
8.2	Rationale for the Security Objectives for the Environment	67
8.3	Rationale for requirements/TOE Objectives.....	69
9	CAVP Certificates	78
10	Key Zeroization	79
11	Annex A: References	80

List of Tables

TABLE 1 ACRONYMS.....	7
TABLE 2 ST AND TOE IDENTIFICATION	10
TABLE 3 IT ENVIRONMENT COMPONENTS	12
TABLE 4 HARDWARE MODELS AND SPECIFICATIONS	16
TABLE 5 cEDGE ROUTER SOFTWARE	19
TABLE 6 SD-WAN CONTROLLERS SOFTWARE	19
TABLE 7 EXCLUDED FUNCTIONALITY	23
TABLE 8 ASSUMPTIONS.....	25
TABLE 9 THREATS	25
TABLE 10 SECURITY OBJECTIVES FOR THE TOE	28
TABLE 11 SECURITY OBJECTIVES FOR THE ENVIRONMENT	29
TABLE 12 EXTENDED COMPONENTS	30
TABLE 13 SECURITY FUNCTIONAL REQUIREMENTS	36
TABLE 14 AUDITABLE EVENTS	37
TABLE 17 SFR DEPENDENCY RATIONALE.....	48
TABLE 18 ASSURANCE REQUIREMENTS	51
TABLE 19 ASSURANCE MEASURES	52
TABLE 20 HOW TOE SFRS MEASURES.....	54
TABLE 21 SUMMARY OF MAPPINGS BETWEEN THREATS, POLICIES AND THE SECURITY OBJECTIVES.....	66
TABLE 22 RATIONALE FOR MAPPINGS BETWEEN THREATS, POLICIES AND THE SECURITY OBJECTIVES	66
TABLE 23 MAPPING ASSUMPTIONS AND THE SECURITY OBJECTIVES FOR THE OE	68
TABLE 24 RATIONALE FOR MAPPING ASSUMPTIONS AND THE SECURITY OBJECTIVES FOR THE OE	68
TABLE 25 SECURITY OBJECTIVE TO SECURITY REQUIREMENTS MAPPINGS	69
TABLE 26 SUMMARY OF MAPPINGS BETWEEN IT SECURITY OBJECTIVE TO SFRS.....	71
TABLE 27 CAVP CERTIFICATES	78
TABLE 28 KEY ZEROIZATION	79
TABLE 29 REFERENCES	80

List of Figures

FIGURE 1 DISTRIBUTED TOE EXAMPLE DEPLOYMENT 14

Acronyms

The following acronyms and abbreviations are common and may be used in this Security Target:

Table 1 Acronyms

Acronyms/Abbreviations	Definition
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
ESP	Encapsulating Security Payload
GE	Gigabit Ethernet port
HTTPS	Hyper-Text Transport Protocol Secure
IKE	Internet Key Exchange
IOS	Internet Operating System
IPsec	Internet Protocol Security
OS	Operating System
PoE	Power over Ethernet
SA	Security Association
SD-WAN	Software-Defined WAN
SFP	Small-form-factor pluggable port
SHS	Secure Hash Standard
ST	Security Target
TCP	Transmission Control Protocol
TSC	TSF Scope of Control

TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User Datagram Protocol
WAN	Wide Area Network

Document Introduction

Prepared By:

Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements.

Revision History

Version	Date	Change
0.1	May 2, 2023	Initial Version
0.2	June 2, 2023	Various fixes
0.3	September 19, 2023	Addressing lab comments
0.4	September 27, 2023	Addressing lab comments
0.5	December 11, 2023	Addressing scheme comments
0.6	January 4, 2024	Addressing lab comments
0.7	February 2, 2024	Transition from CC:2022 to CCv3.1 Rel5 and various fixes
0.8	February 26, 2024	Addressing lab comments
0.9	May 6, 2024	Addressing lab and scheme comments
1.0	July 30, 2024	Addressing lab and scheme comments
1.1	August 21, 2024	Addressing lab comments
1.2	December 16, 2024	Addressing lab comments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2024 Cisco Systems, Inc. All rights reserved.

1 Security Target Introduction

The Security Target contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- Extended Components Definition [Section 5]
- Security Requirements [Section 6]
- TOE Summary Specification [Section 7]
- Rationale [Section 8]
- Annex A: References [Section 9]

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex D, and Part 3, Chapter 8.

1.1 ST and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

Table 2 ST and TOE Identification

Name	Description
ST Title	Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12 Security Target
ST Version	1.2
Publication Date	December 16 2024
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12
TOE Hardware Models	cEdge Router models: • ASR1001-HX, ASR1002-HX • ISR4461 • C8300-1N1S-6T, C8300-2N2S-6T • C8500-12X • C8000V machines on VMware ESXi 7.0 on Cisco Unified Computing System™ (UCS), C-Series M5, UCS C220/C240 SD-WAN controllers:

	• vManage virtual machine on VMware ESXI 7.0 on Cisco Unified Computing System™ (UCS), C-Series M5, UCS C220/C240 • vSmart virtual machine on VMware ESXI 7.0 on Cisco Unified Computing System™ (UCS), C-Series M5, UCS C220/C240 • vBond virtual machine on VMware ESXI 7.0 on Cisco Unified Computing System™ (UCS), C-Series M5, UCS C220/C240
TOE Software Version	IOS-XE 17.12.04, SD-WAN 20.12.04
TOE Guidance	Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12 Operational User Guidance and Preparative Procedures
Keywords	Router, Network Device, Firewall, SD-WAN

1.2 TOE Overview

Cisco cEdge routers running IOS XE 17.12 with SD-WAN 20.12 is a distributed TOE which consists of cEdge routers running IOS XE version 17.12 and version 20.12 SD-WAN controller. The cEdge routers are purpose-built routing platforms that include firewall functionality provided by the Cisco IOS XE software. SD-WAN is a software-defined WAN solution that provides a software overlay running over standard network transport and simplifies WAN management. The SD-WAN controllers are separate virtual machines running on the same ESXi server to handle management, provisioning and maintenance of the cEdge routers. The TOE includes the hardware models as defined in Table 4. This Security Target only addresses the functions that provide for the security of the TOE itself as described in Section 1.8 Logical Scope of the TOE. Functionality not described in the Security Target is outside the scope of the evaluation.

1.3 TOE Product Type

The TOE is comprised of both software and hardware and is a distributed system. The hardware is comprised of the cEdge routers as described in 1.7 Physical Scope of the TOE. The software is comprised of the Cisco IOS XE version IOS XE 17.12 images and the SD-WAN version 20.12 images.

Cisco SD-WAN offers a software-defined WAN solution that enables enterprises and organizations to connect users to their applications securely. It provides a software overlay that runs over standard network transport. This virtualized network runs on Cisco's broadly deployed cEdge routers which offer networking, security, and firewall capability. They act as central connection points for distributed WAN traffic, such as traffic to and from remote workers or branch locations.

SD-WAN's centralized controllers, which oversee the control plane of the Cisco SD-WAN fabric, efficiently and securely manage the provisioning, maintenance, and security for the entire overlay network. The vManage controller provides a dashboard that simplifies network operations. It provides centralized configuration, management, operation, and monitoring across the entire SD-WAN fabric.

1.4 Supported non-TOE Hardware/ Software/ Firmware

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

Table 3 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Management Workstation with Web Browser using HTTPS	Yes	This includes any IT Environment Management workstation with a supported web browser installed that is used by the TOE administrator to support TOE administration through HTTPS-TLS protected channels.
Management Workstation with Local Console	Yes	For a physical device this includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration. In the case of the VMs, this function is fulfilled by the ESXi remote local console.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Also referred to as audit server in the ST.

Component	Required	Usage/Purpose Description for TOE performance
VMWare ESXi 7.0	Yes	This includes the hypervisor required for all virtual machines (SD-WAN controllers and C8000V) to run.

1.5 TOE Description

The TOE is a distributed TOE comprised of both software and hardware and includes cEdge routers and SD-WAN controllers. Physical Cisco cEdge routers are further described in 1.7 Physical Scope of the TOE. One Cisco cEdge router, the C8000V, is a virtual machine deployment. The TOE software for cEdge Router platform is comprised of Cisco IOS XE version 17.12. Models include:

- ASR1001-HX, ASR1002-HX
- ISR4461
- C8300-1N1S-6T, C8300-2N2S-6T
- C8500-12X
- C8000V (Virtual Machine)

The Cisco SD-WAN controllers are virtual machine (VM) instances that provide a software overlay which runs over standard network transport. This virtualized network runs on the cEdge routers. Cisco cEdge routers offer networking, security, and firewall capability, and act as central connection points for distributed WAN traffic.

SD-WAN controllers, vManage, vSmart, and vBond, oversee the control plane of the Cisco SD-WAN fabric, and manage the provisioning, maintenance, and security for the entire overlay network.

- Cisco vManage provides a dashboard that simplifies network operations. It provides centralized configuration, management, operation, and monitoring across the entire SD-WAN fabric from a simple graphical dashboard.
- Cisco vSmart controls the flow of data traffic throughout the network. vSmart works with Cisco vBond to authenticate Cisco cEdge devices as they join the network and to orchestrate connectivity among the cEdge routers.
- Cisco vBond automatically orchestrates connectivity between edge routers and the Cisco vSmart Controller(s). It ensures SD-WAN fabric on-boarding. It holds the information needed to authenticate cEdges that wish to join the fabric and also a list of vSmart Controllers and vManage to pass along to the cEdges routers.

All management functions are executed via vManage. All other controllers and all cEdge routers management functions are blocked and handled by vManage. All communications between SD-WAN controllers and cEdge routers are protected via DTLS channels.

The Cisco IOS XE version 17.12 and SD-WAN version 20.12 software is used to meet all of the requirements as specified in this document regardless of the hardware platform.

1.6 TOE Evaluated Configuration

In the evaluated configuration, the TOE consists of at least one cEdge router running IOS XE version 17.12 and deployment of the SD-WAN controller VMs vManage, vSmart, and vBond version 20.12. 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. If the TOE is remotely administered, the management station must connect using SSHv2 or using web browser for the UI over HTTPS. A syslog server can also be used to store audit records.

cEdge router models:

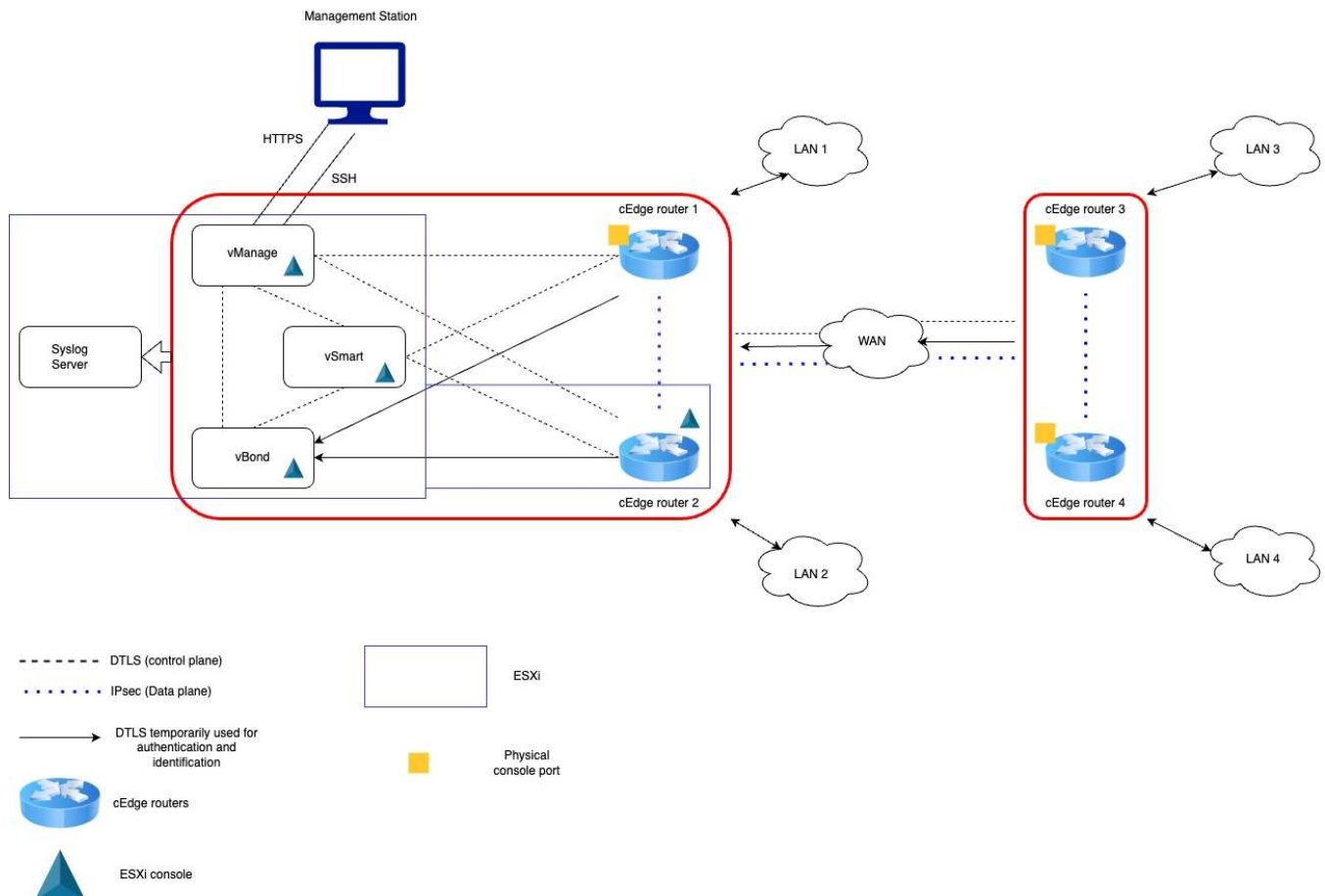
- ASR1001-HX, ASR1002-HX
- ISR4461
- C8300-1N1S-6T, C8300-2N2S-6T
- C8500-12X
- C8000V (Virtual Machine)

SD-WAN controller VMs:

- vManage
- vSmart
- vBond

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a solid red line.

Figure 1 Distributed TOE Example Deployment



The Figure 1 includes the following:

- TOE components (vManage, vBond, vSmart, cEdge routers)
- The following are considered to be in the IT Environment:
 - Management Workstation (UI/HTTPS, console (via ESXi for all VMs, physical for all physical routers, SSH))
 - Audit (Syslog) Server
 - ESXi hypervisor running on Cisco UCS M5

1.7 Physical Scope of the TOE

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

- ASR1000
 - ASR1001-HX
 - ASR1002-HX
- ISR4000
 - ISR4461

- Cat8300
 - C8300-1N1S-6T
 - C8300-2N2S-6T
- Cat8500
 - C8500-12X
- Cat8000V
 - C8000V (Virtual Machine) running on ESXi 7.0 on a Cisco UCS M5

The TOE guidance documentation that is considered to be part of the TOE is the Cisco Cisco cEdge Routers running IOS XE 17.12 with SD-WAN 20.12 Operational User Guidance and Preparative Procedures v0.8 (12/16/2024), a PDF document that can be downloaded from the <http://cisco.com> web site.

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 version 17.12. In addition, the software image is downloadable from the Cisco web site. The hardware is either shipped from Cisco to the customer directly or sent to a distributor which will distribute the hardware to the customer. 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 4 below:

Table 4 Hardware Models and Specifications

Hardware	Processor	Features
ASR1001-HX, ASR1002-HX, 	ASR1001-HX • Intel Xeon E3-1125C v2 (Ivy Bridge) ASR1002-HX • Intel Xeon E3-1125C v2 (Ivy Bridge)	Physical dimensions (H x W x D in.) • ASR1001-HX – 1.71 x 17.3 x 18.38 • ASR1002-HX - 3.5 x 17.3 x 19.25 Interfaces ASR1001-HX • Shared Port Adapters: 0 • Built-in Gigabit Ethernet ports: 8+4 optional • ESP Bandwidth: 60 Gbps ASR1002-HX • Shared Port Adapters: 0 • Built-in Gigabit Ethernet ports: 8 • ESP Bandwidth: 100 Gbps

Hardware	Processor	Features
ISR4461 	ISR4461 Intel Xeon D-1540 (Broadwell)	Physical dimensions (H x W x D in.) - ISR4461 - 1.75 x 17.25 x 17.25 1RU Interfaces 1 USB console port 1 Serial console port RJ45 ISR4461 3 10/100/1000 ports - Aggregate Throuput: 100 to 300 Mbps 2 RJ-45 ports 2 SFP-based ports 2 NIM slots 1 USB 2.0 (Type A) 4/16Default /maximum flash memory GB
C8300-1N1S-6T C8300-2N2S-6T 	C8300-1N1S-6T - Intel Xeon D-1563N (Broadwell) C8300-2N2S-6T - Intel Xeon D-2148NT (Skylake)	Physical dimensions (H x W x D in.) - C8300-1N1S-6T - 1.71 x 17.3 x 16.5 1RU - C8300-2N2S-6T - 3.5 x 17.25 x 18.52 2RU Interfaces C8300-1N1S-6T 1 SM 1 NIM Slots 6 1-Gigabit Ethernet Ports 8GB DRAM 16GB Storage C8300-2N2S-6T 2 SM 2 NIM Slots 6 1-Gigabit Ethernet Ports 8GB DRAM 16GB Storage

Hardware	Processor	Features
C8500-12X 	C8500-12X Intel Xeon D-1563N (Broadwell)	Physical dimensions (H x W x D in.) 1.73 x 17.50 x 18.46 1RU Interfaces C8500-12X 12 1/10GE ports
C8000V on a Cisco UCS C-Series M5 Server running VMWare ESXi 7.0.	Intel Xeon Scalable 2 nd Generation (Cascade Lake) with ESXi 7.0	Physical dimensions (H x W x D in.) N/A VM Interfaces Two or more vNICs, up to maximum allowed by hypervisor
SD-WAN controllers (vManage, vSmart, vBond) on a Cisco UCS C-Series M5 Server running VMWare ESXi 7.0.	Intel Xeon Scalable 2 nd Generation (Cascade Lake) with ESXi 7.0	Cisco UCS C-Series M5 Servers and General-purpose computing hardware Interfaces: All compatible hardware platforms have a dedicated OOB management port and at least two physical Gigabit ethernet interfaces. VM Interfaces: - One dedicated management port with adaptor type VMXNET3 that are mapped to physical ethernet ports on the host server via ESXi - Two or more virtual network interfaces with adaptor type VMXNET3 that are mapped to physical ethernet ports on the host server via ESXi

Software details are listed below per hardware model

Table 5 cEdge router software

Models	Software Version	Image Name	Image hash values
ASR1001-HX, ASR1002-HX,	IOS XE 17.12	asr1000- universalk9.17.12.04 .SPA.bin (751.08 MB)	f2e21de23b557c926b08d9e6c314fe04ed973 f711acb123da40703e9e10a19bf1d1aadcb06 bc7935b7f15942e2c2a46bfb9e6299ee0b753 a15a36550cf7704da
ISR4461		isr4400v2- universalk9.17.12.04 .SPA.bin (816.82 MB)	6d3c18ac645c26482b42974b9dd3f63f4aa52 25605a3e56509d3a691a22a0f6594c4c2b92 4ac74b4f7f19487fbb2fb3e8d326cf55230f410 80b2aa8999296815
C8300-1N1S-6T C8300-2N2S-6T		c8000be- universalk9.17.12.04 .SPA.bin (840.65 MB)	bf90f9a0ff66f48e50fb433d37ad1fa604055ab a90a7e701464246d465084337b156b348d3f 00725a8479c3ca25637438000c88139d0db2 16adb4ae5d15b8390
C8500-12X		c8000aep- universalk9.17.12.04 .SPA.bin (751.08 MB)	626d27c24bf34ca38ca4c99da4901bb0d6f4cf 8dc8ab4f3cf14b2842fe63e21b7357b36036bf 0db0aeacc0d8acc057cd6b1e547d30fcf4145 8efb721bac922ac
C8000V		c8000v- universalk9.17.12.04 .SPA.bin (821.60 MB)	2cebff37a633820a19475606fa6ee9b0d7fb1b 6349a63e59934526cec3cbd7bb6dbb8c2c0c ee4d5a81ba7b582b7a19a662c700eb679cdb aeadd652d3ddc28a614

Software details are listed below per controller

Table 6 SD-WAN controllers software

Models	Software Version	Image Name	Image hash values
vManage	SD-WAN 20.12	viptela-vmanage- 20.12.4-genericx86- 64.ova (4263.92 MB MB)	85bd96506ab39fb1a3f7d06ff5d35cef6b3094 975043104d709fd4bed88129face738b2f427 a2939d16e7ab5c43a6edeabc07766c6fc13a6 fd04d69711e980af
vBond		viptela-edge- 20.12.4-genericx86- 64.ova (178.08 MB)	dc30510c09b041442edcd1da0a8b7b08cf93a 20ace4c0c43d097ff1b4b2ebb3d9fc385285c6 137b33bb57d12f17e0f31cb3c0896e724a758 1979c0bca0952a9b
vSmart		viptela-smart- 20.12.4-genericx86- 64.ova (178.08 MB)	7d1a8e4e971b08327621b3227f66dfa92b50b 8a6e3aef8a62e1c7d3c1b5cf59b17bb453ac8

Models	Software Version	Image Name	Image hash values
			75ddcd24bc3b26b9c469a74a230c173d92c23394e4a6e2b4c80732

1.8 Logical Scope of the TOE

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
- User Data Protection
- Cryptographic support
- Identification and Authentication
- Security Management
- Firewall
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

These features are described in more detail in the subsections below.

1.8.1 Security Audit

The TOE generates audit messages that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include:

- all use of the user identification mechanism;
- all use of the authentication mechanism;
- all modification in the behavior of the functions in the TSF;
- all modifications of the default settings;
- all modifications to the values of the TSF data;
- use of the management functions;
- changes to the time;
- terminations of an interactive session; and
- attempts to use the trusted path functions

The TOE will write audit records to the internal database by default. The TOE provides an interface available for the Authorized Administrator to delete audit data stored locally on the TOE to manage the audit log space.

The logs can be viewed on the TOE using the Web interface and using the CLI. The records include the date/time the event occurred, the event/type of event, the user associated with the event, additional information of the event and its success and/or failure.

1.8.2 User Data Protection

The TOE forwards network packets from source network entities to destination network entities based on available routing information. All packets flowing between cEdge routers are protected with IPsec tunnels. The TOE has the capability to regulate the information flow across its interfaces. Traffic filters can be set in accordance with the presumed identity of the source, the identity of the destination, the transport layer protocol, the source service identifier, and the destination service identifier.

1.8.3 Cryptographic support

The TOE provides cryptography in support of the IPsec functionality. The TOE leverages the IOS Common Cryptographic Module (IC2M) Rel5a.

1.8.4 Identification and authentication

The TOE performs two types of authentication: device-level authentication of cEdge router 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 using DTLS when contacting controllers (cEdge-Control). Device-level authentication is performed via IKE/IPsec mutual authentication. The TOE supports use of IKEv1 key exchange over control channels (cEdge-Control-cEdge) and IKEv2 pre-shared keys for authentication of IPsec tunnels (cEdge-cEdge).

The TOE provides authentication services for administrative users to connect to the TOE's secure CLI administrator interface and to the web GUI via HTTPS. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. 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 provides an automatic lockout when a user attempts to authenticate and enters invalid information. After a pre-defined number of authentication attempts fail exceeding the allowable attempts, the user is locked out until an authorized administrator can enable the user account.

1.8.5 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 (physical connection for physical devices. Remote console via ESXi for C8000v and all SD-WAN controllers) and remotely;
- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE;

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

The TOE supports two separate administrator roles: non-privileged administrator and privileged administrator. Only the privileged administrator can perform the above security relevant management functions. Management of the TSF data is restricted to Security Administrators (privileged administrators). The ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE is restricted to security administrators.

Security 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.

1.8.6 Firewall

The TOE provides stateful traffic firewall functionality including IP address-based filtering to address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance. Address filtering can be configured to restrict the flow of network traffic between protected networks and WAN based on source and/or destination IP addresses. Port filtering can be configured to restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) and/or receiving (destination) port (service). System monitoring functionality includes the ability to generate audit messages for any explicitly defined (permitted or denied) traffic flow. TOE administrators have the ability to configure permitted and denied traffic flows, including adjusting the sequence in which flow control rules will be applied, and to apply rules to any network interface of the cEdge routers.

1.8.7 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. SD-Wan controllers are not general-purpose virtual machines either.

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 or use an external NTP server for automatic synchronization. Finally, the TOE performs testing to verify correct operation of all TOE components including SD-WAN VMs.

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.

The TOE protects all communications between SD-WAN controllers and cEdge routers using DTLS channels.

1.8.8 TOE Access

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

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

1.8.9 Trusted path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over for CLI access (SSH) or HTTPS for web UI access.

1.9 Excluded Functionality

The following functionality is excluded from the evaluation:

Table 7 Excluded Functionality

Excluded Functionality	Exclusion Rationale
SNMP: The Simple Network Management Protocol is an application layer protocol, facilitates the exchange of management information among network devices	SNMP is not associated with Security Functional Requirements claimed.
Telnet	Telnet sends authentication data in plain text. This feature must remain disabled in the evaluated configuration. SSHv2 must be used to secure the trusted path for remote administration for all SSHv2 sessions.
Unified Security Policy / Unified Threat Defense	This feature allows to configure a single unified security policy for firewall and Unified Threat Defense (UTD) security features such as IPS, Cisco URL Filtering, AMP, and TLS/SSL proxy. This is out of scope for the evaluation.

These services will be disabled by configuration settings.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The ST and the TOE it describes are conformant with the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017 o Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017 o Part 3 Conformant

The ST and TOE are package conformant to evaluation assurance package:

- EAL2 augmented with ALC_FLR.2

2.2 Protection Profile Conformance Claim

This ST claims no compliance to any Protection Profiles.

3 Security Problem Definition

This chapter identifies the following:

Significant assumptions about the TOE's operational environment.
 IT related threats to the organization countered by the TOE.
 Organizational security policies for the TOE as appropriate.

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name. Organizational Security Policies (OSPs) are identified as P.osp with "osp" specifying a unique name.

3.1 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 8 Assumptions

Assumption	Assumption Definition
A.ADMIN	All Authorized Administrator are assumed not evil, will follow the administrative guidance and will not disrupt the operation of the TOE intentionally.
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.
A.LOCATE	The processing resources of the TOE and those services provided by the operational environment will be located within controlled access facilities, which will prevent unauthorized physical access.
A.PHYSEC	The hardware components on which the TOE's components are installed are kept physically secure.

3.2 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 9 Threats

Threat	Threat Definition
T.ACCOUNTABILITY	An authorized administrator can not be held accountable for their actions on the TOE because the audit records are not generated, do not include the required data, including properly sequenced through application of correct timestamp.
T.NOAUTH	An unauthorized person (attacker) may attempt to bypass the security of the TOE so as to access data and use security functions and/or non-security functions provided by the TOE to disrupt operations of the TOE.
T.VPN	A malicious user or process may intercept traffic and cause TSF data to be inappropriately accessed (viewed, modified, or deleted) during transfer with a remote VPN endpoint (cedge).
T.ASPOOF	An unauthorized person on an external network may attempt to by-pass the information flow control policy by disguising authentication data (e.g., spoofing the source address) and masquerading as a legitimate user or entity on an internal network.
T.MEDIAT	An unauthorized person may send impermissible information through the TOE, which results in the exploitation of resources on the internal network.
T.NETWORK_COMPROMISE	An unauthorized user may monitor the enterprise network in an attempt to obtain sensitive data, such as passwords, or to modify transmitted data.

3.3 Organizational Security Policies

No Organizational Security Policies (OSPs) have been defined for this TOE.

4 Security Objectives

This section identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

This document identifies objectives of the TOE as O.objective with objective specifying a unique name. Objectives that apply to the IT environment are designated as OE.objective with objective specifying a unique name.

4.1 Security Objectives for the TOE

The following table, Security Objectives for the TOE, identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies.

Table 10 Security Objectives for the TOE

Security Objectives	IT Security Objective Definition
O.ACCESS_CONTROL	The TOE will restrict access to the TOE management functions to the Authorized Administrator.
O.ADMIN	The TOE will provide the Authorized Administrator with a set of privileges to isolate administrative actions and to make the administrative functions available remotely.
O.AUDIT_GEN	The TOE will generate audit records that will include the event, the time that the event occurred, the identity of the user performing the event and the outcome of the event.
O.AUDIT_VIEW	The TOE will provide the Authorized Administrator the capability to review audit data.
O.DATA	The TOE will protect the configuration and user data from unauthorized disclosure.
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all administrative users before granting management access.
O.SELFPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.TIME	The TOE will provide a reliable time stamp for its own use.
O.VPN	The TOE will provide a means to ensure TOE components carrying user data are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity. The TOE must be able to protect the integrity and confidentiality of VPN data.
O.TOE_ADMINISTRATION	The TOE will provide the functions necessary for an administrator to configure the packet filtering rules, as well as the cryptographic aspects of the IPsec protocol that are enforced by the TOE.

Security Objectives	IT Security Objective Definition
O.MEDIATE	The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE.
O.PROTECTED_COMMS	The TOE will protect all communication between it's distributed components from disclosure and modification.

4.2 Security Objectives for the Environment

All of the assumptions stated in section 3.1 are considered to be security objectives for the environment. The following are the non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 11 Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.ADMIN	The Authorized Administrator are well trained and trusted to manage the TOE and to configure the IT environment and required non-TOE devices for the proper network support.
OE.CONNECTION	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.
OE.LOCATE	The processing resources of the TOE and those services provided by the operational environment will be located within controlled access facilities, which will prevent unauthorized physical access.
OE.PHYSEC	The operational environment of the TOE shall have a physical security policy preventing unauthorized physical access to the TOE. The policy must document physical security controls including access control, physical separation of hardware, and monitoring policies to ensure no unauthorized physical access to the TOE is allowed.

5 Extended Components Definition

The Author has defined extended components that are listed below and may be claimed in this Security Target (ST). Extended SFRs are identified by having a label “EXT” at the end of the Security Functional Requirement name.

Table 12 Extended Components

Component Identification	Component Name
FCS_RBG_EXT.1	Random Bit Generation
FFW_RUL_EXT.1	Stateful Traffic Filtering
FIA_PMG_EXT.1	Password Management
FPT_APW_EXT.1	Protection of Administrator Passwords

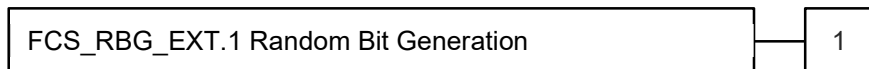
5.1 Cryptographic Support (FCS)

5.1.1 Random Bit Generation (FCS_RBG_EXT.1)

Family Behaviour

Components in this family address the requirements for random bit/number generation. This is a new family defined for the FCS class.

Component Levelling



FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards and seeded by an entropy source.

Management: FCS_RBG_EXT.1

The following actions could be considered for the management functions in FMT:

- a) There are no management activities foreseen

Audit: FCS_RBG_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- a) Minimal: No specific audit requirements

FCS_RBG_EXT.1	Random Bit Generation
----------------------	------------------------------

Hierarchical to: No other components

Dependencies: None

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [assignment: number of software-based sources] software-based noise source, [assignment: number of platform-based sources] platform-based noise source] with a minimum of [selection: 128 bits, 192 bits, 256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate

5.2 Firewall (FFW)

5.2.1 Stateful Traffic Filtering (FFW_RUL_EXT)

Family Behaviour

This requirement is used to specify the behavior of a Stateful Traffic Filter Firewall. The network protocols that the TOE can filter, as well as the attributes that can be used by an administrator to construct a ruleset are identified in this component. How the ruleset is processed (i.e., ordering) is specified, as well as any expected default behavior on the part of the TOE.

Component Levelling



FFW_RUL_EXT.1 Stateful traffic filtering requires the TOE to filter network traffic based on a ruleset configured by an authorized administrator.

Management: FFW_RUL_EXT.1

The following actions could be considered for the management functions in FMT:

- enable/disable a ruleset on a network interface
- configure a ruleset
- specifying rules that govern the use of resources

Audit: FFW_RUL_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal:

- Dynamical definition of rule
- Establishment of a session

FFW_RUL_EXT.1	Stateful Traffic Filtering
----------------------	-----------------------------------

Hierarchical to: No other components

Dependencies: None

FFW_RUL_EXT.1.1 The TSF shall perform Stateful Traffic Filtering on network packets processed by the TOE.

FFW_RUL_EXT.1.2 The TSF shall allow the definition of Stateful Traffic Filtering rules using the following network protocol fields: [assignment: *list of attributes supported by the ruleset*].

FFW_RUL_EXT.1.3 The TSF shall allow the following operations to be associated with stateful traffic filtering rules: permit or drop with the capability to log the operation.

FFW_RUL_EXT.1.4 The TSF shall allow the stateful traffic filtering rules to be assigned to each distinct network interface.

FFW_RUL_EXT.1.5 The TSF shall:

- a) accept a network packet without further processing of stateful traffic filtering rules if it matches an allowed established session for the following protocols: [assignment: *list of supported protocols for which state is maintained*] based on the following network packet attributes: [assignment: *list of attributes associated with each of the protocols*].
- b) Remove existing traffic flows from the set of established traffic flows based on the following: [selection: *session inactivity timeout, completion of the expected information flow*].

FFW_RUL_EXT.1.6 The TSF shall enforce the following default stateful traffic filtering rules on all network traffic: [Selection:

- a) The TSF shall drop and be capable of [selection: counting, logging] packets which are invalid fragments;
- b) The TSF shall drop and be capable of [selection: counting, logging] fragmented packets which cannot be re-assembled completely;
- c) The TSF shall drop and be capable of logging packets where the source address of the network packet is defined as being on a broadcast network;
- d) The TSF shall drop and be capable of logging packets where the source address of the network packet is defined as being on a multicast network;
- e) The TSF shall drop and be capable of logging network packets where the source address of the network packet is defined as being a loopback address;

- f) The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0);
- g) The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is defined as an “unspecified address”;
- h) The TSF shall drop and be capable of logging network packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified; and
- i) [selection: [assignment: other default rules enforced by the TOE],no other rules].

FFW_RUL_EXT.1.7 The TSF shall be capable of dropping and logging according to the following rules: [assignment: *list of specific rules that the TOE is capable of enforcing*].

FFW_RUL_EXT.1.8 The TSF shall process the applicable stateful traffic filtering rules in an administratively defined order.

FFW_RUL_EXT.1.9 The TSF shall deny packet flow if a matching rule is not identified.

FFW_RUL_EXT.1.10 The TSF shall be capable of limiting an administratively configured number of [selection: counted,logged].

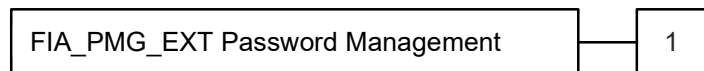
5.3 Identification and Authentication (FIA)

5.3.1 Password Management (FIA_PMG_EXT)

Family Behaviour

The TOE defines the attributes of passwords used by administrative users to ensure that strong passwords and passphrases can be chosen and maintained.

Component Levelling



FIA_PMG_EXT.1 Password management requires the TSF to support passwords with varying composition requirements, minimum lengths, maximum lifetime, and similarity constraints.

Management: FIA_PMG_EXT.1

No management functions

Audit: FIA_PMG_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the ST:

No specific audit requirements

FIA_PMG_EXT.1	Password Management
----------------------	----------------------------

Hierarchical to: No other components

Dependencies: None

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

- a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: "!", "@", "#", "\$", "%", "^", "&", "*", "(", ")", [assignment: other characters]];

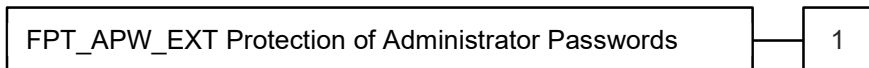
5.4 Protection of the TSF (FPT)

5.4.1 Protection of Administrator Passwords (FPT_APW_EXT)

Family Behaviour

Components in this family ensure that the TSF will protect plaintext credential data such as passwords from unauthorized disclosure.

Component Levelling



FPT_APW_EXT.1 Protection of Administrator passwords requires that the TSF prevent plaintext credential data from being read by any user or subject.

Management: FPT_APW_EXT.1

The following actions could be considered for the management functions in FMT:

- a) None

Audit: FPT_APW_EXT.1

The following actions should be auditable if FAU_GEN Secudity audit data generation is included in the PP/ST:

- a) No audit necessary

FPT_APW_EXT.1	Protection of Administrator Passwords
----------------------	--

Hierarchical to: No other components

Dependencies: None

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

5.5 Extended Components Rationale

The extended classes defined above were included to reflect the modelling of firewall filtering functionality, password management, and password protection which are not readily captured by the existing CC Part 2 components.

FCS_RBG_EXT.1 was included to distinctly and concisely represent the TOE's Random bit generation and align with the Cryptographic Algorithm Validation Program (CAVP) compared to CC Part 2 component.

6 Security Requirements

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, dated: April 2017 and all international interpretations and Extended Components listed in Section 5 of the ST.

6.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Refinement: Indicated with **bold** text and strikethroughs (), if necessary;
- Selection: Indicated with text in brackets;
- Assignment: Indicated with *text* in brackets;
- Assignment within a Selection: Indicated with *text* in brackets;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

6.2 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in the following table are described in more detail in the following subsections.

Table 13 Security Functional Requirements

Class Name	Component Identification	Component Name
FAU: Security audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User identity association
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG.4	Prevention of audit data loss
FCS: Cryptographic support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.4	Timing and event of cryptographic key destruction
	FCS_COP.1(1)	Cryptographic operation
	FCS_COP.1(2)	Cryptographic operation
	FCS_RBG_EXT.1	Random Bit Generation
FDP: User Data Protection	FDP_ITT.1	Basic Internal transfer protection
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Information flow control functions
FFW: Firewall	FFW_RUL_EXT.1	Stateful Traffic Filtering
FIA: Identification and authentication	FIA_AFL.1	Authentication Failure Management
	FIA_PMG_EXT.1	Password Management
	FIA_UID.1	Timing of Authentication
	FIA_UAU.2	Password-based Authentication Mechanism

Class Name	Component Identification	Component Name
	FIA_UAU.7	Protected Authentication Feedback
FMT: Security management	FMT_MOF.1(1)	Management of security functions behaviour
	FMT_MOF.1(2)	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on security roles
FPT: Protection of the TSF	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_STM.1	Reliable Time Stamps
	FPT_ITT.1	Basic internal TSF data transfer
	FPT_TST.1	TSF testing
FTA: TOE Access	FTA_SSL.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_TRP.1	Trusted Path

6.2.1 Security audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shut-down of the audit functions;
- All auditable events for the [not specified] level of audit;
- and *[the events listed in Table 14]*.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information: Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

For each audit event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, *[information specified in column three of Table 14]*.

Table 14 Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_STG.1	None	None
FAU_STG.4	None	None
FCS_CKM.1	None	None
FCS_CKM.2	None	None
FCS_CKM.4	None	None
FCS_COP.1	None	None
FCS_RBG_EXT.1	None	None
FDP_ITT.1	None	None
FDP_IFC.1	None	None
FDP_IFF.1	All decisions on requests for information flow	None
FFW_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport Layer Protocol TOE Interface
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded. Administrator lockout due to excessive authentication failures	Origin of the attempt (e.g., IP address)
FIA_PMG_EXT.1	None	None
FIA_UID.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address)
FIA_UAU.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).

SFR	Auditable Event	Additional Audit Record Contents
FIA_UAU.7	None	None
FMT_MOF.1 (1)	Any attempt to initiate a manual update	None
FMT_MOF.1 (2)	None	None
FMT_MSA.1	None	None
FMT_MSA.3	None	None
FMT_MTD.1	None	None
FMT_SMF.1	All management activities of TSF data	None
FMT_SMR.2	None	None
FPT_APW_EXT.1	None	None
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation. The old and new values for the time. Origin of the attempt (e.g., IP address)
FPT_ITT.1	None	None
FPT_TST.1	None	None
FTA_SSL.1	The termination of a local session by the session locking mechanism.	None
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None
FTA_SSL.4	The termination of an interactive session.	None
FTA_TAB.1	None	None

SFR	Auditable Event	Additional Audit Record Contents
FTP_TRP.1	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None.

6.2.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.1.3 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail.

6.2.1.4 FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [overwrite the oldest stored audit records] and *[no other actions]*, if the audit data storage is full.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm: [CTR_DRBG] and specified cryptographic key sizes *[256 bits]* that meet the following :*[SP 800-90A]*.

6.2.2.2 FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *[DTLS]* that meets the following: *[RFC 6347]*

6.2.2.3 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *[zeroize, overwritten with new value of the key]* that meets the following *[none]*.

6.2.2.4 FCS_COP.1(1) Cryptographic operation

FCS_COP.1 The TSF shall perform [*encryption, decryption*] in accordance with a specified cryptographic algorithm [*AES-GCM*] and cryptographic key sizes [*256 bit*] that meet the following: [*ISO 18033-3 and ISO 19772*]

6.2.2.5 FCS_COP.1(2) Cryptographic operation

FCS_COP.1 The TSF shall perform [*hashing*] in accordance with a specified cryptographic algorithm [*HMAC*] and cryptographic key sizes [*256 bit*] that meet the following: [*FIPS 198*]

6.2.2.6 FCS_RBG_EXT.1 Random bit generation (RBG)

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [*CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [*[1] platform based noise source*] with a minimum of [*256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_ITT.1 Basic Internal transfer protection

FDP_ITT.1.1 The TSF shall enforce the [*VPN SFP*] to prevent the [*disclosure, modification*] of user data when it is transmitted between physically-separated parts of the TOE.

6.2.3.2 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [*FIREWALL SFP*] on [

- *subjects: packets received by cEdge Router interfaces,*
- *information: packet headers, source zone, desination zone*
- *operations that cause controlled information to flow to and from controlled subjects covered by the SFP: drop, pass, inspect].*

6.2.3.3 FDP_IFF.1 Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [*FIREWALL SFP*] based on the following types of subject and information security attributes: [

Subjects	Information	Security Attributes
<i>packets received</i>	<i>packet header</i>	<i>Source IP address</i>

<i>packets received</i>	<i>packet header</i>	<i>Destination IP address</i>
<i>packets received</i>	<i>packet header</i>	<i>Protocol (ICMP, TCP, or UDP)</i>
<i>packets received</i>	<i>packet header</i>	<i>Source port (TCP port or UDP port)</i>
<i>packets received</i>	<i>packet header</i>	<i>Destination port (TCP port or UDP port)</i>
<i>packets received</i>	<i>source zone</i>	<i>Zone ID of cEdge Router ingress interface</i>
<i>packets received</i>	<i>destination zone</i>	<i>Zone ID of cEdge Router destination interface</i>

]

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *[an administratively-defined rule within an active policy explicitly allows traffic matching any combination of information security attribute values]*.

FDP_IFF.1.3 The TSF shall enforce the *[none]*.

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: *[none]*.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based ~~on~~ **if any of** the following rules apply: [

- *An administratively-defined rule within an active policy that explicitly blocks traffic matching any combination of the information security attribute values is a higher priority rule within the policy than any rule that would explicitly allow the information flow;*
- *The information received via the ingress interface contains a presumed address of the source subject that is known by the TOE's routing table to not be reachable via the ingress interface;*
- *The presumed address of the source subject is a broadcast address;*
- *The presumed address of the source subject is on a loopback network.]*

6.2.4 Firewall (FFW)

6.2.4.1 FFW_RUL_EXT.1 Stateful Traffic Filtering

FFW_RUL_EXT.1.1 The TSF shall perform stateful traffic filtering on network packets processed by the TOE.

FFW_RUL_EXT.1.2 The TSF shall allow the definition of stateful traffic filtering rules using the following network protocol fields:

[

- *ICMPv4*
 - *Type*
 - *Code*
- *IPv4*

- Source Address
- Destination Address
- Transport Layer Protocol
- TCP
 - Source Port
 - Destination Port
- UDP
 - Source Port
 - Destination Port

And distinct interface.]

FFW_RUL_EXT.1.3 The TSF shall allow the following operations to be associated with stateful traffic filtering rules: permit or drop with the capability to log the operation.

FFW_RUL_EXT.1.4 The TSF shall allow the stateful traffic filtering rules to be assigned to each distinct network interface.

FFW_RUL_EXT.1.5 The TSF shall

- a) Accept a network packet without further processing of stateful traffic filtering rules if it matches an allowed established session for the following protocols: [TCP, UDP, [no other protocols]] based on the following *network packet attributes*: [
 1. *TCP: source and destination addresses, source and destination ports, sequence number, Flags;*
 2. *UDP: source and destination addresses, source and destination ports;*
- b) Remove existing traffic flows from the set of established traffic flows based on the following: [session inactivity timeout, completion of the expected information flow].

FFW_RUL_EXT.1.6 The TSF shall enforce the following default stateful traffic filtering rules on all network traffic: [

- a) The TSF shall drop and be capable of [counting, logging] packets which are invalid fragments;
- b) The TSF shall drop and be capable of [counting, logging] fragmented packets which cannot be re-assembled completely;
- c) The TSF shall drop and be capable of logging packets where the source address of the network packet is defined as being on a broadcast network;
- d) The TSF shall drop and be capable of logging packets where the source address of the network packet is defined as being on a multicast network;
- e) The TSF shall drop and be capable of logging network packets where the source address of the network packet is defined as being a loopback address;
- f) The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0);
- g) The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is defined as an “unspecified address”;
- h) The TSF shall drop and be capable of logging network packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified; and
- i) [selection: no other rules].]

FFW_RUL_EXT.1.7 The TSF shall be capable of dropping and logging according to the following rules: [

- a) *The TSF shall drop and be capable of logging network packets where the source address of the network packet is equal to the address of the network interface where the network packet was received;*
- b) *The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is a link-local address;*
- c) *The TSF shall drop and be capable of logging network packets where the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received.]*

FFW_RUL_EXT.1.8 The TSF shall process the applicable stateful traffic filtering rules in an administratively defined order.

FFW_RUL_EXT.1.9 The TSF shall deny packet flow if a matching rule is not identified.

FFW_RUL_EXT.1.10 The TSF shall be capable of limiting an administratively defined number of half-open TCP connections. In the event that the configured limit is reached, new connection attempts shall be dropped and the drop event shall be [logged].

6.2.5 Identification and authentication (FIA)

6.2.5.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when [an Administrator configurable positive integer within [1 to 25]] unsuccessful authentication attempts occur related to [Administrators attempting to authenticate remotely using a password].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password until an authorized Administrator unlocks the locked user account].

6.2.5.2 FIA_PMG_EXT.1 Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

- a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, “)”, “.”];

6.2.5.3 FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [displaying the warning banner in accordance with FTA_TAB.1] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated action on behalf of that user.

6.2.5.4 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.5.5 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only [*obscured feedback*] to the **administrative user** ~~user~~ while the authentication is in progress.

6.2.6 Security management (FMT)

6.2.6.1 FMT_MOF.1(1) Management of Security Functions Behavior

FMT_MOF.1.1(1) The TSF shall restrict the ability to [enable] the functions [*to perform manual update*] to [Security Administrators].

6.2.6.2 FMT_MOF.1(2) Management of Security Functions Behavior

FMT_MOF.1.1(2) The TSF shall restrict the ability to [disable, enable, modify the behaviour of] the functions [*to transmit audit data to an external IT entity*] to [Security Administrators].

6.2.6.3 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the [*FIREWALL SFP*] to restrict the ability to [change default, query, modify, delete] the security attributes [*listed in FDP_IFF. 1*)] to [Security Administrators].

6.2.6.4 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1 The TSF shall enforce the [*FIREWALL SFP*] to provide [restrictive] default values for **information flow control rules** ~~security attributes~~ that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow [Security Administrators] to specify alternative initial values to override the default values when an object or information is created.

6.2.6.5 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [manage] the [TSF data] to [Security Administrators].

6.2.6.6 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:[

- *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 configure the authentication failure parameters for FIA_AFL.1;*
- *Manually unlock a locked administrator account;*
- *Ability to configure firewall rules;*
- *Update the TOE software]*

6.2.6.7 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles: [
Security Administrator
cEdge Administrator]

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions [

- *The Security Administrator role shall be able to administer the TOE locally;*
- *The Security Administrator role shall be able to administer the TOE remotely;*
- *The cEdge Administrator role shall be able to access the TOE locally;*
- *The cEdge Administrator role shall be able to access the TOE remotely.]*

are satisfied;

6.2.7 Protection of the TSF (FPT)

6.2.7.1 FPT_APW_EXT.1 Extended: Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

6.2.7.2 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2.7.3 FPT_ITT.1 Basic Internal TSF data transfer protection

FPT_ITT.1: The TSF shall protect TSF data from [disclosure, modification] when it is transmitted between separate parts of the TOE.

6.2.7.4 FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self-tests [during initial start-up, periodically during normal operation] to demonstrate the correct operation of [*the TSF*].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [the cEdge routers configuration].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [TSF].

6.2.8 TOE Access (FTA)

6.2.8.1 FTA_SSL.1 (1) TSF-initiated Session Locking

FTA_SSL.1.1 The TSF shall lock an interactive session after [*10 to 1092 minutes*] by:

- a) clearing or overwriting display devices, making the current contents unreadable;
- b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [*identification and authentication*].

6.2.8.2 FTA_SSL.1 (2) TSF-initiated Session Locking

FTA_SSL.1.1 The TSF shall lock an interactive session after [*1 to 300 minutes*] by:

- a) clearing or overwriting display devices, making the current contents unreadable;
- b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [*identification and authentication*].

6.2.8.3 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1: The TSF shall terminate interactive session after a [*Security Administrator-configurable time interval of session inactivity*].

6.2.8.4 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 The TSF shall allow ~~user-initiated~~ **Administrator-initiated** termination of the ~~user's~~ **Administrator's** own interactive session.

6.2.8.5 FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1: Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

6.2.9 Trusted Path/Channels (FTP)

6.2.9.1 FTP_TRP.1 Trusted Path

FTP_TRP.1.1: The TSF shall provide a communication path between itself and [remote] users administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The TSF shall permit [remote users Administrators] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [initial user Administrator authentication, and all remote administration actions].

6.3 TOE SFR Dependencies Rationale for SFRs

This section of the Security Target demonstrates that the identified TOE Security Functional Requirements include the appropriate hierarchical SFRs and dependent SFRs. The following table lists the TOE Security Functional Components and the Security Functional Components, each are hierarchical to and dependent upon and any necessary rationale.

N/A in the Rationale column means the Security Functional Requirement has no dependencies and therefore, no dependency rationale is required. Satisfied in the Rationale column means the Security Functional Requirements dependency was included in the ST.

Table 15 SFR Dependency Rationale

SFR	Dependency	Rationale
FAU_GEN.1	FPT_STM.1	Met by FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 included Met by FIA_UID.1
FAU_STG.1	FAU_GEN.1	Met by FAU_GEN.1
FAU_STG.4	FAU_STG.1	Met by FAU_STG.1
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 or FCS_CKM.4	Met by FCS_CKM.2 Met by FCS_COP.1

SFR	Dependency	Rationale
FCS_CKM.2	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.4	Met by FCS_CKM.1 Met by FCS_CKM.4
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	Met by FCS_CKM.1
FCS_COP.1(1)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.4	Met by FCS_CKM.1 Met by FCS_CKM.4
FCS_COP.1(2)	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.4	Met by FCS_CKM.1 Met by FCS_CKM.4
FCS_RBG_EXT.1	None	None
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Met by FDP_IFC.1
FDP_IFC.1	FDP_IFF.1	Met by FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Met by FDP_IFC.1 Met by FMT_MSA.3
FFW_RUL_EXT.1	None	None
FIA_AFL.1	FIA_UAU.1	Met by FIA_UAU.2
FIA_PMG_EXT.1	None	None
FIA_UID.1	None	None
FIA_UAU.2	FIA_UID.1	Met by FIA_UID.1
FIA_UAU.7	FIA_UAU.1	Met by FIA_UAU.2

SFR	Dependency	Rationale
FMT_MOF.1 (1)	FMT_SMR.1	Met by FMT_SMR.2
	FMT_SMF.1	Met by FMT_SMF.1
FMT_MOF.1 (2)	FMT_SMR.1	Met by FMT_SMR.2
	FMT_SMF.1	Met by FMT_SMF.1
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	Met by FDP_IFC.1
	FMT_SMF.1	Met by FMT_SMF.1
	FMT_SMR.1	Met by FMT_SMR.2
FMT_MSA.3	FMT_MSA.1	Met by FMT_MSA.1
	FMT_SMR.1	Met by FMT_SMR.2
FMT_MTD.1	FMT_SMF.1	Met by FMT_SMF.1
	FMT_SMR.1	Met by FMT_SMR.2
FMT_SMF.1	None	None
FMT_SMR.2	FIA_UID.1	Met by FIA_UID.1
FPT_APW_EXT.1	None	None
FPT_STM.1	None	None
FPT_ITT.1	None	None
FPT_TST.1	None	None
FTA_SSL.1	FIA_UAU.1	Met by FIA_UAU.2
FTA_SSL.3	None	None
FTA_SSL.4	None	None
FTA_TAB.1	None	None
FTP_TRP.1	None	None

6.4 Security Assurance Requirements

6.4.1 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in the table below:

Table 16 Assurance Requirements

Assurance Class	Components	Components Description
Security Target (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE summary specification
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic Design
Guidance documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative Procedures
Life cycle support (ALC)	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw Reporting Procedures
Tests (ATE)	ATE_IND.2	Independent testing - sample
	ATE_FUN.1	Functional testing
	ATE_COV.1	Evidence of coverage
Vulnerability assessment (AVA)	AVA_VAN.2	Vulnerability analysis

6.4.2 Security Assurance Requirements Rationale

This Security Target claims conformance to EAL2 augmented with ALC_FLR.2. This target was chosen to ensure that the TOE has a moderate level of assurance in enforcing its security functions when instantiated in its intended environment which imposes no restrictions on assumed activity on applicable networks. Augmentation was chosen to address having flaw remediation procedures and correcting security flaws as they are reported.

6.5 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Cisco to satisfy the assurance requirements. The table below lists the details.

Table 17 Assurance Measures

Component	How requirement will be met
ADV_FSP.2	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.
ADV_ARC.1	The architecture description provides the justification how the security functional requirements are enforced, how the security features (functions) cannot be bypassed, and how the TOE protects itself from tampering by untrusted active entities. The architecture description also identifies the system initialization components and the processing that occurs when the TOE is brought into a secure state (e.g. transition from a down state to the initial secure state (operational)).
ADV_TDS.1	The TOE design describes the TOE security functional (TSF) boundary and how the TSF implements the security functional requirements. The design description includes the decomposition of the TOE into subsystems and/or modules, thus providing the purpose of the subsystem/module, the behavior of the subsystem/module and the actions the subsystem/module performs. The description also identifies the subsystem/module as SFR (security function requirement) enforcing, SFR supporting, or SFR non-interfering; thus identifying the interfaces as described in the functional specification. In addition, the TOE design describes the interactions among or between the subsystems/modules; thus providing a description of what the TOE is doing and how.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.2	The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s), identifies

Component	How requirement will be met
ALC_CMS.2	the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error. The TOE will also be provided along with the appropriate administrative guidance.
ALC_DEL.1	The Delivery document describes the delivery procedures for the TOE to include the procedure on how to download certain components of the TOE from the Cisco website and how certain components of the TOE are physically delivered to the user. The delivery procedure detail how the end-user may determine if they have the TOE and if the integrity of the TOE has been maintained. Further, the delivery documentation describes how to acquire the proper license keys to use the TOE components.
ALC_FLR.2	Cisco documents the flaw remediation and reporting procedures so that security flaw reports from TOE users can be appropriately acted upon, and TOE users can understand how to submit security flaw reports to the developer.
ATE_IND.2	Cisco will provide the TOE for testing.
ATE_FUN.1	The Test document(s) consist of a test plan describes the test configuration, the approach to testing, and how the subsystems/modules and TSFI (TOE security function interfaces) has been tested against its functional specification and design as described in the TOE design and the security architecture description. The test document(s) also include the test cases/procedures that show the test steps and expected results, specify the actions and parameters that were applied to the interfaces, as well as how the expected results should be verified and what they are. Actual results are also included in the set of Test documents.
ATE_COV.1	
AVA_VAN.2	Cisco will provide the TOE for testing.

7 TOE Summary Specification

7.1 TOE Security Functional Requirement Measures

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 18 How TOE SFRs Measures

TOE SFRs	How the SFR is Met
FAU_GEN.1	<u>SD-WAN Controllers only</u> The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include: startup and shutdown of the audit mechanism cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table within the FAU_GEN.1 SFR, "Auditable Events Table"). Each of the events is specified in syslog records in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred such as generating keys, including the type of key. The audit trail consists of the individual audit records; one audit record for each event that occurred. The audit record can contain up to 80 characters and a percent sign (%), which follows the time-stamp information. As noted above, the information includes at least all of the required information. Example audit events are included below: <i>May 2 08:54:11 vManage-1 sshd[50081]: Accepted keyboard-interactive/pam for admin from 10.26.166.81 port 61370 ssh2</i> <i>May 2 08:54:11 vManage-1 sshd[50081]: pam_unix(sshd:session): session opened for user admin(uid=1000) by (uid=0)</i> The logging buffer size can be configured from a range of 1 to 20 megabytes. It is noted to not make the buffer size too large because the TOE could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the TOE. However, this value is the maximum available, and the buffer size should not be set to this amount. The log buffer is circular, so newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging privileged EXEC command to view the audit records. The first message displayed is the oldest message in the buffer. There are other associated commands to clear the buffer, to set the logging level, etc. The logs can be saved to flash memory so records are not lost in case of failures or restarts. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.

TOE SFRs	How the SFR is Met
	The administrator can configure the audit file rotation before a file is discarded from 1 to 10. The administrator can set the level of the audit records to be sent to a syslog server. All audit messages can be sent to a syslog server. The audit records are transmitted to the syslog server. If the communications to the syslog server is lost, the TOE generates an audit record and all permit traffic is denied until the communication is re-established. <u>cEdge routers only</u> The configuration for cEdge routers logging is done via a template in vManage. The template allows an administrator to configure the maximum file and the file rotation.
FAU_GEN.2	The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result, they are traceable to a specific user. For example, a human user, user identity or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented. A sample audit record from vManage is provided below: May 2 08:52:29 vManage-1 login[1049]: pam_unix(login:auth): authentication failure; logname=LOGIN uid=0 euid=0 tty=/dev/tty0 ruser= rhost= user=sdwan-admin May 2 08:52:30 vManage-1 getty[48346]: tcgetattr: Input/output error May 2 08:52:32 vManage-1 login[1049]: FAILED LOGIN (1) on '/dev/tty0' FOR 'sdwan-admin', Authentication failure May 2 08:53:43 vManage-1 sshd[50081]: username_raw:admin, username:, remote_ip:10.26.166.81 May 2 08:53:45 vManage-1 sshd[50085]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.26.166.81 user=admin May 2 08:53:49 vManage-1 sshd[50081]: error: PAM: Authentication failure for admin from 10.26.166.81
FAU_STG.1 FAU_STG.4	The authorized administrator can view the audit log records via the GUI interface (vManage only) or via the CLI interface (all TOE components). There is no interface to modify an audit record. However, the authorized administrator can delete records to manage the log file space. The audit log file space can also be managed by configured log retention policies as defined by the Authorized Administrator.

TOE SFRs	How the SFR is Met
FCS_CKM.1 FCS_CKM.2 FCS_CKM.4	The cEdge routers generate keys and send them to vSmart via DTLS tunnels. vSmart then redistributes the keys to other routers along with via DTLS channels. AES symmetric cryptographic keys used for encryption/dectyption are generated with a key size of 256 bit on the cEdge routers using a Counter DRBG as defined in FCS_RBG_EXT.1 as described In SP 800-90A. The TOE acts as both a sender and receiver for IPsec communications between cEdge routers. Tunnels are established in 2 steps. The cEdge routers create outbound and inbound tunnels using the keys distributed by vSmart. Keys are destroyed (zeroized) when no longer needed or overwritten every 24 hours when a new key is generated and sent to the routers.
FCS_COP.1	The TOE provides symmetric encryption and decryption capabilities using AES in GCM mode (256 bits) as described in ISO/IEC 18033-3 and ISO/IEC 19772. AES is implemented in IPsec protocols. For IPsec Security Association (SA), the authentication integrity esp-sha256-hmac (HMAC-SHA-256) with message digest sizes of 256 bits is part of the IPsec SA transform-set to be used with all cEdge routers for user data transfer.
FCS_RBG_EXT.1	The TOE implements a NIST-approved AES-CTR DRBG, as specified in ISO/IEC 18031:2011 seeded by an entropy source that accumulates entropy from a TSF-software based noise source.
FDP_ITT.1	The TOE automatically creates IPsec tunnels (transport mode) between cEdge routers allowing protection and confidentiality of all user data sent to and from all routers. All rules are configured at vManage and pushed to the cEdge routers by vSmart via DTLS channels. All traffic is subject to filtering based on rules defined in FFW_RUL_EXT.1.
FDP_IFC.1 FDP_IFF.1	<u>cEdge routers only</u> All traffic going through the TOE is filtered using ACLs (Access Control Policy) and is either dropped, or forwarded by the TOE. The TOE provides traffic filtering of IPV4 network traffic, and filtering will be stateful or stateless depending on whether the administrator configured the ACL rule action as “pass” (stateless) or “inspect” (stateful). During startup, when the TOE configuration has yet to be loaded, no traffic can flow through the any of its interfaces. No traffic can flow through the TOE interfaces until booting has completed and the configuration has been loaded. The firewall uses a flexible and easily understood zone-based model for traffic inspection. A zone is a grouping of one or more VPNs. Grouping VPNs into

TOE SFRs	How the SFR is Met
	zones allows you to establish security boundaries in your overlay network so that you can control all data traffic that passes between zones. The firewall is also referred as Zone-Based Firewall (ZBFW).
FFW_RUL_EXT.1	<u>cEdge routers only</u> When ACL rules contain the “inspect” action, the TOE provides stateful traffic filtering of IPV4 network traffic. An authorized administrator can define the traffic rules and apply them to any interface on cEdge routers to filter traffic based on IP parameters including source and destination address, transport layer protocol, type and code, and TCP and UDP port numbers. The TOE allows establishment of communications between remote endpoint, and tracks the state of each session (e.g. initiated, established and tear-down), and will clear established session after proper tear-down is completed as defined by each protocol, or when session timeouts are reached. To track the statefulness of sessions to/from and through the firewall, the cEdge routers maintain a table of connections in various connection states. The TOE updates the table (adding, and removing connections, and modifying states as appropriate) based on configurable connection timeout limits, and by inspecting fields within the packet headers. To ensure that established stateful sessions are properly removed, the IOS XE firewall can be configured to remove connections based on normal completion and/or timeout conditions. For example, the firewall can be configured to remove TCP connections after a period of inactivity, or to remove UDP sessions after a certain amount of time has elapsed. Additionally, the firewall can be configured to indicate when session removal becomes effective, such as before the next packet that might match the session is processed. The proper session establishment and termination followed by the TOE is as defined in the following RFCs: • RFC 792 (ICMPv4) • RFC 791 (IPv4) • RFC 793, section 2.7 Connection Establishment and Clearing (TCP) During initialization/startup (while the TOE is booting) the configuration has yet to be loaded, and no traffic can flow through any of its interfaces. No traffic can flow through the TOE interfaces until the POST (Power on Self Test) has completed, and the configuration has been loaded. If any aspect of the POST fails during boot, the TOE will reload without forwarding traffic. If a critical component of the TOE fails while the TOE is in an operational state, the traffic flow will be stopped. If a component such as a network interface, which is not critical to the operation of the TOE, but may be critical to one or more traffic flows, fails while the TOE is operation, the TOE will continue to function, though all traffic flows through the failed network interface(s) will be dropped.

TOE SFRs	How the SFR is Met
	When traffic exceeds the maximum rate the TOE can handle, the TOE drops the excess traffic and ensures that no traffic that wouldn't pass stateful traffic filtering rules would be passed through. The TOE supports filtering of the following protocols and enforces proper session establishment, management, and termination as defined in each protocol's RFC, using the following filtering options configured via vManage. Filtering can be based on different matching conditions: • Protocol • Source Data Prefix • Source Port • Destination Data Prefix • Destination Port And the actions can be configured as follow: • Inspect ○ Additional: log • Drop ○ Additional: log Each firewall rule on the TOE has an admin-specified action ("permit", "deny", or "inspect"), and each rule can be configured to cause a log message to be generated when a new session matches the rule. The rules are either enforced on specific zones (VPNs) or specific interfaces. Traffic flows that originate in a given zone are allowed to proceed to another zone based on the policy between the two zones. A zone is a grouping of one or more VPNs. Grouping VPNs into zones allows you to establish security boundaries in your overlay network so that you can control all data traffic that passes between zones. Zone configuration consists of the following components: • Source zone—A grouping of VPNs where the data traffic flows originate. A VPN can be part of only one zone. • Destination zone—A grouping of VPNs where the data traffic flows terminate. A VPN can be part of only one zone. • Firewall policy—A security policy, similar to a localized security policy, that defines the conditions that the data traffic flow from the source zone must match to allow the flow to continue to the destination zone. Firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, ICMP, and applications. Matching flows for prefixes, ports, and protocols can be accepted or dropped, and the packet headers can be logged. Nonmatching flows are dropped by default. Matching applications are denied. • Zone pair—A container that associates a source zone with a destination zone and that applies a firewall policy to the traffic that flows between the two zones. All cEdge routers have default policies that would block and log invalid packet fragments, fragmented packets which cannot be re-assembled completely, packets where the source address of the network packet is defined as being on a broadcast network, packets where the source address of the network packet is defined as being on a multicast network, packets where the source address

TOE SFRs	How the SFR is Met
	of the network packet is defined as being a loopback address, packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0), packets where the source or destination address of the network packet is defined as an “unspecified address and packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified. All cEdge routers drop and log all packets where the source address of the network packet is equal to the address of the network interface where the network packet was received, packets where the source or destination address of the network packet is a link-local address and packets where the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received by default. The TOE allows administrator to configure the rules and to set the sequence in which they are applied. The rules are always applied in an ascending order. If the ordering is changed, the enforcing of the rules will change automatically when processing the network traffic. An implicit “Deny All” rule is applied to all interfaces/zones to which an explicit rule has been applied. The implicit “Deny All” rule is implemented as the last rule following all administrator defined rules and will drop all traffic that has not been explicitly permitted to flow through cEdge routers. The TOE allows administrators to configure the maximum number of half-open TCP connections allowed by creating a rule defining the limits. Once the limit is reached, the TOE will drop any additional packets.
FIA_AFL.1	The TOE provides the privileged administrator the ability to specify the maximum number of unsuccessful authentication attempts before privileged administrator or non-privileged administrator is locked out through the administrative CLI and GUI using a privileged CLI command. While the TOE supports a range from 1-25, in the evaluated configuration, the maximum number of failed attempts is recommended to be set to 3. All successive unsuccessful authentication attempts are logged on the router. When a privileged administrator or non-privileged administrator attempting to log into the administrative CLI or GUI reaches the administratively set maximum number of failed authentication attempts, the user will not be granted access to the administrative functionality of the TOE until a privileged administrator resets the user's number of failed login attempts through the administrative GUI. Administrator lockouts are not applicable to the local console.
FIA_PMG_EXT.1	The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, and “”).
FIA_UID.1 FIA_UAU.2	The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed.

TOE SFRs	How the SFR is Met
	Administrative access to the TOE is facilitated through the TOE's Web GUI. The TOE mediates all administrative actions through the Web GUI. Once a potential administrative user attempts to access the GUI of the TOE through an HTTPS session, the TOE shows a login banner then prompts the user for a user name and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated. The TOE provides a local password based authentication mechanism. The administrator authentication policies include authentication to the local user database. The process for authentication is the same for administrative access whether administration is occurring via a directly connected console, remotely via SSHv2 secured connection or via HTTPS. At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grant administrative access (if the combination of username and password is correct) or indicate that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.
FIA_UAU.7	When a user enters their password at the local console, the TOE displays no characters so that the user password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered.
FMT_MOF.1(1) FMT_MOF.1(2)	The TOE provides the ability for Security Administrators to access TOE data, such as audit data, configuration data, security attributes, routing tables, and session thresholds and to perform manual updates to the TOE. Each of the predefined and administratively configured roles has create (set), query, modify, or delete access to the TOE data. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged roles. For the purposes of this evaluation, the privileged role, netadmin, is full administrative access, which is the default access for SD-WAN GUI and CLI. See FMT_SMF.1 for services the Security Administrator is able to start and stop. Management functionality of the TOE is provided through the TOE CLI. The term "Security Administrator" is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions. Therefore, semi-privileged administrators with only a subset of privileges can also modify TOE data based on if granted the privilege. No administrative functionality is available prior to administrative login.
FMT_SMF.1	The TOE provides all the capabilities necessary to securely manage the TOE and the services provided by the TOE. The management functionality of the

TOE SFRs	How the SFR is Met
	TOE is provided through the TOE GUI. The specific management capabilities available from the TOE include : • Local and remote administration of the TOE and the services provided by the TOE via the TOE GUI and CLI; • The ability to manage the warning banner message and content – allows the Authorized Administrator the ability to define warning banner that is displayed prior to establishing a session (note this applies to the interactive (human) users; e.g. administrative users; • The ability to manage the time limits of session inactivity which allows the Authorized Administrator the ability to set and modify the inactivity time threshold; • The ability to update the SD-WAN and IOS XE software. • The ability to configure the authentication failure parameters for FIA_AFL.1; • The ability to set the time which is used for time-stamps; • The ability to manually unlock a locked administrator account; The ability of the Security Administrator to: • The ability to configure firewall rules; Information about TSF-initiated Termination is covered in the TSS under FTA_SSL.1 or FTA_SSL.3. The TOE does not provide any interface for an Administrator to read or export cryptographic keys.
FMT_SMR.2	The TOE platform maintains privileged and semi-privileged administrator roles. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged roles. For the purposes of this evaluation, the privileged role is equivalent to full administrative access to the GUI and CLI, which is the default access for SD-WAN (netadmin). Once a cEdge device is controlled by vManage, there are no administrative management functions available. The term “Security Administrator” is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions. The privilege level determines the functions the user can perform; hence the Security Administrator with the appropriate privileges. Refer to the Guidance documentation and IOS-XE Command Reference Guide for available commands and associated roles and privilege levels. The TOE can and shall be configured to authenticate all access to the command line interface using a username and password.

TOE SFRs	How the SFR is Met
	The TOE supports both local administration via a web session and remote administration via SSH. The cEdge administrator is an account created on vManage to monitor other components via CLI such as vBond, vSmart and all cEdge devices. The account allows reading all audit logs and configuration files.
FMT_MSA.1 FMT_MSA.3	The TOE restricts the ability to configure firewall rules to authorized administrators only. The TOE allows an authorized administrator to create, view, modify and delete any firewall rules and apply such rules to designated cEdge router's interfaces.
FPT_APW_EXT.1	Password encryption is configured by default and cannot be undone. There are no administrative interfaces available that allow passwords to be viewed as they are encrypted.
FPT_STM.1	The TOE provides a source of date and time information used in audit event timestamps. The clock function is reliant on the system clock provided by the underlying hardware. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. The time information is also used in various routing protocols such as, OSPF, BGP, and ERF; Set system time, determining I&A timeout, and administrative session timeout.
FPT_ITT.1	All communications between SD-WAN controllers and cEdge routers are secured over DTLS (DTLS v1.2). The DTLS ciphersuites supported by SD-WAN are the following: ◦ <i>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)</i> ◦ <i>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)</i> ◦ <i>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)</i> All DTLS tunnels are supported by FOM 7.2a (CAVP# A1420).
FPT_TST.1	cEdge routers only: The TOE runs a suite of self-tests during initial start-up to verify its correct operation. For testing of the TSF, the TOE automatically runs checks and tests at startup, during resets and periodically during normal operation to ensure the TOE is operating correctly, including checks of image integrity and all cryptographic functionality. These tests include: • AES Known Answer Test – For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. • RNG/DRBG Known Answer Test – For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly.

TOE SFRs	How the SFR is Met
	• HMAC Known Answer Test – For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly. • Software Integrity Test – The Software Integrity Test is run automatically whenever the IOS system images is loaded and confirms that the image file that's about to be loaded has maintained its integrity. If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen and saved in the crashinfo file. All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in PASS state and ports are allowed to forward data traffic. These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected because any deviation in the TSF behavior will be identified by the failure of a self-test. The cEdge routers running configurations are verified by vManage automatically. vManage provide the ability to Security Administrators to verify the cEdge routers statuses in and to determine which device is "In Sync" or "Out of Sync".
FTA_SSL.1(1) FTA_SSL.1(2) FTA_SSL.3	An administrator can configure maximum inactivity times individually for both CLI and GUI administrative sessions through the use of the "idle-timeout" command for the CLI and through the "Client Session Timeout" for the GUI. When a session is inactive (i.e., no session input from the administrator) for the configured period of time the TOE will terminate the session, and no further activity is allowed requiring the administrator to log in (be successfully identified and authenticated) again to establish a new session. If a remote user session is inactive for a configured period of time, the session will be terminated and will require authentication to establish a new session. The allowable inactivity timeout range for SD-WAN Controllers is from 600 to 1800 seconds for the CLI and from 30 to 604,800 seconds (168 Hours) for the GUI. The allowable inactivity timeout for cEdge routers is from 60 to 1800 seconds.
FTA_SSL.4	An administrator is able to exit out of both local and remote administrative sessions. Each administrator logged onto the TOE can manually terminate their session using the "exit" command in the CLI or using the Sign Out button in the GUI.

TOE SFRs	How the SFR is Met
FTA_TAB.1	The TOE displays a privileged Administrator specified banner on the GUI management interface prior to allowing any administrative access to the TOE. This interface is applicable for both GUI and SSH TOE administration.
FTP_TRP.1	All remote administrative communications take place over a secure encrypted SSHv2 session or an HTTPS web session (TLS v1.2 or TLS v1.3). The remote users are able to initiate SSHv2 communications or the web session with the TOE. The SD-WAN controllers support the following SSH algorithms: Key Exchange algorithms: ◦ <i>ecdh-sha2-nistp256</i> ◦ <i>ecdh-sha2-nistp384</i> ◦ <i>ecdh-sha2-nistp521</i> ◦ <i>diffie-hellman-group-exchange-sha256</i> ◦ <i>diffie-hellman-group14-sha256</i> ◦ <i>diffie-hellman-group16-sha512</i> ◦ <i>diffie-hellman-group18-sha512</i> ◦ <i>diffie-hellman-group14-sha1</i> ◦ <i>diffie-hellman-group-exchange-sha1</i> Host Key Algorithms: ◦ <i>rsa-sha2-512</i> ◦ <i>rsa-sha2-256</i> ◦ <i>ssh-rsa</i> ◦ <i>ecdsa-sha2-nistp256</i> ◦ <i>ssh-ed25519</i> Encryption algorithms: ◦ <i>aes256-ctr</i> ◦ <i>aes256-gcm@openssh.com</i> ◦ <i>aes128-ctr</i> ◦ <i>aes128-gcm@openssh.com</i> ◦ <i>aes192-ctr</i> Mac algorithms: ◦ <i>hmac-sha2-256-etm@openssh.com</i> ◦ <i>hmac-sha2-512-etm@openssh.com</i> ◦ <i>hmac-sha2-256</i> ◦ <i>hmac-sha2-512</i> vManage supports the following TLS v1.2 ciphersuites: ◦ <i>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)</i> ◦ <i>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)</i> vManage supports the following TLS v1.3 ciphersuites: ◦ <i>TLS_AES_128_GCM_SHA256 (secp256r1)</i> ◦ <i>TLS_AES_256_GCM_SHA384 (secp256r1)</i>

TOE SFRs	How the SFR is Met
	The cEdge routers support the following SSH algorithms: Key Exchange algorithms: ◦ <i>curve25519-sha256</i> ◦ <i>curve25519-sha256@libssh.org</i> ◦ <i>ecdh-sha2-nistp256</i> ◦ <i>ecdh-sha2-nistp384</i> ◦ <i>ecdh-sha2-nistp521</i> ◦ <i>diffie-hellman-group14-sha256</i> ◦ <i>diffie-hellman-group16-sha512</i> Host Key algorithms: ◦ <i>rsa-sha2-512</i> ◦ <i>rsa-sha2-256</i> ◦ <i>ssh-rsa</i> Encryption algorithms: ◦ <i>aes128-gcm@openssh.com</i> ◦ <i>aes256-gcm@openssh.com</i> ◦ <i>aes128-gcm</i> ◦ <i>aes256-gcm</i> ◦ <i>aes128-ctr</i> ◦ <i>aes192-ctr</i> ◦ <i>aes256-ctr</i> Mac algorithms: ◦ <i>hmac-sha2-256-etm@openssh.com</i> ◦ <i>hmac-sha2-512-etm@openssh.com</i>

8 Rationale

This section describes the rationale for the Security Objectives and Security Functional Requirements as defined within this Security Target. Additionally, this section describes the rationale for not satisfying all of the dependencies. The table below illustrates the mapping from Security Objectives to Threats and Policies

8.1 Rationale for TOE Security Objectives

Table 19 Summary of Mappings between Threats, Policies and the Security Objectives

	T.ACCOUNTABILITY	T.NOAUTH	T.VPN	T.ASPOOF	T.MEDIATE	T.NETWORK
O.ACCESS_CONTROL		X				
O.ADMIN		X				
O.AUDIT_GEN	X					
O.AUDIT_VIEW	X					
O.DATA		X				
O.IDAUTH		X				
O.SELFPRO		X				
O.TIME	X					
O.VPN			X			
O.TOE_ADMINISTRATION		X				
O.MEDIATE				X	X	
O.PROTECTED_COMMS						X

Table 20 Rationale for Mappings between Threats, Policies and the Security Objectives

Objective	Rationale for Coverage
-----------	------------------------

T.ACCOUNTABILITY	An authorized administrator is not held accountable for their actions on the TOE because the audit records are not generated, do not include the required data, including properly sequenced through application of correct timestamps or reviewed. The O.AUDIT_GEN objective mitigates the threat by requiring the TOE generate audit records for events performed on the TOE. The O.AUDIT_VIEW requires the TOE to provide the authorized administrator with the capability to view audit data. The O.TIME objective mitigates this threat by providing the accurate time to the TOE for use in the audit records O.AUDIT_GEN.
T.NOAUTH	O.SELFPRO objective ensures that an unauthorized person (attacker) that may attempt to bypass the security of the TOE to access data and use security functions and/or non-security functions provided by the TOE to disrupt operations of the TOE is not successful. The O.DATA objective protects the configuration and user data from unauthorized disclosure. The O.IDAUTH objective requires the administrative user to enter a unique identifier and authentication credentials before management access is granted. The O.ADMIN objective ensures the authorized administrator has access to the TOE to configure access controls and the O.ACCESS_CONTROL objective restricts access to the TOE management functions to the Authorized Administrator. O.TOE_ADMINISTRATION provides an administrator the capabilities to configure firewall rules on TOE components where user data flows through and to configure
T.VPN	O.VPN objective ensures no user data flows between TOE appliances in plaintext by encrypting all channels using IPsec.
T.ASPOOF	O.MEDIATE objective ensures all traffic flowing through the TOE has been allowed by an administrator via firewall rules based on attributes such as IP address, port, protocol or zone id.
T.MEDIAT	O.MEDIATE objective ensures all traffic flowing through the TOE has been allowed by an administrator via firewall rules.
T.NETWORK_COMPROMISE	O.PROTECTED_COMMS ensures all communications between TOE components are protected.

8.2 Rationale for the Security Objectives for the Environment

The security requirements are derived according to the general model presented in Part 1 of the Common Criteria. Specifically, the tables below illustrate the mapping between the security requirements and the security objectives and the relationship between the threats, policies and IT security objectives. The functional and assurance requirements presented in this Security Target are mutually supportive and their combination meets the stated security objectives.

Table 21 Mapping Assumptions and the Security Objectives for the OE

	OE.ADMIN	OE.CONNECTION	OE.LOCATE	OE.PHYSEC
A.ADMIN	X			
A.CONNECTIONS		X		
A.LOCATE			X	
A.PHYSEC				X

Table 22 Rationale for Mapping Assumptions and the Security Objectives for the OE

Assumptions	Rationale for Coverage of Environmental Objectives
A.ADMIN	All Authorized Administrator are assumed not evil, will follow the administrative guidance and will not disrupt the operation of the TOE intentionally. The OE.ADMIN objective ensures that Authorized Administrator are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance; however, they are capable of error.
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. The OE.CONNECTION objective ensures all traffic going through the TOE is subject to Flow Control SFPs.
A.LOCATE	The processing resources of the TOE and those services provided by the operational environment will be located within controlled access facilities, which will prevent unauthorized physical access. The OE.LOCATE objective ensures the processing resources of the TOE and those services provided by the operational environment will be located within controlled

Assumptions	Rationale for Coverage of Environmental Objectives
	access facilities, which will prevent unauthorized physical access.
A.PHYSEC	The OE.PHYSEC objective ensures that the TOE is physically protected from unauthorized access.

8.3 Rationale for requirements/TOE Objectives

The security requirements are derived according to the general model presented in Part 1 of the Common Criteria. Specifically, the tables below illustrate the mapping between the security requirements and the security objectives and the relationship between the threats, and IT security objectives.

Table 23 Security Objective to Security Requirements Mappings

	O.ACCESS_CONTROLL	O.ADMIN	O.AUDIT_GEN	O.AUDIT_VIEW	O.DATA	O.IDAUTH	O.SELFPRO	O.TIME	O.VPN	O.TOE_ADMINISTRATION	O.MEDIATE	O.PROTECTED_COMMS
FAU_GEN.1	X		X					X				
FAU_GEN.2	X		X					X				
FAU_STG.1				X								
FAU_STG.4	X											
FCS_CKM.1									X			
FCS_CKM.2									X			
FCS_CKM.4									X			
FCS_COP.1									X			

Security Target

	O.ACCESS_CONTROLL	O.ADMIN	O.AUDIT_GEN	O.AUDIT_VIEW	O.DATA	O.IDAUTH	O.SELFPRO	O.TIME	O.VPN	O.TOE_ADMINISTRATION	O.MEDIATE	O.PROTECTED_COMMS
FCS_RBG_EXT.1									X			
FDP_ITT.1					X		X		X	X		
FDP_IFC.1					X		X			X	X	
FDP_IFF.1		X								X	X	
FFW_RUL_EXT.1										X	X	
FIA_AFL.1					X	X	X					
FIA_PMG_EXT.1						X						
FIA_UID.1					X	X	X					
FIA_UAU.2	X	X					X					
FIA_UAU.7	X	X										
FMT_MOF.1(1)	X	X			X							
FMT_MOF.1(2)	X	X										
FMT_MSA.1			X					X				
FMT_MSA.3			X					X				
FMT_MTD.1	X					X	X					
FMT_SMF.1		X					X					
FMT_SMR.2	X					X	X					
FPT_APW_EXT.1		X			X							

	O.ACCESS_CONTROLL	O.ADMIN	O.AUDIT_GEN	O.AUDIT_VIEW	O.DATA	O.IDAUTH	O.SELFPRO	O.TIME	O.VPN	O.TOE_ADMINISTRATION	O.MEDIATE	O.PROTECTED_COMMS
FPT_STM.1	X	X				X		X				
FPT_ITT.1												X
FPT_TST.1							X					
FTA_SSL.1	X					X	X	X				
FTA_SSL.3	X						X	X				
FTA_SSL.4	X	X										
FTA_TAB.1		X										
FTP_TRP.1	X	X				X	X					

Table 24 Summary of Mappings between IT Security Objective to SFRs

SFR	Rational
FAU_GEN.1	This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDIT, O.AUDIT_GEN, O.TIME.
FAU_GEN.2	This component ensures that the TSF traces audit records to the user that causes them. This component traces back to and aids in meeting the following objective: O.AUDIT_GEN, O.ACCESS_CONTROL, O.TIME.

SFR	Rational
FAU_STG.1	This component is chosen to ensure that the audit trail is protected from tampering, the security functionality is limited to the authorized administrator and that start-up and recovery does not compromise the audit records. This component traces back to and aids in meeting the following objectives: O.AUDIT_VIEW.
FAU_STG.4	This component ensures that the authorized administrator will be able to take care of the audit trail if it should become full. But this component also ensures that no other auditable events as defined in FAU_GEN.1 occur. Thus the authorized administrator is permitted to perform potentially auditable actions though these events will not be recorded until the audit trail is restored to a non-full status. This component traces back to and aids in meeting the following objectives: O.SELPRO,
FCS_CKM.1	This component ensures the cryptographic keys are generated with the AES scheme using cryptographic key sizes of 256 bit that meet the following: ISO/IEC 18031:2011. This component traces back to and aids in meeting the following objectives: O.VPN
FCS_CKM.2	This component provides secure key distribution through DTLS that meets the RFC 6347. This component traces back to and aids in meeting the following objectives: O.VPN
FCS_CKM.4	This component ensures the cryptographic keys generated in FCS_CKM.1 are either zeroized when no longer needed or overwritten by a new key value. This component traces back to and aids in meeting the following objectives: FDP_ITT.1
FCS_COP.1(1)	This component ensures the keys generated in FCS_CKM.1 are used for encryption and decryption of the VPN SFP defined in FDP_ITT.1. This component traces back to and aids in meeting the following objectives: O.VPN

SFR	Rational
FCS_COP.1(2)	This component ensures the tunnels in FDP_ITT.1 use a hash algorithm to provide authentication protection of the VPN SFP defined in FDP_ITT.1. This component traces back to and aids in meeting the following objectives: O.VPN
FCS_RBG_EXT.1	This component ensures the TOE components use a valid entropy source for all tunnels and defines the method of generating random numbers used in FDP_ITT.1. This component traces back to and aids in meeting the following objectives: O.VPN.
FDP_ITT.1	This component ensures that all sensitive user data flowing in the information flow control SFP between TOE components are protected. This component traces back to and aids in meeting the following objectives: O.DATA, O.SELFPRO.
FDP_IFC.1	This component identifies the entities involved in the FIREWALL information flow control SFP (i.e., users sending information to other users and vice versa). This component traces back to and aids in meeting the following objective: O.DATA, O.SELFPRO.
FDP_IFF.1	This component identifies the attributes of the users sending and receiving the information in the information flow control SFP, as well as the attributes for the information itself. Then the policy is defined by saying under what conditions information is permitted to flow. This component traces back to and aids in meeting the following objective: O.ACCESS, O.ADMIN, O.IDAUTH.
FFW_RUL_EXT.1	This components identifies the attributes that the firewall supports and the options that are available to administrators to configure. This component traces back to and aids in meeting the following objective: O.DATA, O_ACCESS_CONTROL.

SFR	Rational
FIA_AFL.1	This component ensures that human users who are not authorized administrators cannot endlessly attempt to authenticate. After some number of failures that the authorized administrator decides, that must not be zero, the user becomes unable from that point on in attempts to authenticate. This goes on until an authorized administrator makes authentication possible again for that user. This component traces back to and aids in meeting the following objective: O.SELFPRO.
FIA_PMG_EXT.1	This components identifies the attributes that are allowed to be used with passwords when cerating a new user or when updating a password for a specific user. This component traces back to and aids in meeting the following objective: O.SELFPRO.
FIA_UID.1	This component ensures that before anything occurs on behalf of a user, the user's identity is identified to the TOE. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.ACCESS_CONTROL.
FIA_UAU.2	This component ensures that before a user is authenticated, the TOE does not provide any administrative functions. This component traces back to and aids in meeting the following objectives: O.ACCESS_CONTROL.
FIA_UAU.7	This component ensures that the TSF will not echo passwords when being entered to mitigate the chance of an accidental password disclosure s. This traces back to and aids in meeting the following objective: O.DATA.
FMT_MOF.1(1)	This component ensures the TSF restricts the ability to modify the behavior of functions such as audit trail management, start up and shut down operation, and multiple authentication function to the authorized administrator. This component traces back to and aids in meeting the following objectives: O.IDAUTH, O.ACCESS_CONTROL.

SFR	Rational
FMT_MOF.1(2)	This component ensures the TSF restricts the ability to modify the behavior of functions such as audit trail management, start up and shut down operation, and multiple authentication function to the authorized administrator. This component traces back to and aids in meeting the following objectives: O.IDAUTH, O.ACCESS_CONTROL.
FMT_MSA.1	This component ensures the TSF enforces the Firewall SFP to restrict the ability to delete, modify, and add within a rule those security attributes that are listed in section FDP_IFF1.1(1). This component traces back to and aids in meeting the following objectives: O.IDAUTH, O.ACCESS_CONTROL.
FMT_MSA.3	This component the TSF allows an administrator to change the values of the Firewall SFP and either allow, deny or inspect packets coming to any router's interfaces. This component traces back to and aids in meeting the following objectives: O.IDAUTH, O.ACCESS_CONTROL.
FMT_MTD.1	This component ensures the TSF restricts the ability to manage the TSF data to Security administrators only. This component traces back to and aids in meeting the following objectives: O.ACCESS_CONTROL, O.IDAUTH.
FMT_SMF.1	This component ensures that the TSF restrict the set of management functions to the authorized administrator. It also ensures that the TSF will provide a minimum set of security functions to ensure the TOE security features can be properly managed. This component traces back to and aids in meeting the following objectives: O.ACCESS_CONTROL, O.IDAUTH.
FMT_SMR.2	This component ensures that the TSF allows an administrator to assign a role to a new user and the user will be allowed to access the TSF remotely and locally. This component traces back to and aids in meeting the following objectives: O.ACCESS_CONTROL, O.ADMIN.

SFR	Rational
FPT_APW_EXT.1	This component ensures that the TSF restricts the ability for any users, including Security administrators, from seeing any password in plaintext. This component traces back to and aids in meeting the following objectives: O.DATA, O.ADMIN.
FPT_STM.1	This component ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objectives: O.AUDIT_GEN, O.TIME.
FPT_ITT.1	This component ensures that all data flowing between SD-WAN controllers and cedge routers is protected. This component traces back to and aids in meeting the following objectives: O.PROTECTED_COMMS
FPT_TST.1	This component ensures the TOE integrity is maintained during reboot and the software hasn't been tampered with. This is important for maintaining the TOE' security. This component traces back to and aids in meeting the following objectives: O.SELFPRO
FTA_SSL.1	This component ensures that the TSF locks an inactive session and removes all abilities tht were previously available. This component traces back to and aids in meeting the following objectives: O.SELFPRO, O.TIME, O.IDAUTH.
FTA_SSL.3	This component ensures that the TSF will terminate local and remote sessions after an administrator defined period of inactivity indicating the user may not be in attendance. This component traces back to and aids in meeting the following objectives: O.ADMIN, O.ACCESS_CONTROL.
FTA_SSL.4	This component ensures that the TSF allows an authenticated administrator to terminate a session manually at any time. This component traces back to and aids in meeting the following objectives: O.ADMIN, O.ACCESS_CONTROL.

SFR	Rational
FTA_TAB.1	This component ensures that the TSF will display a configured advisory banner whenever a user/administrator connects to the TOE. This component traces back to and aids in meeting the following objective: O.ACCESS_CONTROL.
FTP_TRP.1	This component ensures that the TSF will protect communication between itself and its administrators from disclosure and modification. This component traces back to and aids in meeting the following objective: O.ADMIN, O.ACCESS_CONTROL.

9 CAVP Certificates

Table 25 CAVP Certificates

SFR	Selection	Algorithm	Implementation	Certificate Number
FCS_CKM.1 – Cryptographic Key Generation	AES	AES- GCM	IC2M Rel5a	A1462
			Octeon II CN6700/6800	AES2346
			Cisco ASIC	AES3871
			Intel QAT	AES 4639 / AES 4638
FCS_RBG_EXT.1	DRBG	Counter- DRB	IC2M Rel5a	A1462
FCS_COP.1(1) – Cryptographic operation	AES- GCM-256	AES	IC2M Rel5a	A1462
			Octeon II CN6700/6800	AES2346
			Cisco ASIC	AES3871
			Intel QAT	AES 4639 / AES 4638
FCS_COP.1(2) – Cryptographic Operation	HMAC	HMAC- SHA256	IC2M Rel5a	A1462

10 Key Zeroization

Table 26 Key zeroization

Name	Description of Key	Zeroization
IPSec encryption key	This is the key used to encrypt IPSec sessions. This key is stored in SDRAM.	Automatically when IPSec session terminated. Overwritten with: 0x00

11Annex A: References

The following documentation was used to prepare this ST:

Table 27 References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-004