Cisco Network Convergence System 540, 5500 and 5700 Series

Common Criteria Security Target

Version: 1.1

Date: March 29, 2023

Cisco Systems, Inc.

Table of Contents

Table of Tables

Table of Figures

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 Network Convergence System 540, 5500 and 5700 (NCS540, NCS5500, NCS5700) Series running IOS-XR, version 7.4. 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. Administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged, privileged administrators, and security administrators in this document.

1. Security Target Introduction

This Security Target contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- Security Requirements [Section 5]
- TOE Summary Specification [Section 6]
- Rationale [Section 7]
- References

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 3 Chapter 4.

1.1 ST and TOE Reference

This section provides information needed to identify and control this ST and its Target of Evaluation (TOE).

Table 1. ST and TOE Identification

Name	Description
ST Title	Cisco Network Convergence System 540, 5500 and 5700 Series Common Criteria Security Target
ST Version	1.1
Publication Date	March 29, 2023
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Network Convergence System (NCS)
TOE Hardware Models	**NCS540** • N540X-8Z16G-SYS-D, N540X-8Z16G-SYS-A , N540X-16Z4G8Q2C-A, N540X-16Z4G8Q2C-D **NCS5500** • NCS-5504-SYS **NCS5700** • NCS-57C3-MOD-SYS
TOE Software Version	Cisco IOS-XR 7.4.1
TOE Guidance	Cisco Network Convergence System 540, 5500 and 5700 Series Common Criteria Operational User Guidance and Preparative Procedures
Keywords	Router, Data Protection, Authentication

1.2 TOE Overview

The TOE is the Cisco Network Convergence System 540, 5500 and 5700 Series (herein after also referred to as Cisco NCS or TOE). The TOE is a purpose-built, routing platform that is designed for redundancy, segment routing, programmable network management and primarily used for Wide Area Network (WAN) aggregation. The TOE includes the hardware models as defined in Table 3 in section1.6.

This Security Target only addresses the functions that provide for the CC-evaluated security features of the TOE itself as described in Section 1.7 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. The hardware is comprised of the Cisco Network Convergence System 540, 5500 and 5700 (NCS540, NCS5500 and NCS5700) Series as described in 1.7 Physical Scope of the TOE. The software is comprised of the Cisco Internet Operating System (IOS) XR software image Release IOS-XR 7.4.

The Cisco NCS consists of:

- N540X-8Z16G-SYS-D is a 1RU small density fixed chassis router.
- N540X-8Z16G-SYS-A is a 1RU small density fixed chassis router.
- N540X-16Z4G8Q2C-D is a 1RU medium density fixed chassis router.
- N540X-16Z4G8Q2C-A is a 1RU medium density fixed chassis router.
- NCS-5504-SYS is a 7RU modular chassis in which TOE Line card NC55-32T16Q4H-A is housed.
- NCS-57C3-MOD-SYS is a 3RU fixed chassis router.

1.3.1 Required non-TOE Hardware/Software/Firmware

The TOE supports the following hardware, software, and firmware components in its operational environment. Each component is identified as being required or not based on the claims made in this Security Target. All of the following environment components are supported by all TOE evaluated configurations.

Table 2. IT Environment Component

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.
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
NTP Server	No	An NTP server is an optional component of the operational environment that would allow for synchronizing the TOE clocks with an external time source.
Audit (syslog) Server	No	A syslog server is an optional component for use with the TOE. It is a supplemental storage system for audit logs, but it does not provide audit log storage for the TOE.

1.4 TOE Description

This section provides an overview of the TOE. This section also defines the TOE components included in the evaluated configuration of the TOE. The TOE is comprised of both software and hardware. The TOE are modular and fixed routers that are primarily used for WAN aggregation.

1.4.1 NCS540

The Cisco NCS 540 includes small and medium density routers.

The Cisco NCS 540 Small Density Routers (N540X-8Z16G-SYS-D and N540X-8Z16G-SYS-A) are compact 1RU, temperature-hardened, conformal-coated platforms with advanced timing (Class C), security, and QoS features that revolutionize sub-100G routing by bringing the power of the IOS XR operating system to 3G/4G/5G cell sites (CSRs) and ease "IP"fication of Radio Access Network (RAN) and small-cell backhaul.

The Cisco Network Convergence System 540 Medium Density Routers (N540X-16Z4G8Q2C-D and N540X-16Z4G8Q2C-A) are designed for cost-effective delivery of next-generation services and applications. These routers are temperature-hardened, high-throughput, small form factor, low-power-consumption devices suitable for both outdoor and indoor deployments. With in-built trust anchor hardware infrastructure and anti-counterfeit protection along with software enabled security features, NCS 540 is most trusted and secured platform. They are powered by Cisco IOS XR software designed for operational efficiency and service agility. Cisco IOS XR software offers advanced features such as programmability, application awareness, network visibility, and automation. The Cisco NCS 540 series of routers is an intelligent converged access platform which enables service providers to deliver next-level business and entertainment experiences.

1.4.2 NCS5500

The Cisco NCS5500 is a high-capacity modular routing series that is designed for redundancy, segment routing, programmable network management and primarily used for WAN aggregation. The NCS5500 includes a Route Processor running IOS XR. The NCS5500 is designed to provide continuous system operation, scalability, security, and high performance.

1.4.3 NCS5700

The Cisco NCS5700 Series Routers are designed for cost-effective delivery of next-generation networking services. These are high-capacity and low-power-consuming devices available in a 3-rack-unit compact form factor. The chassis along with the Modular Port Adapters (MPAs) provide options of using different types of interfaces ranging from 1GE to 400GE. These devices also provide Control Plane redundancy, thereby enabling high availability and reliability.

The Cisco NCS5700 Series is powered by 64-bit version of IOS XR NOS designed on operational efficiency, optimized utilization, and service agility (evolved programmable network). Cisco IOS XR Software offers rich features such as iPXE boot, auto provisioning, native support for third-party application hosting, machine-to-machine interface, telemetry, and flexible software package delivery.

1.4.4 IOS-XR

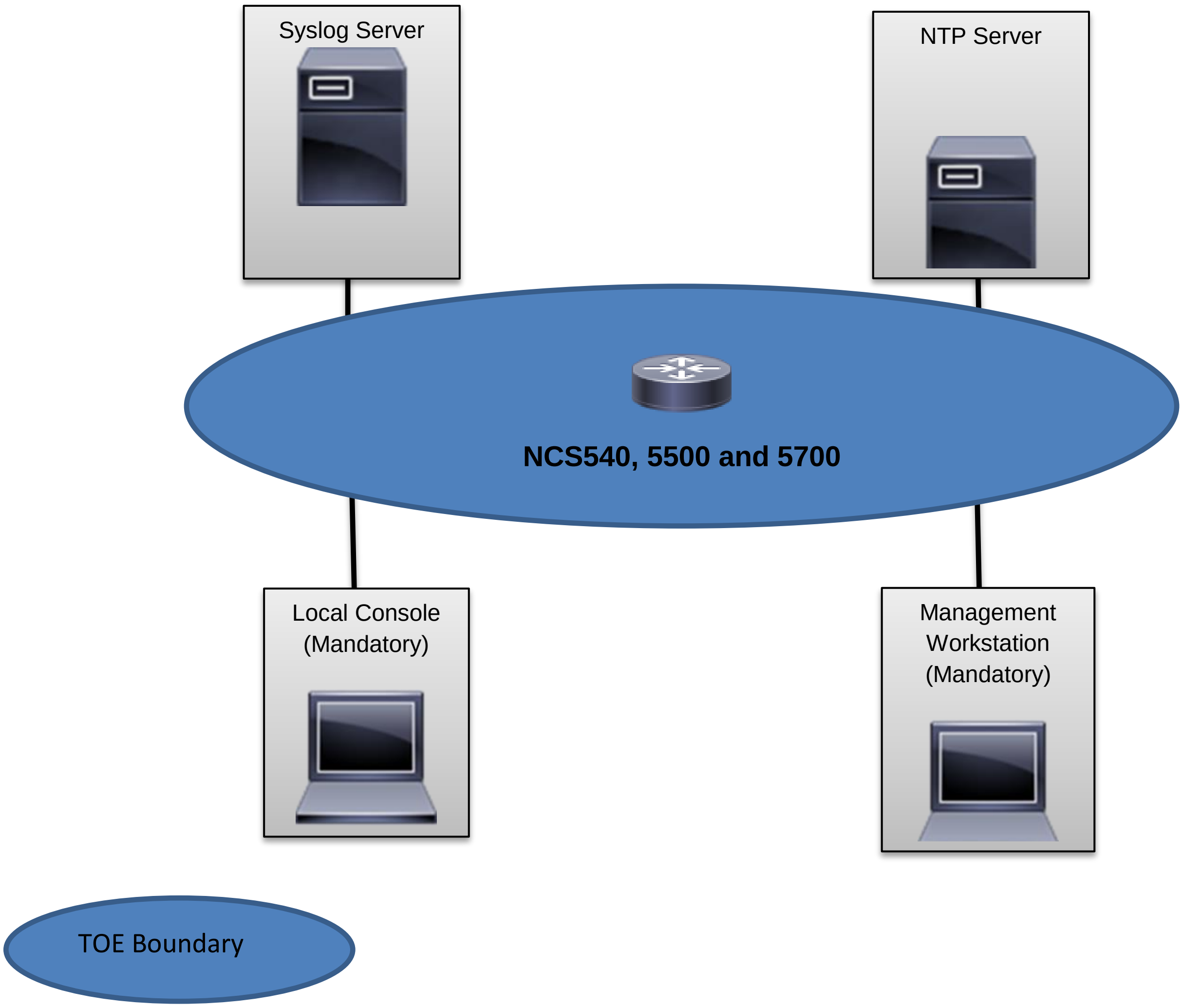
The NCS routers run Cisco IOS-XR that is a distributed microkernel-based network operating system. IOS-XR can process data as it comes into the router without buffering delays. The microkernel is responsible for specific functions such as memory management, interrupt handling, scheduling, task switching, synchronization, and interprocess communication. The microkernel's functions do not include other system services such as device drivers, file system, and network stacks; those services are implemented as independent processes outside the kernel, and they can be restarted like any other application.

The Cisco IOS-XR 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.

1.5 TOE Evaluated Configuration

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary includes all the hardware shown within Figure 1.

Figure 1 Example TOE Deployment



The previous figure includes the following:

- Examples of TOE Models
- The following are considered to be in the IT Environment:
  - Management Workstation
  - Audit (Syslog) Server
  - Local Console
  - NTP Server

In the evaluated configuration, an administrator must assign an ACL to all interfaces prior to enabling an interface.

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

1.6 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the Cisco NCS, and and the TOE guidance documentation.

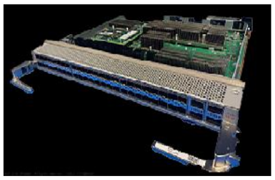
The software is the Cisco IOS-XR v7.4 (Xx). The network, on which they reside, is considered part of the environment. In addition, the software image is downloadable from the Cisco web site https://software.Cisco.com. A login ID and password is required to download the software image. For ordering of the TOE and delivery via commercial carriers, see https://apps.cisco.com/ccw/cpc/guest/home

The TOE guidance documentation that is considered to be part of the TOE is the Cisco Network Convergence System 540, 5500 and 5700 Series Common Criteria Operational User Guidance and Preparative Procedures v1.1 (March 23 2023), a PDF document that can be downloaded from the http://cisco.com web site.

The TOE is comprised of the following physical specifications as described in Table 3 – Hardware Models and Descriptions below.

Table 3. Hardware Models and Description

Model	Description	Processor	Interfaces
NCS540			
N540X-8Z16G-SYS-D N540X-8Z16G-SYS-A 	4-core 2GHz CPU 8 GB DRAM 16 GB eMMC 1 + 1 Fixed redundant DC 1 + 1 Fixed redundant AC Usable Rack Space: 1 RU	Marvell Cortex-A72 Armv8	8x 10/1GE 4x 1GE SFP 4x 1GE RJ45 8x 1GE SFP or 16x 1GE cSFP
N540X-16Z4G8Q2C-D N540X-16Z4G8Q2C-A 	8-core 1.7GHz x86 CPU 8GB DRAM 32GB storage Fixed dual redundant DC Modular Fan Tray with redundant fans Usable Rack Space: 1 RU	Intel Atom C3708 (Goldmont)	4x 1GE RJ-45 (10/100M) 16x 1GE/10GE 8x 1GE/10GE/25GE 2x 40GE/100GE
NCS5500			
NCS-5504-SYS 	Supports up to 4 line cards, 6 switch fabric cards, 2 route processors, 2 system controllers, 3 fan trays, 4 power supplies (AC or DC). Usable Rack Space: 7RU		Based on route processors and line-cards installed. For the evaluation: NC55-32T16Q4H-A

NC55-32T16Q4H-A 	2 x 10GE SFP+, 16 x 25GE SFP28 and 4x 100GE QSFP28 ports, 1 forwarding ASIC.	Intel Xeon D-1528 (Broadwell)	2 x 10GE SFP+ 16 x 25GE SFP28 4x 100GE QSFP28
NCS5700			
NCS-57C3-MOD-SYS	8 cores at 2 GHz 32GB DRAM 256GB Flash 2 hot-swappable power supplies provide 1 + 1 redundancy Front-to-back airflow6 hot-swappable fan trays provide 5 + 1 redundant system cooling Usable Rack Space: 3RU	Intel Xeon D-1563N (Broadwell)	1 USB RJ-45 Console Management Ethernet Fixed 48x 1/10/25G 8x 100G 3x MPA Base Chassis
Software	Cisco IOS-XR 7.4.1		
Guidance Documents	Cisco Network Convergence System 540, 5500 and 5700 Series Common Criteria Operational User Guidance and Preparative Procedures v1.1.pdf (*Including all supplemental guidance documents referenced therein.*)		

Software details are listed below per model

Table 4 - TOE Software

Models	Software Version	Image Name	Image hash values
N540X-8Z16G-SYS-D N540X-8Z16G-SYS-A	IOS XR 7.4.1	ncs540l-aarch64-7.4.1.iso	744d5adb7e7cca2be7aa9a615d84c613d8dd162a9c438f6d36963cd67439a6b361d17a4251fccef6c8be93c46fc43df1f65db06228fe85012e7baf732593945d
N540X-16Z4G8Q2C-D N540X-16Z4G8Q2C-A		ncs540l-x64-7.4.1.iso	dfa3b8685964cebd1558ad96cc810fb79512f35996794decb515a2ab0377caf034c50be264ae43a91a3e56b8ab4f8866774c987e539db732ffe2a19fba7f9026
NCS-5504-SYS		NCS5500-iosxr-7.4.1.tar	c98035eae1f3b85a650c2cff575f623bc2b55d458adb42c0b7806c759015da2d778cf995736c1fa790b05b2003a7515ee5e1b0d602c1ece1a808cb02459

Models	Software Version	Image Name	Image hash values
			0623e
NCS-57C3-MOD-SYS		NCS5500-iosxr-7.4.1.tar	c98035eae1f3b85a650c2cff575f623bc2b55d458adb42c0b7806c759015da2d778cf995736c1fa790b05b2003a7515ee5e1b0d602c1ece1a808cb024590623e

1.7 Logical Scope of the TOE

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

- Security Audit
- User data protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

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

1.7.1 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 CLI interfaces. 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.

1.7.2 User Data Protection

The TOE provides the ability to control traffic flow into or out of the Cisco NCS routers. The following types of traffic flow are controlled for both IPv4 and IPv6 traffic:

- Layer 3 Traffic – ACLs
- Layer 2 Traffic – Layer 2 Access Control Lists
- Virtual Routing and Forwarding - VRFs

An ACL is an administratively configured Information Flow Control list that is applied to Layer 3 traffic that is routed into or out of the Cisco NCS. A Layer 2 ACL is an administratively configured Information Flow Control list that is applied to Layer 2 traffic that is routed into Cisco NCS. The Virtual Routing and Forwarding (VRF), allow multiple instances of routing tables to exist within the TOE component simultaneously.

1.7.3 Identification and Authentication

The TOE performs user authentication for the Authorized Administrator of the TOE and device level authentication. The TOE provides authentication services for administrative users to connect to the TOE's secure administrator interfaces (CLI). The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length as well as mandatory password complexity rules.

For each Authorized Administrator account, they must have a unique username. For authentication purposes, a password is required for each Authorized Administrator account.

1.7.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All CLI TOE administration occurs either through SSHv2 secure connection or a direct local console connection. The TOE provides the ability to securely manage:

- Administer the TOE remotely
- Manage audit functionality
- Manage Information Flow Control Policies and Rules
- Manage Authorized Administrator’s security attributes
- Review audit record logs
- Configure and manage the system time
- Maintain the system.

1.7.5 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and limit configuration options to the Authorized Administrator. Additionally, Cisco IOS-XR is not a general-purpose operating system and access to Cisco IOS-XR memory space is restricted to only Cisco IOS-XR functions.

The TOE use of Information Flow Control Policies and Rules to ensure routing protocol communications between the TOE and neighbour switches is logically isolated from traffic.

The TOE internally maintains the date and time. This date and time are used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually, or optionally can configure the TOE to use NTP to synchronize the TOE's clock with an external time source.

1.7.6 TOE Access

The TOE enforces the termination of inactive sessions after an Authorized Administrator configurable time-period has expired. Once a session has been terminated, the TOE requires the Authorized Administrator to re-authenticate to establish a new session.

1.7.7 Trusted Path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 for remote CLI access.

1.8 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 5. Excluded Functionality and Rationale

Function Excluded	Rationale
Telnet	Telnet Sends authentication data in plain text. This feature is disabled by default and must remain disabled in the evaluated configuration.
SNMP	SNMP may allow an unauthorized third party to gain access to a network device. This feature will be disabled in the evaluated configuration.

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 Conformant
- 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 section describes the following security environment in which the TOE is intended to be used.

- Significant assumptions about the TOE’s operational environment.
- IT related threats to the organization countered by the TOE
- Environmental threats requiring controls to provide sufficient protection.
- 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.

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 6. TOE 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 facility housing the TOE must 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 system is allowed.

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 Basic.

Table 7. Threats

Threat	Threat Definition
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.
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.

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 identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 8. Security Objectives for the TOE

Environment Security Objective	IT Environment 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.

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 9. 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. 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.

5.1 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:

Table 10. Security Requirement Conventions

Convention	Indication
Assignment	Allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [**[*selected-assignment*]**])
Selection	Allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
Iteration	Allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number placed at the end of the component. (e.g., (1), (2), (3).)
Refinement	Allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
Extended Requirements	Are identified with "(EXT)" in of the functional class/name and are those not found in Part 2 of the CC.
Other	Sections of the ST use bolding to highlight text of special interest, such as captions.

5.2 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 11. 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_SAR.1	Audit Review
	FAU_STG.1	Protected Audit Event Storage

FDP: User data protection	FDP_IFC.1	Complete information flow control
	FDP_IFF.1	Subset information flow control
FIA: Identification and authentication	FIA_ATD.1	Password Management
	FIA_SOS.1	Authentication Failure Handling
	FIA_UAU.2	Password-based Authentication Mechanism
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
FMT: Security management	FMT_MSA.1	Secure Security Attributes (Access Control)
	FMT_MSA.3	Static Attribute Initialization (Access Control)
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
FPT: Protection of the TSF	FPT_STM.1	Reliable Time Stamps
FTA: TOE Access	FTA_SSL.3	TSF-initiated Termination
FTP: Trusted path/channels	FTP_TRP.1	Trusted Path

5.3 Security Functional Requirements

5.3.1 Class: Security Audit (FAU)

5.3.1.1 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:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [***not specified***] level of audit **specified in Table 11 Auditable Events**; and

c) [**no additional events**].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, [**information specified in the Additional Audit Record Contents column of Table 12 Auditable Events**].

Table 12. Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_SAR.1	None.	None.
FAU_STG.1	None.	None.
FDP_IFC.1	None	None.
FDP_IFF.1	None	None.
FIA_ATD.1	None	None.
FIA_SOS.1	None	None.
FIA_UAU.2	All use of the authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_UID.2	All use of the identification mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FMT_MSA.1	None	None.
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules and all modifications of the initial values of security attributes.	None
FMT_MTD.1	All modifications to the values of TSF data	The identity of the authorized administrator performing the operation.
FMT_SMF.1	Use of the management functions	The identity of the authorized administrator performing the operation.
FMT_SMR.1	None	None.
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation.
FTA_SSL.3	Termination of an interactive session by the session locking mechanism.	None
FTP_TRP.1	Attempts to use the trusted path functions.	Identification of the user associated with all trusted path invocations including failures, if available.

5.3.1.2 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.

5.3.1.3 FAU_SAR.1 –Audit Review

FAU_SAR.1.1 The TSF shall provide [**authorized administrator**] with the capability to read [**all TOE audit trail data**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.3.1.4 FAU_STG.1 – Protected Audit Event Storage

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

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

5.3.2 Class: User Data Protection (FDP)

5.3.2.1 FDP_IFC.1 Subset Information Flow control

FDP_IFC.1.1 The TSF shall enforce the [**information flow Control SFP**] on [

- **Subject: Physical and virtual network interfaces;**
- **Information: Network packets;**
- **Operations: Permit, drop, ignore**]

5.3.2.2 FDP_IFF.1 Security attribute based access control

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

- **Subjects: Physical and virtual network interfaces**
- **Subject Security Attribute:**
  - **Interface identifier**
  - **Tenant (VRF) identifier (if applicable)**
- **Information Security Attributes:**
  - **IP address source identifier**
  - **IP address destination identifier**
  - **Protocol (IPv4 and IPv6)**
  - **Interfaces configured as trusted (Layer 2 and Layer3)**

].

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: [**if the combination of subject, subject security attributes and information security attributes matches then the network packets are allowed to flow**]

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 the following rules**: [**

- **For IP Network Traffic Flows:**

  - *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;*
- **For Non-IP Network Traffic Flows:**
  - *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;*

5.3.3 Class: Identification and Authentication (FIA)

5.3.3.1 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**user identity and password].**

5.3.3.2 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**at least eight characters long; includes upper and lower alpha characters and alpha numeric characters].**

5.3.3.3 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.

5.3.3.4 FIA_UAU.7 – Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only [**no feedback or any locally visible representation of the user-entered password**] to the user while the authentication is in progress.

5.3.3.5 FIA_UID.2 – User Identification before any action

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

5.3.4 Class: Security Management (FMT)

5.3.4.1 FMT_MSA.1 – Management of security attributes

FIA_MSA.1.1 The TSF shall enforce the [**Information Flow Control SFP**] to restrict the ability to [***modify***, **[*none*]**] the security attributes [**listed in section FDP_IFF1.1**] to [**Authorized Administrator**].

5.3.4.2 FMT_MSA.3 –Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the [**Information Flow Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

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

5.3.4.3 FMT_MTD.1– Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [***modify***] the [**all TSF data**] to [**Authorized Administrator**].

5.3.4.4 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**
- **Manage the information control security attributes**
- **Manage Authorized Administrator's security attributes**
- **Review audit record logs**
- **Configure and manage the system time**].

5.3.4.5 FMT_SMR.1 –Security Roles

FMT_SMR.1.1 The TSF shall maintain the following roles [**Authorized Administrator**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.3.5 Class: Protection of the TSF (FPT)

5.3.5.1 FPT_STM.1 – Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps **for its own use**.

5.3.6 Class: TOE Access (FTA)

5.3.6.1 FTA_SSL.3 – TSF-initiated Termination

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

5.3.7 Class: Trusted Path (FTP)

5.3.7.1 FTP_TRP.1 – Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [***remote***] users 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***] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [***initial user authentication***, **[*management of the TOE via administrative interfaces*]**].

5.4 TOE SFR Dependencies Rationale

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.

Table 13. 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	Met by: FAU_GEN.1 FIA_UID.2
FAU_SAR.1	FAU_GEN.1	Met by: FAU_GEN.1
FAU_STG.1	FAU_GEN.1	Met by: FAU_GEN.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 FMT_MSA.3
FIA_ATD.1	No dependencies	N/A
FIA_SOS.1	No dependencies	N/A
FIA_UAU.2	FIA_UID.1	Met by: FIA_UID.2
FIA_UAU.7	FIA_UAU.1	Met by: FIA_UAU.2
FIA_UID.2	No dependencies	N/A
FMT_MSA.1	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Met by: FDP_IFC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Met by: FMT_SMR.1 FMT_MSA.1
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Met by: FMT_SMF.1 FMT_SMR.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1	Met by: FIA_UID.2

SFR	Dependency	Rationale
FPT_STM.1	No dependencies	N/A
FTA_SSL.3	No dependencies	N/A
FTP_TRP.1	No dependencies	N/A

5.5 Security Assurance Requirements

5.5.1 SAR Requirements

The TOE assurance requirements for this ST are EAL2 augmented with ALC_FLR.2 derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in the table below.

Table 14. SAR Requirements

Assurance Class	Components	Components Description
Development	ADV_ARC.1	Architectural Design with domain separation and non-bypassability
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life Cycle Support	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_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

5.5.2 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.

5.6 Assurance Measures

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

Table 15. Assurance Measures

Assurance Component	Rationale
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_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_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 ALC_CMS.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 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.

Assurance Component	Rationale
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_COV.1 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_IND.2	Cisco will provide the TOE for testing.
AVA_VAN.2	Cisco will provide the TOE for testing.

6. TOE Summary Specification

6.1 TOE Security Functional Requirement Measures

The table below identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 16. How TOE SFRs Measures

TOE SFRs	How the SFR is Met
FAU_GEN.1 FAU_GEN.2	Auditing is on by default at TOE startup and cannot be turned off. A record is generated when the TOE starts and when the TOE is shutdown, thus indicating the starting and stopping of auditing. Each auditable event, the recorded information includes the user that triggered the event, the outcome or result of the event and when the event occurred. The user that triggered the event could be a human user where the 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. Auditing of the contracts PACLS, RACL, and EPG to EPG traffic is enabled by default. However, a more verbose logging can be configured for contracts. This verbose logging results in packets that match deny rules in the contract will also be logged. A full list of the contents of the generated audit information can be found in Table 12.
FAU_SAR.1 FAU_STG.1	The Authorized Administrators can view the audit log records via the CLI interface. There are no other methods to view the audit records. 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. The audit records include sufficient information for the Authorized Administrator to determine the event, the user who initiated the event, the date and time of the event and the outcome of the event. The audit records are stored in an internal file and this internal file cannot be altered.
FDP_IFC.1 and FDP_IFF.1	The TOE enforces the Information Flow Control SFP on network traffic received on the TOE's network interfaces, both virtual and physical. Whenever an endpoint device attempts to send network traffic to the TOE protected network, the TOE verifies traffic complies with the administratively configured security policies before the endpoint device can send network traffic to TOE protected resources. The TOE interfaces including any Layer 3 interface, Physical Layer 3 interfaces, Layer 3 Ethernet sub-interfaces, Layer 3 Ethernet port-channel interfaces, Layer 3 Ethernet port channel sub-interfaces, Tunnels, Management interfaces, Layer 2 interfaces, or Layer 2 Ethernet port-channel interfaces. For endpoint devices that comply with the administratively configured policies, the TOE permits the network traffic to flow to the TOE protected resource in the network. For endpoint devices that do not comply with administratively configured security policies, the TOE either denies the traffic flow or redirects to an interface.

TOE SFRs	How the SFR is Met
FIA_ATD.1	The TOE supports definition of Authorized Administrator by individual user IDs. For each Authorized Administrator, the TOE maintains the following attributes: a) user identity b) password Authorized Administrator are administrators that are granted access to specific resources and permission to perform specific tasks.
FIA_SOS.1	To prevent users from choosing insecure passwords, the TOE prompts the user that the password should meet the following requirements: • At least eight characters long • includes upper and lower case characters • Includes alpha numeric characters This requirement applies to the local password database and on the password selection functions provided by the TOE.
FIA_UID.2 and FIA_UAU.2	By default, the TOE uses the local database for identification and authentication. No access is allowed prior encountering an authentication prompt and then being successfully identified and authenticated. Only after authentication, is the Authorized Administrator able to perform any actions.
FIA_UAU.7	When a user enters their password at the local console, CLI the TOE does not echo any feedback, nor any of the characters of the password or any representation of the characters.
FMT_MSA.1	The TOE provides the Authorized Administrator the ability to modify the security attribute values used for resource information flow control.
FMT_MSA.3	The TOE provides restrictive default values for resources information flow control via ACL. In the evaluated configuration, an administrator must apply an ACL to an interface before enabling it. Each access rule includes an implicit deny-all rule. Once a rule is applied to an interface, only the explicitly allowed traffic will flow through the TOE. Every other packet will be dropped. By default, all interfaces are disabled and block all traffic.
FMT_MTD.1	The TOE provides the ability for Authorized Administrator to access and modify as allowed, all TOE configuration, management and audit data.
FMT_SMF.1	The TOE provides all the capabilities necessary to securely manage the TOE. The Authorized Administrator can connect to the TOE using the CLI with SSHv2 secure connection to perform the following functions: Administer the TOE remotely Configure and manage information flow control attributes, rules and policies Manage Authorized Administrator's security attributes Review audit record logs Configure and manage the system time
FMT_SMR.1	The TOE maintains Authorized Administrator role to administer the TOE locally and remotely. During the installation of the TOE, the Authorized Administrator user is created. Additional Authorized Administrator users may be created; each must be assigned a unique username and password. All users of the TOE are considered Authorized Administrators. It is assumed all administrators are trusted, trained, knowledgeable, and will follow the guidance to ensure the TOE is properly monitored and operated in a secure manner. The Authorized Administrator can connect to the TOE using the CLI with SSHv2secure session.
FPT_STM.1	The TOE provides a source of date and time information used in audit event timestamps and in

TOE SFRs	How the SFR is Met
	validating service requests. This function can only be accessed from within the configuration exec mode via the privileged mode of operation of the router. The clock function is reliant on the system clock provided by the underlying hardware. This date and time are used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions.
FTA_SSL.3	An administrator can configure maximum inactivity times individually for both local and remote administrative sessions through the use of the “exec-timeout” setting applied to the console and vty for remote sessions. These settings are not immediately activated for the current session. The current line console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session. If a local user session is inactive for a configured period of time, the session will be terminated and will require re-authentication 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.
FTP_TRP.1	The TOE ensures the communication path and the remote administer interfaces is protected and distinct from other communications paths. The CLI uses SSHv2.

6.2 TOE Bypass and interference/logical tampering Protection Measures

The TOE consists of a hardware and software solution. All administration and configuration operations are performed within the physical boundary of the TOE. All security policy enforcement functions must be invoked and succeed prior to functions proceeding.

The TOE has been designed so that all locally maintained TSF data can only be manipulated via the secured management interface, a CLI interface. The CLI interface achieves a trusted path via SSH password authentication and is recommended for authorized administrator access from outside the network boundary protecting the TOE servers. There are no undocumented interfaces for managing the product.

All sub-components included in the TOE rely on the main chassis for power and memory while the TOE software provides the management functions and control. To access any portion of the TOE, the Identification and Authentication mechanisms of the TOE must be invoked and succeed.

No processes outside of the TOE are allowed direct access to any TOE memory. The TOE only accepts traffic through legitimate TOE interfaces. Specifically, processes outside the TOE are not able to execute code on the TOE. None of these interfaces provides any access to internal TOE resources.

Only the Authorized Administrator has access to the TOE security functions.

There are no unmediated traffic flows into or out of the TOE or unauthenticated access, thus providing a distinct protected domain for the TOE that is logically protected from interference and is not bypassable.

7. Rationale

This section describes the rationale for the Security Objectives and Security Functional Requirements as defined within this Security Target.

7.1 Rationale for TOE Security Objectives

Table 17. Threats & IT Security Objectives Mapping

	T.ACCOUNTABILITY	T.NOAUTH
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	

Table 18. TOE Threat/Policy/Objective Rationale

Threat / Policy	Rationale for Coverage
T.ACCOUNTABILITY	An authorized administrative 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

Threat / Policy	Rationale for Coverage
	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.

7.2 Rationale for TOE 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 19. Threats & IT Security Objectives Mappings for the Environment

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

Table 20. Assumptions/Threats/Objectives Rationale

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.

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

7.3 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 21. Security Objective to Security Requirements Mappings

	O.ACCESS_CONTROLL	O.ADMIN	O.AUDIT_GEN	O.AUDIT_VIEW	O.DATA	O.IDAUTH	O.SELPRO	O.TIME
FAU_GEN.1	X		X					X
FAU_GEN.2	X		X					X

	O.ACCESS_CONTROLL	O.ADMIN	O.AUDIT_GEN	O.AUDIT_VIEW	O.DATA	O.IDAUTH	O.SELPRO	O.TIME
FAU_SAR.1				X				
FAU_STG.1	X							
FDP_IFC.1					X		X	
FDP_IFF.1					X		X	
FIA_ATD.1	X	X				X		
FIA_SOS.1						X		
FIA_UAU.2					X	X	X	
FIA_UAU.7						X		
FIA_UID.2					X	X	X	
FMT_MSA.1	X	X					X	
FMT_MSA.3	X	X					X	
FMT_MTD.1	X	X						
FMT_SMF.1	X	X			X			
FMT_SMR.1	X	X						
FPT_STM.1			X					X
FTA_SSL.3	X					X	X	
FTP_TRP.1		X					X	

Table 22. Objectives to Requirements Rationale

Objective	Rationale
O.ACCESS_CONTROL	The TOE will restrict access to the TOE Management functions to the Authorized Administrator. The TOE is required to provide the ability to restrict the use of TOE management/administration/security functions to Authorized Administrator of the TOE. The Authorized Administrator performs these functions on the TOE. Only Authorized Administrator of the TOE may modify TSF data [FMT_MTD.1] and delete audit data stored locally on the TOE [FAU_STG.1]. The TOE must be able to recognize the administrative privilege level that exists for the TOE [FIA_ATD.1, FMT_SMR.1]. The TOE must allow the Authorized Administrator to specify alternate initial values when an object is created [FMT_MSA.1, FMT_MSA.3]. The TOE ensures that all user actions resulting in the access to TOE security functions and configuration data are controlled [FMT_SMF.1] and audited [FAU_GEN.1, FAU_GEN.2]. The SFR FTA_SSL.3 also meets this objective by terminating a session due to meeting/exceeding the inactivity time limit.
O.ADMIN	The TOE will provide administrative functions to isolate administrative actions by configuring and assigning Authorized Administrator accounts [FIA_ATD.1, FMT_SMR.1], thus controlling access to the TSF data and configuration [FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1]. The TOE will also make the administrative functions available remotely via SSHv2 [FTP_TRP.1].
O.AUDIT_GEN	The TOE will generate audit records which will include the time [FPT_STM.1] that the event occurred and if applicable, the identity of the user performing the event [FAU_GEN.2]. All TOE security relevant events are auditable and will include the required information to identify when the event occurred, the event, who performed the action, and the success or failure of the event [FAU_GEN.1 and FAU_GEN.2]. Timestamps associated with the audit record must be reliable [FPT_STM.1].
O.AUDIT_VIEW	The TOE will provide the Authorized Administrator the capability to review Audit data via the CLI interfaces. Security relevant events are available for review by Authorized Administrator [FAU_SAR.1].
O.DATA	The TOE is required to protect the TSF data from unauthorized access therefore each Authorized Administrator must be identified and authenticated prior to gaining access [FIA_UAU.2 and FIA_UID.2]. The TOE ensures that access to TOE configuration settings (CLI commands), data and resources is done in accordance with the management functions [FMT_SMF.1]. The TOE is also required to restrict traffic flows to and through the TOE based on the Information Flow Control SFP. Whenever an endpoint device attempts to send network traffic to the TOE protected network, the TOE verifies that the endpoint devices complies with the administratively configured security policies before the endpoint device can send network traffic to TOE protected resources. For endpoint devices that comply with the administratively configured policies, the

Objective	Rationale
	TOE permits the network traffic to flow to the TOE protected resource in the network. For endpoint devices that do not comply with administratively configured security policies the traffic is not permitted. This is met by [FDP_IFC.1, FDP_IFF.1].
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all administrative users before granting management access. The Authorized Administrators' password must meet formatting requirements to prevent the use of weak credentials [FIA_SOS.1]. The TOE is required to store user security attributes to enforce the authentication policy of the TOE and to associate security attributes with users [FIA_ATD.1]. Users authorized to access the TOE must be defined using an identification and authentication process and all users must be successfully identified and authenticated [FIA_UID.2 and FIA_UAU.2]. The password is obscured when entered [FIA_UAU.7]. If the period of inactivity has been exceeded, the user is required to re-authenticate to re-establish the session [FTA_SSL.3].
O.SELFPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions. [FDP_IFC.1, FDP_IFF.1, FIA_UID.2 and FIA_UAU.2] supports this objective by ensuring access to the resources is controlled and only Authorized Administrator can manage the resources [FMT_MSA.1 and FMT_MSA.3]. The [FTP_TRP.1] ensures the communication path and the remote administer interfaces is protected and distinct from other communications paths. The SFR [FTA_SSL.3] also meet this objective by terminating a session due to meeting/exceeding the inactivity time limit thus ensuring the session does not remain active and subject to attack.
O.TIME	The TSF will provide a reliable time stamp for its own use. The TOE is required to provide reliable timestamps for use with the audit record [FAU_GEN.1, FAU_GEN.2 and FPT_STM.1,].

8. Annex A: References

The documentation listed below was used to prepare this ST

Table 23. 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

9. Annex B: Acronyms

The following acronyms and terms are common and may be used in this Security Target.

Table 24. Acronyms

Acronym/Term	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standards
API	Application Programming Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
EAL	Evaluation Assurance Level
FC	Fibre Channel
HDD	Hard-disk drives
IP	Internet Protocol
PACLs	Port Access Control List
OS	Operating System
RACLs	Receive Access Control List
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SM	Service Module
SSD	Solid-state disk
SSH	Secure Shell
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security

TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
VLAN	Virtual Local Area Network
VRF	Virtual Routing and Forwarding
VSAN	Virtual Storage Area Network
XML	Extensible Markup Language
WAN	Wide Area Network

10. Annex C – Terminology

The following terms are common and may be used in this Security Target.

Table 25. Terms

Term	Definition
Layer 2 (L2)	Layer 2, also known as the Data Link Layer, is the second level in the seven-layer OSI reference model for network protocol design. Layer 2 is equivalent to the link layer (the lowest layer) in the TCP/IP network model. Layer2 is the network layer used to transfer data between adjacent network nodes in a wide area network or between nodes on the same local area network.
Layer 3 (L3)	Layer 3 refers to the third layer of the Open Systems Interconnection (OSI) Model, which is the network layer. Layer 3 is responsible for all packet forwarding between intermediate routers, as opposed to Layer 2 (the data link layer), which is responsible for media access control and flow control, as well as error checking of Layer 1 processes. Traditional switching operates at layer 2 of the OSI model, where packets are sent to a specific switch port based on destination MAC addresses. Routing operates at layer 3, where packets are sent to a specific next-hop IP address, based on destination IP address. Devices in the same layer 2 segment do not need routing to reach local peers. What is needed however is the destination MAC address which can be resolved through the Address Resolution Protocol (ARP)
Users	The users of the TOE are the processes and applications on the TOE that access the storage which is provided by the TOE.
Virtual Local Area Network (VLAN)	The VLANs enable efficient traffic separation, provide better bandwidth utilization, and alleviate scaling issues by logically segmenting the physical local-area network (LAN) infrastructure into different subnets so that VLAN packets are presented to interfaces within the same VLAN. The most important requirement of VLANs is the ability to identify the origination point for packets with a VLAN tag to ensure packets can only travel to interfaces for which they are authorized, thus creating Layer 2 (data link) implementations of subnets.

11. Annex D: Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What’s New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What’s New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

12. Contacting Cisco

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.