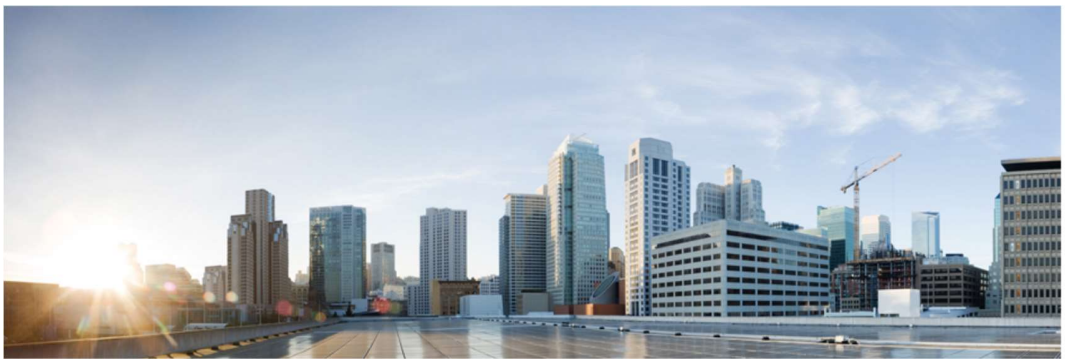

Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders

Common Criteria Security Target

Version 1.0

14 January 2021

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

Table of Contents

List of Tables

List of Figures

Acronyms and Abbreviations

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

Table 1 Acronyms and Abbreviations

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
APIC	Application Policy Infrastructure Controller
BRI	Basic Rate Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
CSU	Channel Service Unit
DSU	Data Service Unit
EAL	Evaluation Assurance Level
EHWIC	Ethernet High-Speed WIC
GE	Gigabit Ethernet port
GUI	Graphical User Interface
HTTPS	Hyper-Text Transport Protocol Secure
IP	Internet Protocol
ISDN	Integrated Services Digital Network
IT	Information Technology
LLDP	Link Layer Discovery Protocol
NTP	Network Time Protocol
OS	Operating System
PoE	Power over Ethernet
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SSHv2	Secure Shell protocol version 2
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
ToR	Top of Rack
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
vPC	virtual Port Channels
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network
WIC	WAN Interface Card

Terminology

The following terms are common for this technology and may be used in this Security Target:

Table 2 Terms

Term	Definition
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF related functions.
Line Cards	The line cards of the Cisco Nexus 9500 Series are equipped with multiple network forwarding engines (NFE) that perform packet lookup, processing and forwarding functions.
Non-IP Traffic	Examples of non-IP traffic include Bridge Protocol Data Unit (BPDU) traffic that contains information regarding ports, switches, port priority and addresses. Another type of non-IP traffic includes QinQ traffic that allows for multiple VLAN tags to be inserted in a single frame; keeping the traffic separate at layer 2
Peer switch	Another switch on the network that the TOE interfaces with.
Privilege level	The Authorized Administrator assigns administrative users to specific privilege levels to manage various aspects of the TOE. The privilege levels are from 1-15 with 15 having full administrator access to the TOE whereas privilege level 1 has the most limited access to the TOE. At this level, the Administrator has access to some information about the TOE, such as the status of interfaces and they can view routes in the routing table. However, the Administrator cannot make any changes or view the running configuration file.
Role	A role gives an Authorized Administrator varying access to the management of the TOE. For the purposes of this evaluation the privilege level of an Administrator is synonymous with the assigned role.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
System Controller	The System Controllers of Cisco Nexus 9500 Series are used to offload the internal non-data-path switching and management functions from the supervisor engines. It also provides the pathway for access to the power supplies and fan trays.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
vty	vty is a term used by Cisco to describe a single terminal (whereas Terminal is more of a verb or general action term).

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), the Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders (9K) and NX-OS software. 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

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]
- IT Security Requirements [Section 5]
- TOE Summary Specification [Section 6]
- Rationale [Section 7]

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 TOE.

Table 3 ST and TOE Identification

Name	Description
ST Title	Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders Common Criteria Security Target
ST Version	1.0
Publication Date	14 January 2021
ST Author	Cisco Systems, Inc.
Developer of the TOE	Cisco Systems, Inc.
TOE Reference	Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders
TOE Hardware Models	Nexus 2000, Nexus 9300, Nexus 9500 and APIC-SERVER- L3/M3
TOE Software Version	Cisco NX-OS System Software-ACI 14.2(4o), APIC 4.2(4o)
TOE Guidance	Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders Common Criteria Operational User Guidance and Preparative Procedures, Version 1.0
Keywords	Switch, Data Protection, Authentication

1.2 TOE Overview

The Cisco Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders (Application-Centric Infrastructure) offer both modular (9500 switches) and fixed (9300 switches) 1, 10, 40, and 100 Gigabit Ethernet (GE) configurations designed to operate in one of two modes:

- Cisco NX-OS mode for traditional architectures and consistency across the Cisco Nexus portfolio;

- ACI mode to take full advantage of the policy-focused services and infrastructure automation features of the ACI.

In addition to the Nexus 9000 Series Switch and APIC, the solution provided by the TOE includes the Cisco Nexus 2000 Series Fabric Extender, and the APIC and NX-OS software. The TOE is intended to be deployed within a physically secure data center. All the TOE components that make up the ACI fabric are installed within the same datacenter. The TOE can be deployed with the Nexus 9K and APIC or Nexus 9K, APIC, and Fabric Extender. The use of the Fabric Extender is optional. The Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders are data center switches that support up to 60 terabits per second (Tbps) of nonblocking performance switching, making them highly capable and effective in the role of data center aggregation layer switches. The TOE is comprised of the Nexus 9000 Series Switches that include the 9300, 9500 models with ACI mode and the APIC including the optional Nexus 2000 Fabric Extenders. The APIC is the security management controller used to manage the ACI fabric. The Nexus 2000 Fabric Extender functions essentially as a remote line card and is optional to the deployment of the Nexus 9000 with APIC/ACI to add additional ports if needed. The 9K switches with ACI, APIC, and optional Fabric Extender are collectively referred to as TOE or individually as TOE Components. The 9300 switches are fixed form factor and the 9500 switches are modular and are available in 8, 32, 36 and 48 slot chassis. The 9500 modular chassis can be outfitted with the following types of modules; noting that at least one supervisor module and one-line card is required. The fabric modules are optional.

- Supervisor modules: Supervisor modules provide scalable control plane and management functions for the switch. The Supervisor modules control Layer 2 and 3 services, redundancy capabilities, configuration management, status monitoring, power and environmental management, and transparent upgrades to I/O and fabric modules.
- Fabric modules: Fabric modules provide the central switching element for fully distributed forwarding on the I/O modules. The addition of each Fabric Module increases the bandwidth to all module slots. The Cisco Nexus 9500 platform supports up to six fabric modules, each with up to 10, 24-Tbps line-rate packet forwarding capacity. All fabric cards are directly connected to all line cards. With load balancing across fabric cards, the architecture achieves optimal bandwidth distribution within the chassis. For additional information, see here https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-736677.html#Productoverview
- Line Card I/O modules: The Line Card Modules are full-featured, high-performance modules with support for high-density 10, 40 and 100 Gigabit Ethernet interfaces.

1.2.1 APIC/ACI

The Cisco Application Policy Infrastructure Controller (Cisco APIC) provides a single security management interface to manage to the TOE. The APIC is the security management interface of the Cisco ACI fabric solution. The APIC is the single point of security management for the Cisco ACI fabric, policy enforcement, and monitoring. The APIC appliance is a centralized, clustered controller that optimizes performance and unifies operation of physical and virtual environments.

The Authorized Administrator can securely connect to the APIC command line interface (CLI) over SSHv2 secure connection and the web based graphical interface (GUI) over HTTPS/TLSv1.2

secure connection. The APIC is a hardware appliance with a software-only image that includes an underlying Linux OS that runs on APIC-SERVER-L3 (UCS C220 M5) or APIC-SERVER-M3 (UCS C240 M5) hardware.

The Cisco ACI fabric is composed of the APIC and the Cisco Nexus 9000 Series with ACI mode leaf and spine switches. The Cisco APIC provides centralized access to all fabric information and supports flexible application provisioning across physical and virtual resources. Cisco ACI consists of:

- APIC
- Nexus 9000 Series Switches in ACI spine and leaf configuration

Typically, the APIC will be deployed in a cluster with a minimum of three controllers for scalability and redundancy purposes, though is not required. Any controller in the cluster can service any user for any operation, and a controller can be transparently added to or removed from the Cisco APIC cluster. The minimum deployment configuration is 1 spine, 2 leafs and 1 APIC.

The Cisco APIC is a physically distributed but logically centralized controller that provides configuration and image management to the fabric for automated startup and upgrades. The Cisco Nexus ACI fabric software is bundled as an ISO image, which can be installed on the Cisco APIC appliance server through the serial console. The Cisco Nexus ACI Software ISO contains the Cisco APIC image, the firmware image for the leaf node, the firmware image for the spine node, default fabric infrastructure policies and required protocols. The switch images are installed on the 9K switches in ACI mode.

The Cisco APIC supports zero-touch provisioning which is a method to automatically bring up the Cisco ACI fabric with the appropriate connections (See Figure 1). After Link Layer Discovery Protocol (LLDP) discovery learns all neighbouring connections dynamically, these connections are validated against a specification rule such as “LEAF can connect to only SPINE-L1-*” or “SPINE-L1-* can connect to SPINE-L2-* or LEAF.” If a rule mismatch occurs, a fault occurs, and the connection is blocked. In addition, an alarm is created indicating that the connection needs attention. Intermediate System-to-Intermediate System (IS-IS) protocol is used within the ACI. Each IS-IS device acts as a router and independently builds a database of the network's topology similar to Open Shortest Path First (OSPF). The Cisco ACI fabric operator has the option of importing the names and serial numbers of all the fabric nodes from a simple text file into the Cisco APIC or discovering the serial numbers automatically and assigning names from the Cisco APIC CLI and GUI.

Before any controller or leaf or spine switch becomes a member of the Cisco ACI fabric, it must be authenticated and admitted by the fabric administrator via the management interface. After that, it becomes an operational component of the fabric.

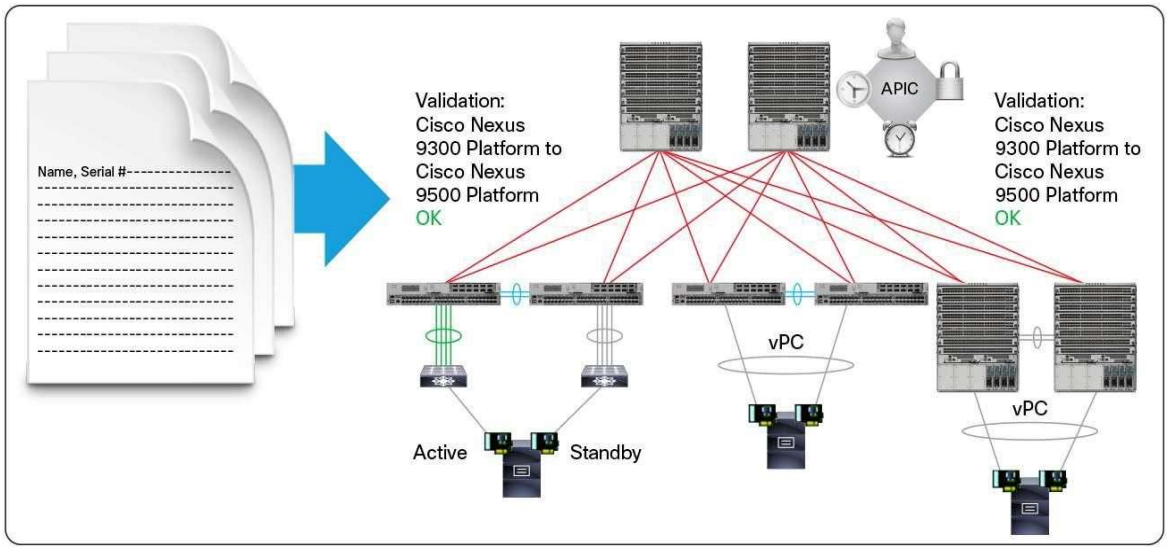

Figure 1 Cisco Automatic Provisioning

In the unlikely event an unauthorized switch is manually cabled to the ACI fabric, there will be a fault raised in the APIC indicating a rogue device was denied to the fabric. The device will not be discovered or authenticated to the ACI fabric.

1.2.2 TOE Product Type

The Cisco Nexus 9500 component is an aggregation switch in the data center. They can be deployed in standalone mode using NX-OS or with the implementation of Application Centric Infrastructure (ACI). In the evaluated configuration, the TOE will be configured in ACI mode.

The following figure provides a visual depiction of the TOE deployment configured in ACI mode.

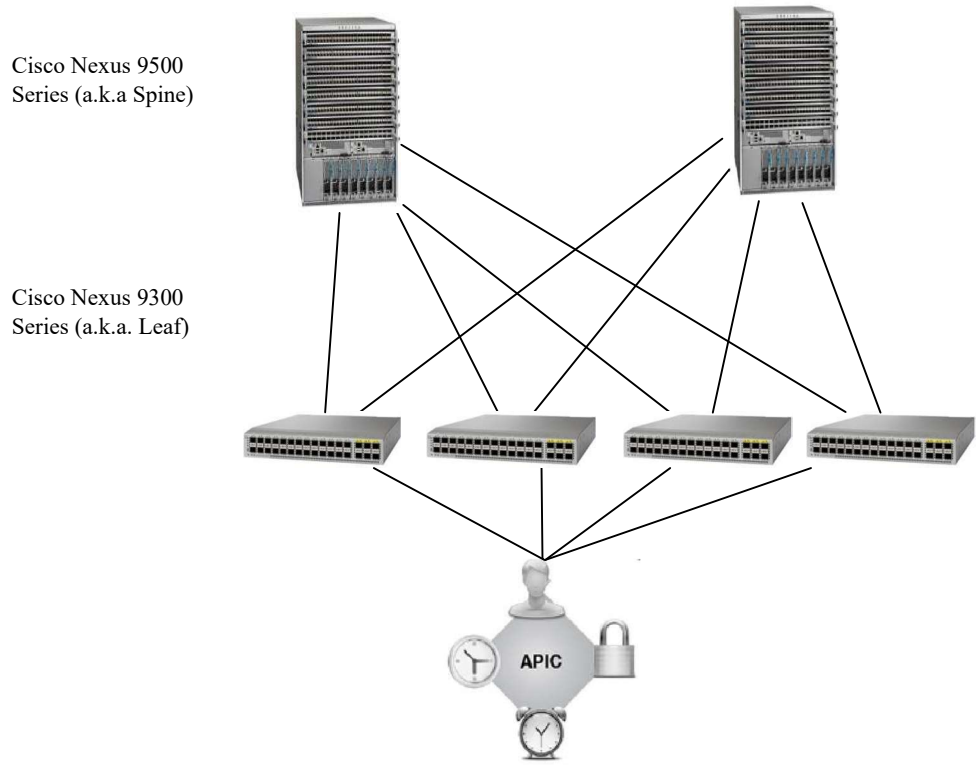

Figure 2 Cisco Nexus APIC ACI TOE Deployment

The APIC is directly connected to the Cisco Nexus 9300 switches only. The Cisco Nexus 9300, also referred to as the 'leaf' switches, are attached to the Cisco Nexus 9500, also referred to as the 'spine' switches and never to each other.

The Cisco Nexus 9500 is a modular chassis that supports up to 16 line cards, 2 supervisor modules, 2 chassis controllers, 3 fan trays, 6 fabric modules, and 10 power supplies. The switch supports comprehensive Layer 2 and 3 functions on nonblocking 1, 10, 40 and 100 Gigabit Ethernet ports.

The Cisco Nexus 9300 platform consists of fixed-port switches designed for top-of-rack (ToR) and middle-of-row (MoR) deployment in data centers that support enterprise applications, service provider hosting, and cloud computing environments. They are Layer 2 and 3 nonblocking 10 and 40 Gigabit Ethernet switches with up to 2.56 terabits per second (Tbps) of internal bandwidth.

Cisco NX-OS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching as well as network virtualization. NXOS is a next-generation data center class operating system designed for maximum scalability and application availability. The NX-OS data center class operating system was built with modularity, resiliency, and serviceability at its foundation. NX-OS is based on the industry proven Cisco Storage Area Network Operating System (SAN-OS) Software and helps ensure continuous availability to set the standard for mission-critical data center environments.

NX-OS provides virtual routing and forwarding capabilities that logically segment the network by virtualizing both the routing control plane and data plane functions into autonomous instances. Routing protocols and interfaces, both physical and logical, become members of a specific VRF instance via configuration. For each VRF, IPv4 and IPv6 tables are created automatically and independent routing and forwarding decisions are made. NX-OS supports up to 1000 unique VRF instances.

For management purposes the TOE provides interfaces to administer the TOE. This TOE only addresses the functions that provide for the security of the TOE itself as described in 1.6 Logical Scope of the TOE below.

1.3 Supported non-TOE Hardware/Software/Firmware

Following is the list of environment components, in some cases optionally for the secure and functional operation of the TOE in its evaluated configuration. It is recommended the operational environment components be installed in a controlled environment where implementation of security policies can be enforced, and access controlled. The Authorized Administrator is responsible for the secure operation of the TOE. While the Authorized Administrator may be assigned responsibility of some or all of the operational environment components that responsibility is not covered by this document unless specifically document within.

Table 4 Environment Components

Component	Required	Usage/Purpose Description for TOE performance
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 Authorized Administrator to support TOE administration.
Firewall	Yes	This includes a firewall that must be placed between the ACI fabric and an external network.
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with an SSH client installed that is used by the TOE Authorized Administrator to support TOE administration through SSH protected path. Any SSH client that supports SSHv2 may be used.
Management Workstation using web browser for HTTPS/TLSv1.2	Yes	This includes any IT Environment Management workstation with a web browser installed that is used by the TOE Authorized Administrator to support TOE administration through HTTPS/TLSv1.2 protected path. Any web browser that supports HTTPS/TLSv1.2 may be used.
NTP Server	Yes	The TOE supports communications with an NTP server.
Syslog Server	No	This includes any syslog server to which the TOE would transmit syslog messages.
RADIUS or TACACS+ AAA Server	No	This includes any IT environment RADIUS or TACACS+ AAA server that provides single-use authentication mechanisms. The TOE correctly leverages the services provided by this RADIUS or TACACS+ AAA server to provide single-use authentication to administrators.

1.4 TOE Description

This section provides an overview of the Target of Evaluation (TOE) Cisco that comprise the Nexus 9000 Switch Series with ACI mode, APIC, Nexus 2000 Fabric Extenders and the NX-OS System Software-ACI v14.2(4o) and APIC v4.2(4o). The TOE includes both the software and hardware.

The Cisco Nexus 9000 switches and the APIC appliances have common hardware characteristics. These characteristics affect only non-TSF relevant functions of the switches (such as throughput and amount of storage) and therefore support security equivalency of the switches in terms of hardware. All security functionality is enforced on the Nexus 9000 Series switches and APIC. Table 5 below, describes the models have been claimed within this evaluation.

Table 5 Hardware Models and Specification

Model	Description	Interfaces
Cisco 9300 ACI Leaf Models		
93180LC-EX	32 x 40/50-Gbps QSFP+ ports OR 18 x 100-Gbps QSFP28 ports, 4 cores CPU, 24 GB system memory, 64 GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
93108TC-EX	48 x 10GBASE-T and 6 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 64GB SSD, Power supplies (up to 2) 500W AC, 650W AC, 930W DC, or 1200W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
93108TC-FX	48 x 100M/1/10GBASE-T ports and 6 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
9348GC-FXP	48 x 100M/1G BASE-T ports, 4 x 1/10/25-Gbps SFP28 ports and 2 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 1200W AC or 1200W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
93216TC-FX2	96 x 100M/1/10GBASE-T ports and 12 x 40/100-Gigabit QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
93180YC-EX	48 x 1/10/25-Gbps and 6 x 40/100-Gbps QSFP28 ports, 6 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC	1 RJ-45 port - (L1 and L2 ports are unused) 1 USB port 1 RS-232 serial port
93180YC-FX	48 x 1/10/25-Gbps and 6 x 40/100-Gbps QSFP28 ports, 6 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC	1 RJ-45 port - (L1 and L2 ports are unused) 1 USB port 1 RS-232 serial port
93240YC-FX2	48 x 1/10/25-Gbps fiber ports and 12 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 1100W AC, 1100W DC, or 1100W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port

Model	Description	Interfaces
93360YC-FX2	96 x 1/10/25-Gbps and 12 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 1200W AC, or 1200W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
9336C-FX2	36 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 1100W AC, 1100W DC, or 1100W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
9364C-GX	64 x 100/40-Gbps QSFP28 ports, 4 core CPU, 32GB system memory, 128GB SSD, Power supplies (up to 2) 1100W AC, 1100W DC, or 1100W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
9316D-GX	16 x 400/100/40-Gbps QSFP-DD ports, 4 core CPU, 32GB system memory, 128GB SSD, Power supplies (up to 2) 1100W AC, 1100W DC, or 1100W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
93600CD-GX	28 x 100/40-Gbps QSFP28 ports and 8 x 400/100-Gbps QSFP-DD ports, 4 core CPU, 32GB system memory, 128GB SSD, Power supplies (up to 2) 1100W AC, 1100W DC, or 1100W HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
Cisco 9300 and 9500 ACI Spine Models		
9332C	32-port 40/100G QSFP28 ports and 2-port 1/10G SFP+ ports, 4 core CPU, 16GB system memory, 128GB SSD, Power supplies 1100W AC, 1100W DC, or 2000W HVAC/HVDC	Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP) 1 USB port 1 RS-232 serial port
9364C	64-port 40/100G QSFP28 ports and 2-port 1/10G SFP+ ports, 4 core CPU, 32GB system memory, 128GB SSD, Power supplies 1200W AC, 93000W DC, or 1100W HVAC/HVDC	Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP) 1 USB port 1 RS-232 serial port
9504	Chassis: 4-slot, up to 4 line cards, up to 4 power supplies, up to 6 fabric modules of same type, up to 2 system controllers, up to 2 supervisors of the same type, and up to 3 fan trays	Based on Supervisor and ACI compatible I/O modules installed. Each line card should be ACI compatible
9508	Chassis: 8-slot, up to 8 line cards, up to 8 power supplies, up to 6 fabric modules of same type, up to 2 system controllers, up to 2 supervisors of the same type, and up to 3 fan trays	Based on Supervisor and ACI compatible I/O modules I/O modules installed
9516	Chassis: 16-slot, up to 16 line cards, up to 10 power supplies, up to 6 fabric modules of same type, up to 2 system controllers, up to 2 supervisors of the same type, and up to 3 fan trays	Based on Supervisor and ACI compatible I/O modules I/O modules installed
Cisco 9500 Model Components		
Supervisor A/A+	4 core cpu, 16 GB of memory and 64 GB of SSD (N9K-SUP-A/A+)	Two USB ports, a serial port, and a 10/100/1000-Mbps Ethernet port
Supervisor B /B+	6 core cpu, 24 GB of memory and 256 GB of SSD (N9K-SUP-B/B+)	Two USB ports, a serial port, and a 10/100/1000-Mbps Ethernet port

Model	Description	Interfaces
Line Card I/O Modules	N9K-X9432C-S: 100 Gigabit Ethernet Line Card	32-port 100-Gigabit Ethernet QSFP28 line card. Every QSFP28 supports 1 x 100, 2 x 50, 1 x 40, 4 x 25, and 4 x10 Gigabit Ethernet
	N9K-X9736PQ: 40 Gigabit Ethernet Line Card	36-port 40-Gigabit Ethernet QSFP+ line card
	N9K-X9636PQ: 40 Gigabit Ethernet Line Card	36-port 40 -Gigabit Ethernet QSFP+ line card
	N9K-X9536PQ: 40 Gigabit Ethernet Line Card	• 36-port 40-Gigabit Ethernet QSFP+ line card • Supports Virtual Extensible LAN (VXLAN) routing and bridging • 1.5:1 oversubscription
	N9K-X9432PQ: 40 Gigabit Ethernet Line Card	32-port 40 Gigabit Ethernet QSFP+ line card
	N9K-X9564PX: 1 and 10 Gigabit Ethernet and 10 and 40 Gigabit Ethernet Line Card	• 48-port 1- and 10-Gigabit Ethernet SFP+ with 4-port 40-Gigabit Ethernet QSFP+ line card • Supports VXLAN routing and bridging
	N9K-X9464PX: 1- and 10-Gigabit Ethernet and 10- and 40-Gigabit Ethernet Line Card	48-port 1- and 10-Gigabit Ethernet SFP+ with 4-port 40-Gigabit Ethernet QSFP+ line card
	N9K-X9564TX: 1 and 10 Gigabit Ethernet Copper and 10 and 40 Gigabit Ethernet Line Card	• 48-port 1 and 10GBASE-T plus 4-port 40-Gigabit Ethernet QSFP+ line card • Supports VXLAN routing and bridging • Supports 100-Megabit Ethernet, 1-Gigabit Ethernet, and 10GBASE-T copper cabling connectivity for server access

Model	Description	Interfaces
	N9K-X9464TX2: 1 and 10 Gigabit Ethernet Copper and 10 and 40 Gigabit Ethernet Line Card	• 48-port 1 and 10GBASE-T plus 4-port 40-Gigabit Ethernet QSFP+ line card • Line rate for packets greater than 200 bytes • Supports 100-Megabit Ethernet, 1-Gigabit Ethernet, and 10GBASE-T copper cabling connectivity for server access
Cisco 2000 Series Fabric Extenders		
2248TP-E	48 x 100/1000BASE-T host interfaces and 4 x 10 Gigabit Ethernet fabric interfaces (SFP+)	As described
2232PP-10GE	32 x 1/10 Gigabit Ethernet and Fibre Channel over Ethernet (FCoE) host interfaces (SFP+) and 8 x 10 Gigabit Ethernet and FCoE fabric interfaces (SFP+)	As described
2232TM-E	32 x 100M, 1/10GBASE-T host interfaces and uplink modules (8 x 10 Gigabit Ethernet fabric interfaces [SFP+]); FCoE support up to 30m with Category 6a and 7 cables	As described
2348TQ-E	48 x 100MBASE-T and 1/10GBASE-T port host interfaces (RJ-45) and up to 6 QSFP+ 10/40 Gigabit Ethernet fabric interfaces; FCoE support up to 30m with Category 6a and 7 cables	As described
2332TQ	32 x 100MBASE-T and 1/10GBASE-T port host interfaces (RJ-45) and up to 4 QSFP+ 10/40 Gigabit Ethernet fabric interfaces; FCoE support up to 30m with Category 6a and 7 cables	As described
2348TQ	48 x 100MBASE-T and 1/10GBASE-T port host interfaces (RJ-45) and up to 6 QSFP+ 10/40 Gigabit Ethernet fabric interfaces; FCoE support up to 30m with Category 6a and 7 cables	As described
2348UPQ	48 x 1/10 Gigabit Ethernet and unified port host interfaces (SFP+) and up to 6 QSFP+ 10/40 Gigabit Ethernet fabric interfaces	As described
APIC		

Model	Description	Interfaces
APIC (Medium - Large) and clustered (cluster requires at least three appliances)	APIC with medium-size CPU, hard drive, and memory configurations (up to 1200 edge ports) (APIC-SERVER-M3) APIC with large CPU, hard drive, and memory configurations (more than 1200 edge ports) (APIC-SERVER-L3) The type of virtual interface card (VIC) installed on the APIC determines the types of interface cables that can be used to connect the leaf switches to the APIC. • The VIC 1225T module supports copper connectors, copper cables, and switches with copper downlink ports (such as: Cisco Nexus 93108TC-EX, 93108TC-FX, 93120TX, 93128TX, 9372TX, 9372TX-E, and 9396TX switches). • The VIC 1225 module supports optical transceivers, optical cables, and switches with optical downlink ports (such as: Cisco Nexus 93180LC-EX, 93180YC-EX, 93180YC-FX, 9332PQ, 9336C-FX2, 9348GC-FXP, 9372PX, 9372PX-E, 9396PX, and 93600CD-GC switches). • The VIC 1455 module supports optical transceivers, optical cables, and switches with optical downlink ports (such as: Cisco Nexus 9336C-FX2, 93180LC-EX, 93180YC-EX, 93180YC-FX, 93240YC=FX2, and 93600CD-GC switches).	Dual 1-Gb/10-Gb Ethernet ports (LAN1 and LAN2) - The dual LAN ports can support 1 Gbps and 10 Gbps, depending on the link partner capability. 1-Gb Ethernet dedicated management port Serial port (RJ-45 connector) USB 3.0 ports (two)
APIC Appliance		
APIC-SERVER-L3 (UCS C220 M5)	**Rear panel** - One 1-Gbps RJ-45 management port (Marvell 88E6176), Two 10GBase-T LOM ports (Intel X550 controller embedded on the motherboard), One RS-232 serial port (RJ45 connector), One DB15 VGA connector, Two USB 3.0 port connectors, One flexible modular LAN on motherboard (mLOM) slot that can accommodate various interface cards **Front panel** - One KVM console connector (supplies two USB 2.0 connectors, one VGA DB15 video connector, and one serial port (RS232) RJ45 connector) **Modular LAN on Motherboard (mLOM) slot**. The dedicated mLOM slot on the motherboard can flexibly accommodate the following cards: • Cisco Virtual Interface Cards • Quad Port Intel i350 1GbE RJ45 Network Interface Card (NIC)	As described

Model	Description	Interfaces
APIC-SERVER-M3 (UCS C240 M5)	**Rear panel -** One 1-Gbps RJ-45 management port (Marvell 88E6176), • Two 10GBase-T LOM ports (Intel X550 controller embedded on the motherboard), One RS-232 serial port (RJ45 connector), One DB15 VGA connector, Two USB 3.0 port connectors, One flexible modular LAN on motherboard (mLOM) slot that can accommodate, various interface cards **Front panel -**One KVM console connector (supplies two USB 2.0 connectors, one VGA DB15 video connector, and one serial port (RS232) **Modular LAN on Motherboard (mLOM) slot** The dedicated mLOM slot on the motherboard can flexibly accommodate the following cards: • Cisco Virtual Interface Cards • Quad Port Intel i350 1GbE RJ45 mLOM Network Interface Card (NIC)	As described

1.4.1 TOE Evaluated Configuration

The TOE consists of one or more switches as specified in Section 1.4.2 Physical Scope of the TOE below and includes the Cisco NX-OS and APIC software. The TOE has two or more network interfaces and is connected to an ACI fabric with APIC that is used for configuration and management of the switches. The Cisco NX-OS configuration determines how packets are handled to and from the TOE's network interfaces. The switch configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination. The following routing protocols are used on all of the TOE models:

- Open Shortest Path First (OSPF) Protocol Versions 2 (IPv4) and 3 (IPv6)
- Intermediate System-to-Intermediate System (IS-IS) Protocol for IPv4
- Border Gateway Protocol (BGP) for IPv4 and IPv6
- Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv4 and IPv6
- Routing Information Protocol Version 2 (RIPv2)
- Protocol Independent Multicast (PIM)

When the TOE is configured for ACI mode, the Nexus 9000 Series Switches are remotely administered via the APIC CLI over SSHv2 secure connection or APIC GUI over a HTTPS/TLSv1.2 secure connection. The APIC controller is using direct fiber to connect to the leaf switch. The TOE can optionally connect to an NTP server on its internal network for time services.

Once an Authorized Administrator has successfully authenticated to the APIC, the whole fabric (ACI) is a private IP network which is used for fabric auto-discovery via LLDP and IS-IS. If the Authorized Administrator configures in-band or out-of-band management access, then an endpoint group (EPG) and a contract must be configured in order to apply a whitelist firewall filter.

The following figure provides a visual depiction of the TOE deployment, including environment components.

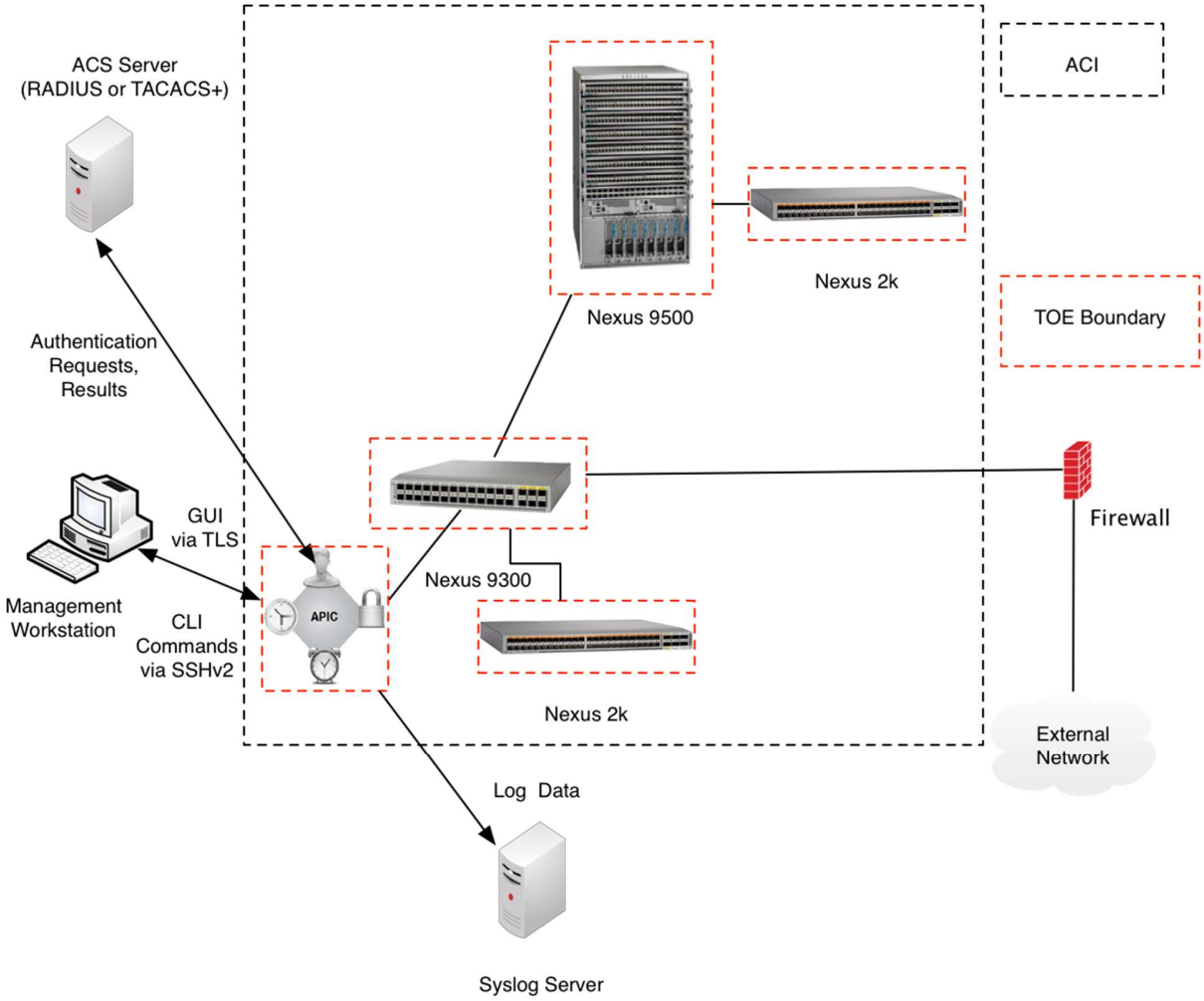

Figure 3 TOE and Environment Components

The evaluated configuration is the configuration of the TOE that satisfies the requirements as defined in this Security Target (ST). For example,

- Security Audit - The TOE generates audit records to assist the Authorized Administrator in monitoring the security state of the TOE as well as trouble shooting various problems that arise throughout the operation of the system. Audit records are stored locally and may be backed up to a remote syslog server. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.
- Full Residual Information Protection - The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic.

- Identification and authentication - The TOE ensures that all Authorized Administrator are successfully identified and authenticated prior to gaining access to the TOE. The TOE also performs device level authentication. The TOE can optionally be configured to support IT environment RADIUS or TACACS+ AAA server that provides single-use authentication mechanisms. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.
- Information Flow Control - The TOE provides the ability to control traffic flow into or out of the Nexus 9000 switch
- Secure 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. In addition, the web-based GUI can be used for TOE administration using HTTPS/TLSv1.2 secure connection. The TOE provides the ability to securely manage:
  - Review audit record logs;
  - Manage information flow policies and rules;
  - Maintain the timestamp;
  - Manage Authorized Administrators security attributes and
  - Administer the TOE remotely
- Protection of the TSF - The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication and limits configuration and access to Authorized Administrators.
- TOE Access – The TOE displays a warning banner prior to allowing any administrative access to the TOE. The TOE also provides the mechanism for the Authorized Administrators to terminate their own sessions.
- Trusted Path – The TOE ensures trusted paths are established to itself from remote administrators over secure SSHv2 connection for remote CLI access and secure HTTPS/TLSv1.2 connection for the web-based GUI

1.4.2 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the switch models as follows: Nexus 9300, 9500, 2000, APIC-SERVER-L3 (UCS C220 M5) and APIC-SERVER-M3 (UCS C240 M5).

The TOE is comprised of the hardware platforms as described in Table 5 Hardware Models and Specification above. Deployment of the Nexus 2000 is optional for additional ports and cable management purposes. For ordering of the TOE and delivery via commercial carries, see https://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/sales-resources-listing.html and https://www.cisco.com/c/en/us/buy.html

The software is the Cisco NX-OS software image and APIC software image Releases: NX-OS System Software-ACI 14.2(4o), APIC 4.2(4o). The network on which they reside is considered part of the environment. The software file format for the 9K is a bin file and the APIC software

file format is an iso file. For ordering and downloading the TOE software, see https://software.cisco.com/#

The TOE Administrator Guidance Documentation (AGD) that is considered to be part of the TOE is the Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders Common Criteria Operational User Guidance and Preparative Procedures, a PDF document that can be downloaded from the https://www.cisco.com/

The following product documentation that is referenced in this document and the Common Criteria Operational User Guidance and Preparative Procedures are downloadable from Cisco web sites:

- https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-installation-and-configuration-guides-list.html
- https://www.cisco.com/c/en/us/support/switches/nexus-2000-series-fabric-extenders/products-installation-and-configuration-guides-list.html
- https://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-installation-and-configuration-guides-list.html
- https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html (APIC)

1.4.3 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
- Full Residual Information Protection
- Identification and Authentication
- Information Flow Control
- Secure Management
- Protection of the TSF
- TOE Access
- Trusted Path

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

1.4.3.1 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 and the GUI 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.

1.4.3.2 Full Residual Information Protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic.

1.4.3.3 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 and web-based GUI). 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.

1.4.3.4 Information Flow Control

The TOE provides the ability to control traffic flow into or out of the Nexus 9000 switch. The following types of traffic flow are controlled for both IPv4 and IPv6 traffic:

- Layer 3 Traffic – RACLs
- Layer 2 Traffic – PACLs
- VLAN Traffic – VACLs
- Virtual Routing and Forwarding - VRFs

A RACL is an administratively configured Information Flow Control list that is applied to Layer 3 traffic that is routed into or out of the Nexus 9000 Series switch. A PACL is an administratively configured Information Flow Control list that is applied to Layer 2 traffic that is routed into Nexus 9000 Series switch. A VACL is an administratively configured Information Flow Control list that is applied to packets that are routed into or out of a VLAN or are bridged within a VLAN. The Virtual Routing and Forwarding (VRF), allow multiple instances of routing tables to exist within the Nexus 9000 Series switch TOE component simultaneously.

1.4.3.5 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. In addition, the web-based GUI can be used for TOE administration using HTTPS/TLSv1.2 secure connection. The TOE provides the ability to securely manage:

- Manage audit functionality
- Manage Information Flow Control Policies and Rules
- Manage Authorized Administrator's security attributes
- Review audit record logs
- Maintain the system time

1.4.3.6 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 NX-OS is not a general-purpose operating system and access to Cisco NXOS memory space is restricted to only Cisco NX-OS functions.

The TOE use of Information Flow Control Policies and Rules to ensure routing protocol communications between the TOE and neighbor 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 can configure the TOE to use NTP to synchronize the TOE's clock with an external time source.

Finally, the TOE performs power-up self-tests and conditional self-tests to verify correct operation of the switch itself.

1.4.3.7 TOE Access

The administrator can terminate their own session by exiting out of the CLI and GUI. The TOE can also be configured to display an Authorized Administrator specified banner on the CLI and GUI management interfaces prior to allowing any administrative access to the TOE.

1.4.3.8 Trusted Path

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 for remote CLI access and HTTPS/TLSv1.2 for the web-based GUI on the APIC.

1.5 Excluded Functionality

The following functionality is excluded from the evaluation.

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

1.6 TOE Documentation

This section identifies the guidance documentation included in the TOE. The documentation for the Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders comprises:

- Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders Common Criteria Operational User Guidance and Preparative Procedures, v1.0 dated [TBD].

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

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

- EAL2

2.2 Protection Profile Conformance

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

Assumptions	Assumption Definition
A.FIREWALL	A firewall provided by the operational environment will be located between the ACI fabric and external networks to protect against malicious or unauthorized traffic from entering the ACI fabric.
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.TRUSTED_ADMIN	All Authorized Administrators are assumed not evil, will follow the administrative guidance and will not disrupt the operation of the TOE intentionally.

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.NET_TRAFFIC	An unauthorized user (attacker) may attempt to send malicious traffic through/to the TOE
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNAUTHORIZED_ACCESS	An unauthorized user (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.

Threat	Threat Definition
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

3.3 Organizational Security Policies

The following table lists the Organizational Security Policies imposed by an organization to address its security needs.

Table 8 Organization Security Policies

Policy Name	Policy Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by gaining authorized access to the 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 9 Security Objectives for the TOE

TOE Objective	TOE 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_REVIEW	The TOE will provide the Authorized Administrator the capability to review audit data.
O.DATA_FLOW_CONTROL	The TOE shall ensure that only authorized traffic is permitted to flow through the TOE to its destination via the configured application profile rules.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE prior to the Authorized Administrator successfully gaining access to the TOE.
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all Administrative users before granting management access.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SELF_FPROTECT	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.TSF_SELF_TEST	The TOE will provide the capability to test the security functionality to ensure it is operating properly.

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 10 Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.ADMIN	The Authorized Administrator is well trained and trusted to manage the TOE, to configure the IT environment and required non-TOE devices for the proper network support.
OE.CONNECTION	The operational environment will have the required protected network support for the operation of the TOE to prevent unauthorized access to the TOE.
OE.FIREWALL	The operational environment of the TOE shall provide a firewall located between the ACI fabric and external networks to protect against malicious or unauthorized traffic from entering the ACI fabric.
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.

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:

- 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. For example, FDP_IFF.1(1) and FDP_IFF.1(2) indicate that the ST includes two iterations of the FDP_IFF.1 requirement, (1) and (2).
- 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 (i.e., those not found in Part 2 of the CC) are identified with "(EXT)" in of the functional class/name.
- 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

Functional Component	
Requirement Class	**Requirement Component**
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 trail storage
FDP: User data protection	FDP_IFC.1: Complete information flow control
	FDP_IFF.1: Simple security attributes
	FDP_RIP.2: Full Residual Information Protection
FIA: Identification and authentication	FIA_ATD.1 User attribute definition
	FIA_SOS.1 Verification of secrets

Functional Component	
	FIA_UAU.2 User authentication before any action
	FIA_UAU.7: Protected authentication feedback
	FIA_UID.2 User identification before any action
FMT: Security management	FMT_MSA.1 Secure Security Attributes
	FMT_MSA.3 Static Attribute Initialization
	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
	FPT_TST.1: TSF Testing
FTA: TOE Access	FTA_SSL.4: User-initiated Termination
	FTA_TAB.1: Default TOE Access Banners
FTP: Trusted Path	FTP_TRP.1: Trusted Path

5.2.1 Security audit (FAU)

5.2.1.1 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:

a) Start-up and shut-down of the audit functions;
b) All auditable events for the [***not specified***] level of audit **specified in Table 12 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 ~~PP~~/ST, [**information specified in the Additional Audit Record Contents column of Table 12 Auditable Events**].

Table 12 Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_SAR.1	None.	
FAU_STG.1	None.	
FDP_IFC.1	None	
FDP_IFF.1	None	
FDP_RIP.2	None	
FIA_ATD.1	None	
FIA_SOS.1	None	

Requirement	Auditable Events	Additional Audit Record Contents
FIA_UAU.2	All use of the authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU.7	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	
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	
FPT_STM.1	Changes to the time.	The identity of the authorized administrator performing the operation.
FPT_TST.1	Execution of the TSF self tests and the results of the tests	None
FTA_SSL.4	Termination of an interactive session by the user	None
FTA_TAB.1	None	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.

5.2.1.2 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.

5.2.1.3 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.

5.2.1.4 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.

5.2.2 User data protection (FDP)

5.2.2.1 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [**Information Flow Control SFP**] on [

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

].

5.2.2.2 FDP_IFF.1 Simple security attributes

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

Subjects: Physical network interfaces and virtual network interfaces
Subject security attributes:

- **Interface identifier (within EPG)**
- **VLAN or VxLAN identifier (if applicable)**
- **Tenant (VRF) identifier (if applicable)**

Information: Network Packets
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 authorise an information flow based on the following rules: [

- **DHCP traffic received on interfaces configured as trusted is always allowed to pass, or**
- **ARP traffic received on interfaces configured as trusted is always allowed to pass**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:
[

- **For IP Network Traffic Flows:**
  - The TOE denies IP traffic flow (broadcast, unknown multicast or unknown unicast) of the Layer 2 traffic is not identified as trusted via a whitelist EPG to EPG combination through Traffic Storm;
  - For IP traffic, if the security attributes do not match an administratively configured Contracts (RACL or VACL) via a whitelist EPG to EPG, the traffic flow is denied;
  - If the IP traffic security attributes do not map to a configured context tenant (VRF), the traffic flow is denied
- **For Non-IP Network Traffic Flows:**
  - For Non-IP traffic, if security attributes do not match an administratively configured Contract (RACL, PACL, or VACL) via a whitelist EPG to EPG, the traffic flow is denied

].

5.2.2.3 FDP_RIP.2 Full Residual Information Protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**deallocation of the resource from**] **all** objects.

5.2.3 Identification and authentication (FIA)

5.2.3.1 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**].

5.2.3.2 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, numeric characters, and the following special characters represented on US keyboard, with the following exception: passwords cannot include these special characters at the beginning of the password: quotation marks (" or '), vertical bars (|), or right angle brackets (>)**].

5.2.3.3 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.

5.2.3.4 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.

5.2.3.5 FIA_UID.2 User Identification Before Any Action

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

5.2.4 Security management (FMT)

5.2.4.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [**Information Flow Control SFP**] to restrict the ability to [***modify***] the security attributes [**defined FDP_IFC.1**] to [**Authorized Administrator**].

5.2.4.1 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.

5.2.4.2 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**].

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

5.2.4.4 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.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 FPT_STM.1 Reliable time stamps

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

5.2.5.2 FPT_TST.1 TSF Testing

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

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of [***TSF data***].

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

5.2.6 TOE Access (FTA)

5.2.6.1 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.

5.2.6.2 FTA_SSL.4: User-initiated termination

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

5.2.7 Trusted Path (FTP)

5.2.7.1 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*]**].

5.3 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
FDP_RIP.2	No dependencies	N/A
FIA_ATD.1	No dependencies	N/A
FIA_SOS.1	No dependencies	N/A
FIA_UAU.2	FIA_UID.1	Met by: FIA_UID.1
FIA_UAU.7	FIA_UAU.1	Met by: FIA_UAU.2
FIA_UID.2	No dependencies	N/A
FMT_MSA.1	FDP_AFF.1 or 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
FPT_STM.1	No dependencies	N/A
FPT_TST.1	No dependencies	N/A
FTA_SSL.4	No dependencies	N/A
FTA_TAB.1	No dependencies	N/A
FTP_TRP.1	No dependencies	N/A

5.4 Security Assurance Requirements

5.4.1 SAR Requirements

The TOE assurance requirements for this ST are EAL2 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
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

5.4.2 Security Assurance Requirements Rationale

This Security Target claims conformance to EAL2. 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.

5.5 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 15 SAR Assurance Measures

Component	How the requirement will be met
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

Component	How the requirement will be met
	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.
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.
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

This section 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, VACL 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 Table 12 Auditable Events
FAU_SAR.1 FAU_STG.1	The Authorized Administrators can view the audit log records via the CLI or GUI interfaces, though the preference is the GUI 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 log files generated on the 9300 and 9500, include events and faults that are transferred to the APIC in the event manager, fault history. The fault history audit log file can be viewed by the Authorized Administrator using the APIC GUI and APIC CLI.
FDP_IFC.1 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 Nexus Layer 3 interface, VLAN interfaces, 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

TOE SFRs	How the SFR is Met
	devices that do not comply with administratively configured security policies, the TOE either denies the traffic flow or redirects to an interface.
FDP_RIP.2	The TOE ensures that packets transmitted from the TOE do not contain residual information from data deallocated from previous packets. Packets that are not the required length, the TOE uses zeros for padding. Packet handling within memory buffers ensures new packets cannot contain portions of previous packets. Packet buffers are used to form a packet in software. The contents of the buffers are sent to the ethernet driver with the appropriate addresses and 64-byte length packet that needs to be transmitted. Once the packet is sent and the buffers are deallocated, new packet data overwrites the old. If the outgoing packet has a size less than 64 bytes then the packet is padded so that it is 64 bytes in length. The buffers are deallocated and reused once the operation is over. This applies to both data plane traffic and administrative session traffic.
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, by default, the TOE is set to check for password-strength which prevents the user from choosing weak passwords. The password must be at least eight characters, include both upper and lower alpha characters, numeric characters and may include the following special characters represented on US keyboard, with the following exception: passwords cannot include these special characters at the beginning of the password: quotation marks (" or '), vertical bars (|), or right angle brackets (>) 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	The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed on behalf of that Administrator user. Administrative access to the TOE is facilitated through the TOE's GUI and CLI interfaces. The TOE mediates all administrative actions through the CLI and GUI. Once a potential administrative user attempts to access the CLI and GUI of the TOE through either a directly connected console or remotely, the TOE 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. Authentication may be provided via either: Authentication against a local database, or Remote authentication (facilitated by IT environment RADIUS or TACACS+ if configured)
FIA_UAU.7	When a user enters their password at the local console, CLI or GUI, 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.

TOE SFRs	How the SFR is Met
FMT_MSA.3	TOE provides restrictive default values for resources information flow control. There are no default access rules on the TOE, therefore no packet flows are allowed. Packet flows are only allowed once the information flow control policies are configured and applied.
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 GUI webpages with an HTTPS/TLSv1.2 secure connection and 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 user name 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 GUI webpages with an HTTPS/TLSv1.2 secure connection and the CLI with SSHv2secure session.
FPT_STM.1	The TOE provides a hardware-based clock timestamp that is used to provide the timestamp in audit records. In the evaluated configuration Network Time Protocol (NTP), a time synchronization protocol for nodes distributed across a network. The clocks are organized into a master-member synchronization hierarchy. Synchronization is achieved by exchanging NTP timing messages, with the members using the timing information to adjust their clocks to the time of their master in the hierarchy. When NTP is enabled, no external master clock (NTP server) is identified, therefore a 9500 switch (spine) will automatically be identified as the master clock during the configuration, to which all of the other components will synchronize the time.
FPT_TST.1	The TOE runs a suite of self-tests during initial start-up to verify its correct operation. The TOE also runs the suite of tests during resets/reboots. If any of the self-tests fail, the TOE transitions into an error state. In the error state, all secure data transmission is halted and the TOE outputs status information indicating the failure. Refer to the Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders Common Criteria Operational User Guidance and Preparative Procedures for information and troubleshooting if issues are identified.
FTA_SSL.4	The Authorized Administrator is able to exit out of both local and remote administrative sessions. For the CLI, the administrator types 'exit' on the command line. For the GUI web interface, the administrator selects 'logout'

TOE SFRs	How the SFR is Met
FTA_TAB.1	The TOE displays a customizable login banner on the local and remote CLI and GUI management interface prior to allowing any administrative access to the TOE.
FTP_TRP.1	The TOE ensures the communication path and the remote administer interfaces is protected and distinct from other communications paths. The remote administrative communications via the CLI that takes place over SSHv2 secure connection and via the GUI that takes place over HTTPS/TLSv1.2 secure connection.

6.2 TOE Bypass and Interference/Logical Tampering Protection Measures

The TOE consists of a hardware platform in which all operations in the TOE scope are protected from interference and tampering by untrusted subjects. All administration and configuration operations are performed within the physical boundary of the TOE. In addition, 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 CLI and GUI interfaces. There are no undocumented interfaces for managing the TOE.

All sub-components included in the TOE rely on the main Nexus 9000 Series switch for power, memory management and information flow control, while the TOE software provides the management functions and control. In order to access any portion of the Nexus 9000 switch, the Identification and Authentication mechanisms of the Nexus 9000 Series switch 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. None of these interfaces provides any access to internal TOE resources.

The Nexus 9000 Series switch provides a secure domain for its operation. Each component has its own resources that other components within the same Nexus 9000 Series switch platform are not able to affect.

There are no unmediated traffic flows into or out of either component of the TOE (Nexus 9000 Series switch). The information flow policies identified in the SFRs are applied to all traffic received and sent by the Nexus 9000 Series TOE component. Both communication types including data plane communication and control plane communications are mediated by the TOE. Control plane communications refer to administrative traffic used to control the operation of the TOE. There is no opportunity for unaccounted traffic flows to flow into or out of the TOE.

The Nexus 9000 Series switch provides a secure domain for each VLAN to operate within. Each VLAN has its own forwarding plane resources that other VLANs within the same Nexus 9000 Series switch TOE component are not able to affect.

The Nexus 9000 Series switch provides a secure domain for each VRF to operate within. Each VRF has its own resources that other VRFs within the same Nexus 9000 Series switch TOE component are not able to affect.

The TOE includes the NX-OS software which is installed on the Nexus 9000 series switch hardware, and the APIC software which is installed on the APIC-SERVER-L3 (UCS C220 M5) or APIC-SERVER-M3 (UCS C240 M5). The NX-OS software is resident within the TOE hardware and is protected by the mechanisms described above. The APIC software includes both a CLI and GUI interfaces. The APIC software is resident within the TOE hardware and is protected by the mechanisms described above.

This design, combined with the fact that only an Authorized Administrators have access to the TOE security functions, provides 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 Policy, Threats and Security Objectives Mappings

	T.ACCOUNTABILITY	T.NET_TRAFFIC	T.TSF_FAILURE	T.UNAUTHORIZED_ACCESS	T.USER_DATA_REUSE	P.ACCESS_BANNER
O.ACCESS_CONTROL			X	X		
O.ADMIN	X		X	X		
O.AUDIT_GEN	X					
O.AUDIT_REVIEW	X			X		
O.DATA_FLOW_CONTROL		X				
O.DISPLAY_BANNER						X
O.IDAUTH	X		X	X		
O.RESUDUAL_INFORMATION_CLEARING					X	
O.SELF_PROTECT			X	X		
O.TIME	X					
O.TSF_SELF_TEST			X			

Table 18 TOE Policy, Threats and Security Objectives 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.ADMIN and O.AUDIT_REVIEW objective mitigates the threat by requiring the TOE to provide the Authorized

Threat / Policy	Rationale for Coverage
	Administrator with the capability to view audit data. The O.IDAUTH objective requires the Administrative user to enter a unique identifier and authentication credentials before access to the TOE and management functions is granted. The O.TIME objective mitigates this threat by providing the accurate date/time to the TOE for use in the audit records.
T.NET_TRAFFIC	O.DATA_FLOW_CONTROL objective ensures that information flow control policies are enforced to limit access to an attacker (unauthorized device and/or user) sending malicious traffic to and/or through the TOE.
T.TSF_FAILURE	O.SELFPROTECT 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_FLOW_CONTROL objective protects the TOE configuration and user data from unauthorized disclosure. The O.IDAUTH objective requires the Administrative user to enter a unique identifier and authentication credentials before access to the TOE and management functions is granted. The O.ADMIN objective ensures the Authorized Administrator has access to the TOE to configure information flow controls and the O.ACCESS_CONTROL objective restricts access to the TOE and management functions to the Authorized Administrator.
T.UNAUTHORIZED_ACCESS	The O.ADMIN ensures the administrator has the capabilities to ensure proper configuration for maintaining a secure state and resource availability. The O.IDAUTH objective requires the Administrative user to enter a unique identifier and authentication credentials before access to the TOE and management functions is granted. The O.SELFPROTECT 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.
T.USER_DATA_REUSE	O.RESIDUAL_INFORMATION_CLEARING objective ensures that data traversing the TOE does not contain any data from a previous network traffic that transverses the TOE or to a user other than that intended by the sender of the original network traffic.
P.ACCESS_BANNER	This Organizational Security Policy is necessary to address the security objective O.DISPLAY_BANNER to ensure an advisory notice and consent warning message regarding unauthorized use of the TOE is displayed before the session is established.

7.2 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 19 Threats and IT Security Objectives Mappings for the Environment

	A.FIREWALL	A.LOCATE	A.TRUSTED_ADMIN
OE.ADMIN			X
OE.CONNECTION		X	
OE.FIREWALL	X	X	
OE.LOCATE		X	

Table 20 Assumptions/Threats/Objectives Rationale

Assumptions	Rationale for Coverage of Environmental Objectives
A.FIREWALL	The operational environment in which the TOE is installed requires a firewall to protect against malicious or unauthorized traffic from entering the ACI fabric. The OE.FIREWALL objective ensures a firewall is located between the ACI fabric and external 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. The OE.LOCATE and OE.CONNECTION objectives ensure the processing resources of the TOE, network connections and those services provided by the operational environment will be located within controlled access facilities, which will prevent unauthorized physical access. The OE.FIREWALL objective ensures a firewall is located between the ACI fabric and external networks.
A.TRUSTED_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.

7.3 Rationale for TOE Security Requirements and Security 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_REVIEW	O.DATA_FLOW_CONTROL	O.DISPALY_BANNER	O.IDAUTH	O.RESIDUAL_INFORMATION_CLEARING	O.SELF_PROTECT	O.TIME	O.TSF_SELF_TEST
FAU_GEN.1	X		X	X						X	
FAU_GEN.2	X		X	X						X	
FAU_SAR.1			X	X							
FAU_STG.1	X			X							
FDP_IFC.1					X				X		
FDP_IFF.1					X				X		
FDP_RIP.2								X			
FIA_ATD.1	X	X					X				
FIA_SOS.1		X					X				
FIA_UAU.2	X	X		X	X		X		X		
FIA_UAU.7							X				
FIA_UID.2	X	X		X	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						X	
FPT_TST.1									X		X
FTA_TAB.1						X					

	O.ACCESS_CONTROLL	O.ADMIN	O.AUDIT_GEN	O.AUDIT_REVIEW	O.DATA_FLOW_CONTROL	O.DISPALY_BANNER	O.IDAUTH	O.RESIDUAL_INFORMATION_CLEARING	O.SELF_PROTECT	O.TIME	O.TSF_SELF_TEST
FTA_SSL.4	X						X				
FTP_TRP.1	X	X					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 and 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 attributes 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.4 also meets this objective by allowing the Authorized Administrator to terminate their own session.
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 and HTTPS/TLSv1.2 [FTP_TRP.1].

Objective	Rationale
O.AUDIT_GEN	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, FAU_GEN.2 and FA_SAR.1]. Timestamps associated with the audit record must be reliable [FPT_STM.1].
O.AUDIT_REVIEW	The TOE will provide the Authorized Administrator [FIA_UAU.2, FIA_UID.2] the capability to review Audit data [FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG.] via the TOE CLI and GUI interfaces FAU_SAR.1].
O.DATA_FLOW_CONTROL	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 and GUI webpages), 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 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.DISPLAY_BANNER	The TOE is required to displaying an advisory notice and consent warning message regarding unauthorized use of the TOE. This is met by [FPT_TAB.1]
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all administrative users before granting access and more specifically, 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] before gaining access to the TOE. The password is obscured when entered [FIA_UAU.7].
O.RESIDUAL_INFORMATION_CLEARING	The TOE must ensure no data from previously transmitted data is included in subsequent network traffic [FDP_RIP.1].
O.SELF_PROTECT	The TOE must protect itself against attempts by unauthorized network traffic or unauthorized users to bypass, deactivate or tamper with TOE security functions. [FDP_IFC.1, FDP_IFF.1, FIA_UID.2, FIA_UAU.2, FMT_MSA.1 and FMT_MSA.3] supports this objective by ensuring network traffic flow is controlled and only Authorized Administrator can access and manage the TOE resources. The [FPT_TST.1] meets this objective by performing self-test to ensure the TOE is operating correctly and all functions

Objective	Rationale
	are available and enforced. The [FTP_TRP.1] also meets this objective by ensuring the communication path and the remote administer interfaces is protected and distinct from other communications paths. Lastly, FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG.1 and FPT_STM.1 meet this objective by auditing actions on the TOE. The audit records identify the user associated with the action/event, whether the action/event was successful or failed, the type of action/event, and the date/time the action/event occurred.
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,].
O.TSF_SELF_TEST	The [FPT_TST.1] meets this objective by performing self-test to ensure the TOE is operating correctly and all functions are available and enforced.

8 ANNEX A: REFERENCES

The following documentation 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, dated April 2017
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 5, dated April 2017
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 5, dated April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 5, dated April 2017