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

Security Target

Version 1.0

April 12, 2018

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

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

Table 1 Acronyms

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 for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CSU	Channel Service Unit
DHCP	Dynamic Host Configuration Protocol
DSU	Data Service Unit
EAL	Evaluation Assurance Level
EHWIC	Ethernet High-Speed WIC
ESP	Encapsulating Security Payload
GE	Gigabit Ethernet port
ICMP	Internet Control Message Protocol
ISDN	Integrated Services Digital Network
IT	Information Technology
NDPP	Network Device Protection Profile
OS	Operating System
PBKDF2	Password-Based Key Derivation Function version 2
PoE	Power over Ethernet
POP3	Post Office Protocol
PP	Protection Profile
SA	Security Association
SFP	Security Function Policy
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
SSHv2	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol
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

Table 2 Terminology

Term	Definition
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.
Peer switch	Another switch on the network that the TOE interfaces with.
Privilege level	Assigns a user specific management access to the TOE to run specific commands. For NX-OS privilege levels in IOS can be mapped to the NX-OS user roles. The privilege levels are from 1-15 with 15 having full administrator access to the TOE similar to root access in UNIX or Administrator access on Windows. Privilege level 1 has the most limited access to the CLI. By default when a user logs in to the Cisco NX-OS, they will be in user EXEC mode (level 1). From this mode, the administrator has access to some information about the TOE, such as the status of interfaces, and the administrator can view routes in the routing table. However, the administrator can't make any changes or view the running configuration file. The privilege levels are customizable so that an Authorized Administrator can also assign certain commands to certain privilege levels.
Role	An assigned role gives a user varying access to the management of the TOE. For the purposes of this evaluation the privilege level of a user is synonymous with the assigned privilege level.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
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). 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]

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 2.

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	Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders
ST Version	1.0
Publication Date	April 12, 2018
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders
TOE Hardware Models	9300, 9500, 2000, APIC
TOE Software Version	NX-OS System Software-ACI 12.3(1f), APICv2.3(1f)
Keywords	Switch, Data Protection, Authentication
TOE Guidance	Cisco Nexus 9000 Series Switch Common Criteria Configuration Guide v1.0

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 of 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. 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:

- **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.
- **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.

A remote administrator can securely connect to the APIC over SSHv2 and via a web GUI. The APIC is a hardware appliance with a software-only image that includes an underlying Linux OS that runs on Cisco UCS C-Series hardware. For the purpose of this evaluation the APIC image that includes the Linux OS and UCS server hardware are all included in the TOE.

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, but 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 Cisco APIC is a physically distributed but logically centralized controller that provides DHCP, bootstrap 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 the protocols required. The switch images are installed on the 9k switches in ACI mode.

The Cisco APIC supports zero-touch provisioning: 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 neighboring 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 a router and independently builds a database of the network's topology similar to 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 command-line interface (CLI) and web based graphical interface (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.

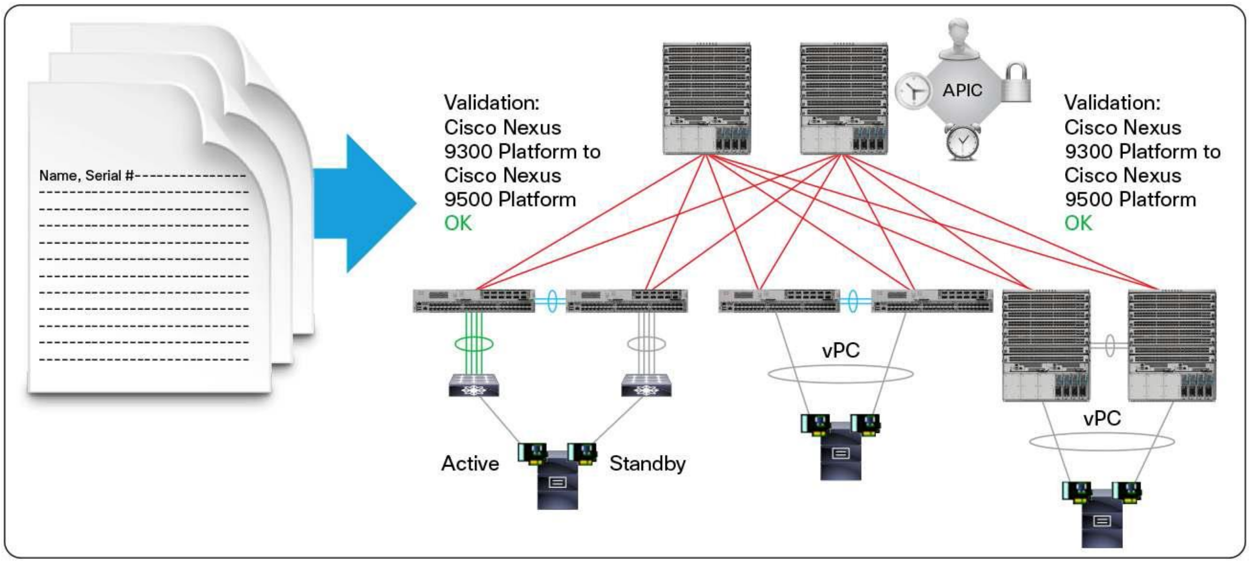


Figure 1 Automatic Provisioning

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 9k TOE component is a data center-class switch for use as an aggregation switch in the data center. They can be deployed in stand alone mode using NX-OS or with the implementation of Application Centric Infrastructure (ACI). In this Common Criteria Evaluation the TOE will be configured in ACI mode.

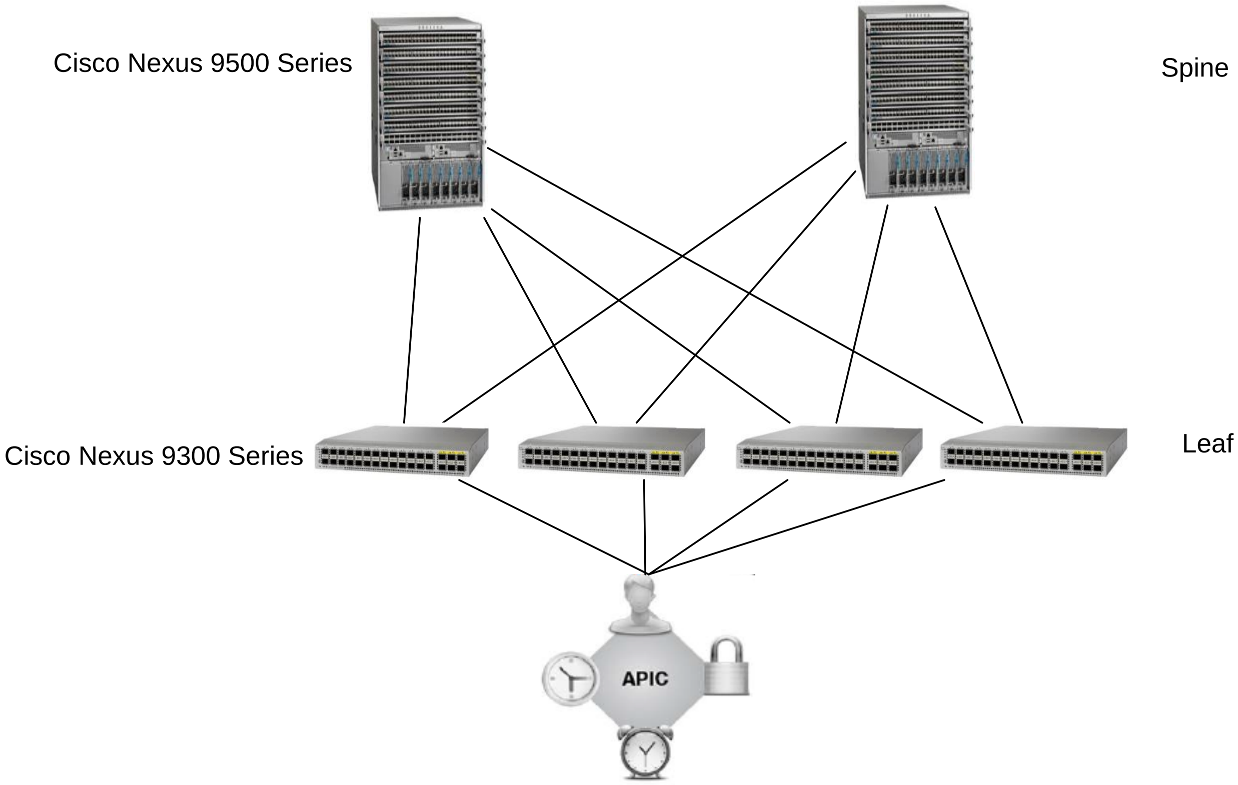


Figure 2 9300 and 9500 typical deployment

The APIC is directly connected to the leaf switches only. The leaf switches are attached to 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. NX-OS 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.

1.2.3 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment when the TOE is configured in its evaluated configuration:

Table 4 IT 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 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	No	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Management Workstation using web browser for HTTPS	Yes	This includes any IT Environment Management workstation with a web browser installed that is used by the TOE administrator to support TOE administration through HTTPS protected channels. Any web browser that supports TLSv1.1 and above with the supported ciphersuites 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.

1.3 TOE DESCRIPTION

This section provides an overview of the Cisco Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders, Target of Evaluation (TOE). The TOE is comprised of both software and hardware. The hardware is comprised of the following model series: 9300, 9500, 2000. The software is comprised of the NX-OS software image and APIC software image Releases: NX-OS System Software-ACI 12.3, APICv2.3.

The Cisco Nexus 9k switches that comprise the TOE have common hardware characteristics. Likewise 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 Specifications

Model	Description	Interfaces
Cisco 9300 models with ACI Support		
9332PQ	QSFP+ 40-Gigabit downlink interface ports. Ports 1 to 12 and 15 to 26 also support 40-Gigabit-to-4x10-Gigabit breakout cables with the Dynamic Breakout feature. QSFP+ 40-Gigabit uplink interface ports (6)	I/O ports as described[1] Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)
9336PQ	36 line-rate QSFP+ ports. 10 and 40 Gigabit Ethernet ports.	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)
N9K-C9372PX-E	Intel Core i3 processor Four 48 x 10/25-Gbps fiber ports and 6 x 40/100-Gbps Quad Small Form-Factor Pluggable 28 (QSFP28) ports	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (1)
9372PX	1- and 10-Gigabit SFP+ interface ports (48) QSFP+ 40-Gigabit interface ports (6)	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)
9372TX	48 1- and 10-Gigabit Ethernet Small Form-Factor 10 Plugable (SFP+) optical ports (supporting 1-Gigabit and 10-Gigabit speeds) QSFP+ 40-Gigabit interface ports (6)	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)
9396PX	4-port 100-Gigabit Ethernet CFP2 optical ports, or 6- or 12-port 40-Gigabit Ethernet Quad Small Form-Factor Plugable (QSFP+) optical ports for connections to other devices 48 1- and 10-Gigabit Ethernet Small Form-Factor 10 Plugable (SFP+) optical ports (supporting 1-Gigabit and 10-Gigabit speeds) to switches or Fabric Extenders (FEXs)	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)
9396TX	4-port 100-Gigabit Ethernet CFP2 optical ports, or 6- or 12-port 40-Gigabit Ethernet Quad Small Form-Factor Plugable (QSFP+) optical ports for connections to other devices 48 10GBASE-T copper ports (supporting 10 100-Megabit, 1-Gigabit, and 10-Gigabit speeds) for connections to other devices	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)
93128TX	Four, six, or 12 40-Gigabit Ethernet Quad Small Form-Factor Plugable (QSFP+) optical ports for uplink connections to aggregation switches	I/O ports as described Management ports: 1 RJ45 connector

Model	Description	Interfaces
	96 10GBASE-T copper ports (supporting speeds 10 of 100 Megabits, 1 Gigabit, and 10 Gigabits) to other devices	Console serial port: 1 RJ45 connector USB ports (2)
C93180LC-EX	Intel Core i3 processor Four 48 x 10/25-Gbps fiber ports and 6 x 40/100-Gbps Quad Small Form-Factor Pluggable 28 (QSFP28) ports	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (1)
93180YC-EX	Intel Core i3 processor Four 48 x 10/25-Gbps fiber ports and 6 x 40/100-Gbps Quad Small Form-Factor Pluggable 28 (QSFP28) ports	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (1)
93108TC-EX	Intel Core i3 processor Four 48 x 10GBASE-T ports and 6 x 40/100-Gbps QSFP28 ports	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (1)
Cisco 9500 models		
9504	Chassis: up to 2 supervisor modules of the same type, 4 I/O modules, and up to 6 fabric modules, 2 system controllers	Based on Supervisor and ACI compatible I/O modules installed. Each line card should be ACI compatible
9508	Chassis: up to 2 supervisor modules of the same type, 8-I/O modules, up to two system controller modules, up to six fabric modules	Based on Supervisor and ACI compatible I/O modules I/O modules installed
9516	Chassis: up to 2 supervisor modules and 16 I/O modules, up to two system controller modules, up to six fabric modules	Based on Supervisor and ACI compatible I/O modules I/O modules installed
Supervisor A	four cores, 1.8 GHz, 16 GB of memory, and 64 GB of SSD (N9K-SUP-A)	Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)
Supervisor B	six cores, 2.1 GHz, 24 GB of memory, and 256 GB of SSD (N9K-SUP-B)	Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)
System Controller	A pair of redundant system controllers offloads chassis management functions from the supervisor modules. The controllers are responsible for managing power supplies and fan trays and are a central point for the Gigabit Ethernet out-of-band channel (EOBC) between the supervisors, fabric modules, and line cards.	Not Applicable
APIC (Medium - Large) and clustered	An APIC appliance comprises either a cluster of Cisco UCS C-Series 220 M4 (second generation appliance) or Cisco UCS C-Series 220 M3 (first generation appliance) servers manufactured with an image secured with Trusted Platform Module (TPM), certificates, and an APIC product ID (PID). The interfaces are the same between the med, large, and clustered APIC its just the processor, hard drive, memory will be larger with more I/O ports for scalability.	Management ports: 2 RJ45 connector Console serial port: 1 RJ45 connector Cisco Integrated Management Controller (CIMC) alternative console port for 1 Gig Ethernet USB ports (2) Virtual Interface Card for optical or 10BaseT
2000 Series Fabric Extenders		
Cisco Nexus	48 100/1000BASE-T host interfaces and 4 10	I/O ports as described

Model	Description	Interfaces
C2248PQ-10GE	Gigabit Ethernet fabric interfaces (SFP+)	
Cisco Nexus 2248TP-E	48 100/1000BASE-T host interfaces and 4 10 Gigabit Ethernet fabric interfaces (SFP+)	I/O ports as described
Cisco Nexus 2248TP-1GE	48 100/1000BASE-T host interfaces and 4 10 Gigabit Ethernet fabric interfaces (SFP+) [32MB Shared Buffer]	I/O ports as described
Cisco Nexus 2232PP-10GE	32 1/10 Gigabit Ethernet and FCoE host interfaces (SFP+) and 8 10 Gigabit Ethernet and FCoE fabric interfaces (SFP+)	I/O ports as described
Cisco Nexus 2232TM-E	32 1/10 G BASE-T host interfaces and 8 10 Gigabit Ethernet (SFP+) Uplink Module (Lower power consumption and improved BER)	I/O ports as described
Cisco Nexus 2348UPQ	48 100M[ĩ]/1/10 Gigabit Ethernet and Unified Port host interfaces (SFP+) and up to 6[ĩ] QSFP+ 10/40 Gigabit Ethernet fabric interfaces.	I/O ports as described
ACI Line Cards		
N9K-X9732C-EX	ACI Ready Spine Line Card: 32p QSFP28 40/100G (32p line rate)	I/O ports as described
N9K-X9736PQ	ACI Ready Spine Line Card: 36p QSFP 40G (36p line rate)	I/O ports as described

1.4 TOE Evaluated Configuration

The TOE consists of one or more switches as specified in section 1.5 below and includes the Cisco NX-OS software. The TOE has two or more network interfaces and is connected to an ACI fabric with APIC 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)

All supported modules for the 9300, 9500, 2000 series are considered part of the TOE evaluated configuration. The TOE can optionally connect to an NTP server on its internal network for time services.

The TOE is remotely administered via the APIC over a secure SSHv2 session using the CLI or TLSv1.2 using the APIC GUI. The APIC controller is using direct fiber to connect to the leaf switch. When the 9k is configured for use in the ACI mode (ie. not standalone), a web browser using TLS is used for remote login to the APIC for management of the 9k switch. On the APIC there are RBAC and AAA policies to validate user access control. 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 an authorized administrator configures in-band or out-of-band management access, then an endpoint group (EPG) and a contract have to be configured in order to apply a whitelist firewall filter. Audit records are stored locally, but may be remotely 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.

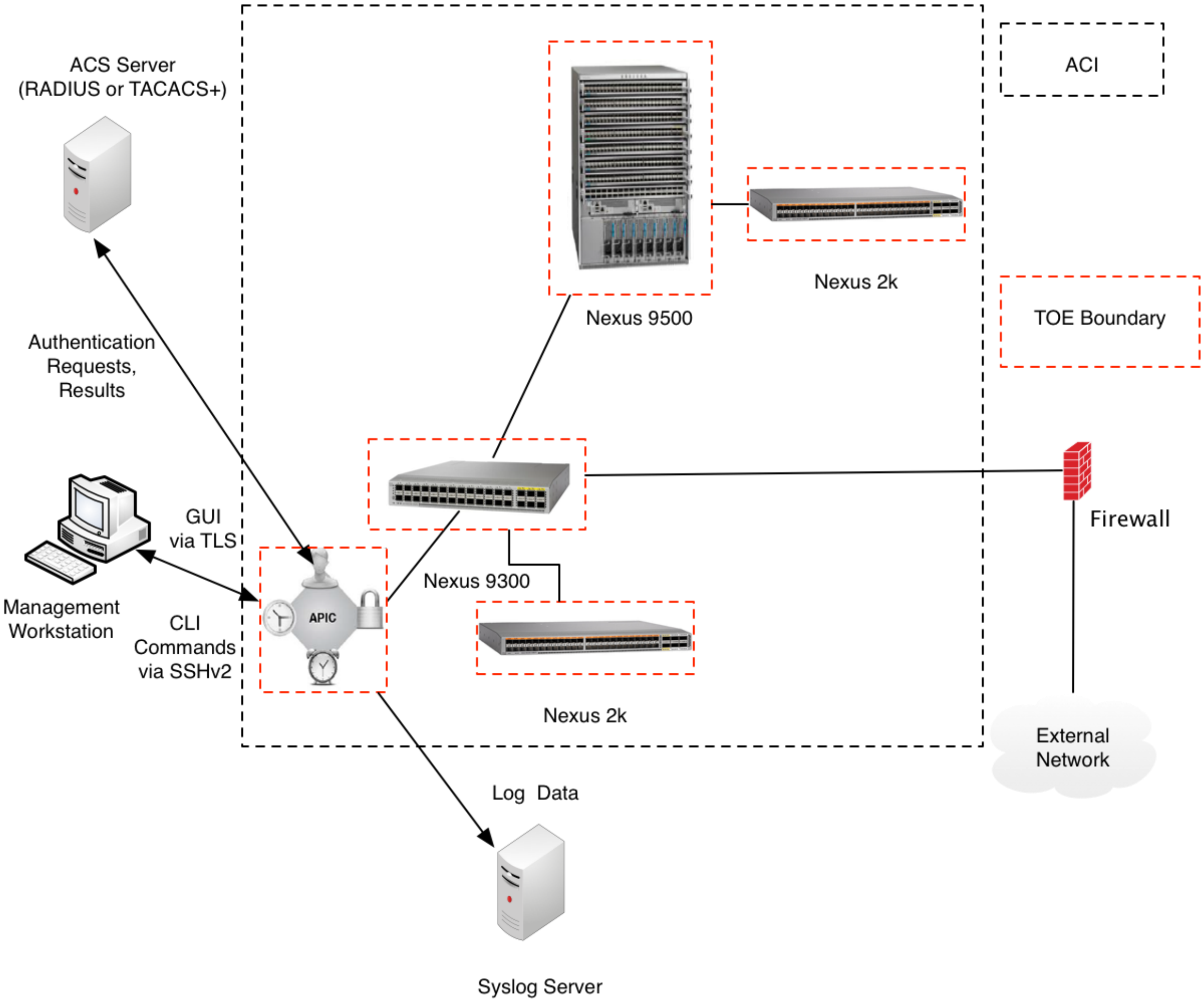


Figure 3 TOE and Environment

1.5 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, and APIC running on UCS C-Series. The network on which they reside is considered part of the environment. The TOE guidance documentation that is considered to be part of the TOE can be found listed in the Cisco Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders documentation is downloadable from the web sites:

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

The TOE is comprised of the following physical specifications as described in Table 5 in section 1.3 above. Deployment of the Nexus 2000 is optional for additional ports and cable management purposes.

1.6 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.

1. Security Audit
2. Cryptographic Support
3. Full Residual Information Protection
4. Information Flow Control
5. Identification and Authentication
6. Security Management
7. Protection of the TSF
8. TOE Access
9. Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs described within the security functional requirements as necessary to satisfy testing/assurance measures prescribed therein.

1.6.1 Security Audit

The Cisco Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, enforcement of information flow control policies and administrative actions. The Cisco Nexus 9000 Switch in ACI mode and APIC generate an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The authorized administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE provides the administrator with a circular audit trail. Logs are written to an internal database.

1.6.2 Cryptographic Support

The TOE provides cryptography in support of other Cisco 9k security functionality. This cryptography has been validated for conformance to the requirements of FIPS 140-2 Level 2 (see Table 6 for certificate references).

Table 6 FIPS References

Algorithm	Supported Mode	Cert. #
Nexus 9000 Series Switch with ACI mode and APIC TOE Components		
AES	CBC, CTR, GCM (128, 192, 256)	3404, 3405, 5267
DSA	1024, 2048, 3072 bits	961, 962
ECDSA	P-256 P-384 P-521	678, 679
SHA-1, SHA-256, SHA-512	Byte Oriented	2817, 2818
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	Byte Oriented	2172, 2173
RSA	1024, 2048, 3072 bits	1743, 1744

The TOE provides cryptography in support of remote administrative management via TLS and SSHv2. The cryptographic services provided by the TOE are described in Table 7 below.

Table 7 TOE Provided Cryptography

Cryptographic Method	Use within the TOE
Secure Shell Establishment	Used to establish initial SSH session
Transport Layer Security (TLS)	Used in TLS session establishment
RSA/DSA Signature Services	Used in SSH session establishment Used in TLS session establishment
SHA-1, SHA-256, SHA-512	Used to provide SSH traffic integrity verification Used to provide TLS traffic integrity verification Password hashing
AES CBC, GCM, and CTR (128, 192, 256)	Used to encrypt SSH session traffic Used to encrypt TLS session traffic
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	Used for keyed hash, integrity services in SSH and TLS session establishment

1.6.3 Full Residual Information Protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Packets are padded with zeros. Residual data is never transmitted from the TOE.

1.6.4 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. 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. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the local serial port referred to as the management port on the Nexus switches. In addition, password-based authentication can be performed when connecting to the TOE CLIs remotely using SSHv2. The SSHv2 interface also supports authentication using SSH keys. The TOE supports use of a RADIUS or TACACS+ AAA server (part of the IT Environment) to facilitate authentication (including single-use authentication, or password-based authentication) and authorization (roles) for administrative users attempting to connect to the TOE's GUI and CLI. When the role is defined through the management interface on the TOE, it is sent to the RADIUS server using Vendor Specific Attributes (VSA). Password based authentication is used for authenticating to the APIC using a browser to access the web based GUI secured by TLS.

1.6.5 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 access control list that is applied to Layer 3 traffic that is routed into or out Nexus 9000 Series switch. A PACL is an administratively configured access control list that is applied to Layer 2 traffic that is routed into Nexus 9000 Series switch. A VACL is an administratively configured access control list that is applied to packets that are routed into or out of a VLAN or are bridged within a VLAN. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces.

RACLs can filter traffic based on the following: Source IP address, Destination IP address, Source port number, Destination port number, Protocol, ICMP message type, ICMP message code, IGMP message type, Precedence, Packet Length, or DSCP value.

PACLs can filter ingress traffic based on the following: Source IP address, Destination IP address, Source port number, Destination port number, Protocol, ICMP message type, ICMP message code, IGMP message type, Protocol, Class of Service (COS), VLAN ID, Precedence, Packet Length, or DSCP value.

Traffic into or out of a VLAN can be filtered by VACLs based on the following: Source IP address, Destination IP address, Source port number, Destination port number, Protocol, ICMP message type, ICMP message code, IGMP message type, Protocol, Class of Service (COS), VLAN ID, Precedence, Packet Length, or DSCP value.

The TOE supports Virtual Routing and Forwarding (VRF). VRFs allow multiple instances of routing tables to exist within the Nexus 9000 Series switch TOE component simultaneously. This increases functionality by allowing network paths to be segmented without using multiple devices. Each VRF instance uses a single routing table. These tables prevent traffic from being forwarded outside a specific VRF path and also keep out traffic that should remain outside the VRF path.

1.6.6 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 a secure SSHv2 session or via a local console connection. In addition, the web based GUI can be used for TOE administration using TLS. The TOE provides the ability to securely manage:

- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- Information Flow Control Policies and Rules;
- The timestamps maintained by the TOE;
- Update to the TOE; and
- TOE configuration file storage and retrieval.

Unlike Cisco IOS devices, which use privilege levels to determine authorization, Cisco NX-OS in ACI mode and APIC devices use role-based access control (RBAC). To enable both types of devices to be administered by the same TACACS+ servers, an authorized administrator can map the privilege levels configured on TACACS+ servers to user roles configured on Cisco NX-OS devices.

The Nexus 9k in ACI mode has preconfigured roles as defined in FMT_SMR.1 and has customized roles that can be created.

For the 9k with ACI, the APIC controls the management of the devices within the ACI fabric. All administrators are considered to be security administrators in this ST. Administrators can create configurable login banners to be displayed at time of login. The 9k has a CLI that can be administered either remotely using SSHv2 or locally via a console that is directly connected via a serial cable. In addition, the web based GUI can be used for TOE administration using TLS.

1.6.7 Protection of the TSF

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

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

Use of separate VLANs is used to ensure routing protocol communications between the TOE and neighbor switches including routing table updates and neighbor switch authentication will be logically isolated from traffic on other VLANs.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually, or 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 and that of the cryptographic module.

1.6.8 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.

1.6.9 Trusted path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 for remote CLI access and TLS using a browser for connection to the web based GUI on the APIC.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 8 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.
Telnet	Telnet will be disabled in the evaluated configuration.
SNMP	SNMP will be disabled in the evaluated configuration.

These functions will be disabled by configuration.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 4, dated: September 2012. For a listing of Assurance Requirements claimed see section 5.6.1. The TOE and ST are EAL2 conformant as well as CC Part 2 extended and CC Part 3 conformant.

2.2 Protection Profile Conformance

This ST and TOE it describes is not claiming conformance to any Protection Profile.

3 SECURITY PROBLEM DEFINITION

This chapter identifies the following:

- ♦ Significant assumptions about the TOE's operational environment.
- ♦ IT related threats to the organization countered by the TOE.
- ♦ 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. Organizational Security Policies (OSPs) are identified as P.osp with "osp" specifying a unique name.

3.1 Assumptions

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

Table 9 TOE Assumptions

Assumption	Assumption Definition
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.FIREWALL	A firewall located between the ACI fabric and external networks to protect against malicious or unauthorized traffic from entering the ACI fabric.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment. The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation.
A.REMOTE_SERVERS	When remote servers are used, such as NTP server and optionally remote authentication servers and syslog servers, the administrator will ensure the session between the TOE and remote server(s) is secured.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

3.2 Threats

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

Table 10 Threats

Threat	Threat Definition
T.NET_TRAFFIC	An attacker may send network traffic to unauthorized destinations through the Nexus 9000 Series switch without detection compromising TOE information flow control policies.

Threat	Threat Definition
T.TSF_FAILURE	An attacker succeeds in triggering an undetected change in the TOE start-up procedure or configuration to cause starting up of the TOE into an insecure state resulting in the loss of integrity of the TSF exposing TOE data to the attacker.
T.UNAUTHORIZED_ACCESS	An attacker succeeds in gaining access to the TOE or to legitimate administrator authentication data communicated between the TOE and a Management Station by successfully masquerading as an authorized administrator or legitimate TOE in order to gain unauthorized access to data or TOE resources.
T.UNDETECTED_ACTIONS	Malicious attackers may take actions that adversely affect the security of the TOE exposing sensitive data. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.USER_DATA_REUSE	An attacker may disrupt the TOE causing user data to 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 11 Organizational 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 accessing the TOE.

4 SECURITY OBJECTIVES

This Chapter 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 12 Security Objectives for the TOE

TOE Objective	TOE Security Objective Definition
O.DATA_FLOW_CONTROL	The TOE shall ensure that only authorized traffic is permitted to flow through the TOE to its destination via the application profile.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators and authorized IT entities.
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.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only trusted administrators are able to log in and configure the TOE.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its 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 13 Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of 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.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment. The Nexus 9k APIC and routers are intended to be deployed in the same physically protected datacenter. The ACI fabric is intended to support datacenter servers and devices, not have end users directly attach into the fabric.
OE.REMOTE_SERVERS	The operational environment of the TOE shall provide NTP server and optionally remote authentication servers and syslog servers, and the administrator will ensure the session between the TOE and remote server(s) is secured.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

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 4, dated: September 2012* and all international interpretations.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs have been organized by class. Table 14 identifies all extended SFRs implemented by the TOE.

Table 14 Extended TOE Security Functional Requirements

Name	Description
FCS_SSH_EXT.1	SSH
FCS_TLS_EXT.1	TLS
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
FIA_UAU_EXT.2	Extended: Password-based Authentication Mechanism
FPT_APW_EXT.1	Extended: Protection of Administrator Passwords
FPT_TST_EXT.1	TSF Testing

5.1.1 Cryptographic Support (FCS)

5.1.1.1 FCS_SSH_EXT.1 SSH

Family Behavior

The component in this family addresses the ability for a server to offer SSH to protect data between a client and the server using the SSH protocol.

Component leveling

FCS_SSH_EXT SSH Server Protocol
1

FCS_SSH_EXT.1 SSH Server requires that the server side of SSH be implemented as specified.

Management: FCS_SSH_EXT.1

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

a) There are no management activities foreseen.

Audit: FCS_SSH_EXT.1

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

a) Failure of SSH session establishment.
b) SSH session establishment
c) SSH session termination

FCS_SSH_EXT.1	**SSH Server Protocol**

Hierarchical to: No other components
Dependencies: FCS_COP.1 Cryptographic operation

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3 The TSF shall ensure that the SSH transport implementation supports the following encryption algorithms: AES-CTR-128, AES-CTR-256.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses SSH_RSA and [selection: PGP-SIGN-RSA, PGP-SIGN-DSS, no other public key algorithms,] as its public key algorithm(s).

FCS_SSH_EXT.1.5 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [selection*:* hmac-sha1, hmac-sha1-96, hmac-md5, hmac-md5-96].

5.1.1.2 FCS_TLS_EXT.1 TLS

Family Behavior

The component in this family addresses the ability for a server to offer TLS to protect data between a client and the server using the TLS protocol.

Component leveling

FCS_TLS_EXT.1 TLS Server requires that the server side of TLS be implemented as specified.

Management: FCS_TLS_EXT.1

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

b) There are no management activities foreseen.

Audit: FCS_TLS_EXT.1

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

a) TLS session establishment
b) TLS session termination

FCS_TLS_EXT.1	TLS Server Protocol

Hierarchical to: No other components
Dependencies: FCS_COP.1 Cryptographic operation

FCS_TLS_EXT.1 TLS

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: TLS1.1, TLS1.2].

5.1.2 Identification and authentication (FIA)

5.1.2.1 FIA_PMG_EXT.1 Password Management

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

Component leveling

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

Management: FIA_PMG_EXT.1

No management functions.

Audit: FIA_PMG_EXT.1

No specific audit requirements.

FIA_PMG_EXT.1	Password Management

Hierarchical to: No other components.
Dependencies: No other components.

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

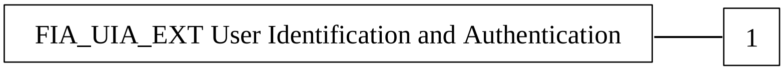
1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”].

5.1.2.2 FIA_UIA_EXT.1 User Identification and Authentication

Family Behavior

The TSF allows certain specified actions before the non-TOE entity goes through the identification and authentication process.

Component leveling



FIA_UIA_EXT.1 User Identification and Authentication requires administrators (including remote administrators) to be identified and authenticated by the TOE, providing assurance for that end of the communication path. It also ensures that every user is identified and authenticated before the TOE performs any mediated functions

Management: FIA_UIA_EXT.1
The following actions could be considered for the management functions in FMT:

a) Ability to configure the list of TOE services available before an entity is identified and authenticated

Audit: FIA_UIA_EXT.1

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

a) All use of the identification and authentication mechanism
b) Provided user identity, origin of the attempt (e.g. IP address)

FIA_UIA_EXT.1	User Identification and Authentication

Hierarchical to: No other components.
Dependencies: FTA_TAB.1 Default TOE Access Banners

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [selection: no other services. [assignment: *list of services, actions performed by the TSF in response to unauthenticated non-TOE requests.*]]

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

5.1.2.3 FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

Family Behavior

Provides for a locally based administrative user authentication mechanism

Component leveling

FIA_UAU_EXT.2 The password-based authentication mechanism provides administrative users a locally based authentication mechanism.

Management: FIA_UAU_EXT.2

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

a) None

Audit: FIA_UAU_EXT.2

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

a) Minimal: All use of the authentication mechanism

FIA_UAU_EXT.2	**Password-based Authentication Mechanism**
Hierarchical to:	No other components.
Dependencies:	None

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [selection: [assignment: *other authentication mechanism(s)*], none] to perform administrative user authentication.

5.1.3 Protection of Administrator Passwords (FPT_APW_EXT)

5.1.3.1 FPT_APW_EXT.1 Protection of Administrator Passwords

Family Behavior

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

Component leveling

FPT_APW_EXT Protection of Administrator Passwords
1

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

Management: FPT_APW_EXT.1

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

a) No management functions.

Audit: FPT_APW_EXT.1

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

a) No audit necessary.

FPT_APW_EXT.1	**Protection of Administrator Passwords**

Hierarchical to: No other components
Dependencies: No other components.

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

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

5.1.3.2 FPT_TST_EXT.1: TSF Testing

Family Behavior
Components in this family address the requirements for self-testing the TSF for selected correct operation.

Component leveling

FPT_TST_EXT.1 TSF Self-test requires a suite of self-tests to be run during initial start-up in order to demonstrate correct operation of the TSF.

Management: FPT_TST_EXT.1
The following actions could be considered for the management functions in FMT:

a) No management functions.

Audit: FPT_TST_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Indication that TSF self-test was completed

FPT_TST_EXT.1	**TSF testing**
Hierarchical to:	No other components.
Dependencies:	None

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

5.2 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: Indicated with [*italicized*] text within brackets;
- Assignment within a selection: Indicated with [*italicized underlined*] text within brackets;
- Refinement: Indicated with **bold** text and/or strikethroughs;
- Selection: Indicated with [underlined] text within brackets;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs.

5.3 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 15 Security Functional Requirements

Class Name	Component Identification	Component Name
FAU: Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User Identity Association
	FAU_STG.1	Protected Audit Trail Storage
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.4	Cryptographic Key Zeroization
	FCS_COP.1	Cryptographic Operation
	FCS_SSH_EXT.1	SSH
	FCS_TLS_EXT.1	TLS
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_PMG_EXT.1	Password Management
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UID.2	User identification before any action
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UAU.7	Protected authentication feedback
FMT: Security management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	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_APW_EXT.1	Extended: Protection of Administrator Passwords
	FPT_STM.1	Reliable Time Stamps
	FPT_TST_EXT.1	TSF Testing
FTA: TOE Access	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_TRP.1	Trusted Path

5.4 SFRs

5.4.1 Security audit (FAU)

5.4.1.1 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; and
c) [

- *When a packet matches a configured Contract via a whitelist EPG to EPG;*
- *Configuration Changes on the APIC;*
- *Administrative Authentication on the APIC;*
- *Administrative Log-off on the APIC*].

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 (if applicable), 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 column two of Table 16*].

Table 16 Auditable Events

Audited Action	Recorded Information
When a deny packet matches a configured Contract via a whitelist EPG to EPG is logged.	*Protocol* *Type* *Source address* *Destination address* *Source Port (if applicable)* *Destination Port (if applicable)*
Configuration Changes on the Nexus 9000 Series switch and via APIC	*Day of Week, Date, Action, User, status of the configuration change, terminal information (when applicable)*
Administrative Authentication on the Nexus 9000 Series switch and APIC	*Day of Week, Date, Action, User, terminal information (when applicable)*
Administrative Log-off on the Nexus 9000 Series switch and APIC	*Day of Week, Date, Action, User, terminal information (when applicable)*

5.4.1.2 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.

5.4.1.3 FAU_STG.1 Protected Audit Trail Storage

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

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

5.4.2 Cryptographic Support (FCS)

5.4.2.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*see first column in Table 17 below*] and specified cryptographic key sizes [*see "key sizes" column in Table 17 below*] that meet the following: [*see last column in Table 17 below*].

Table 17 Cryptographic Key Generation

Cryptographic key generation algorithm	Key sizes	List of standards
AES (CBC, CTR, GCM)	*128 bits* *192 bits* *256 bits*	*FIPS 140-2, FIPS PUB 197, NIST SP 800-38A, NIST SP 800-38D*

Cryptographic key generation algorithm	Key sizes	List of standards
ECDSA	*P-192* *P-256* *P-384* *P-521*	*FIPS 140-2*
DSA	*1024-bits* *2048-bits*	*FIPS 140-2,* *FIPS PUB 186-3, "Digital Signature Standard"*
RSA	*1024,* *2048 bits*	*FIPS 140-2*
Diffie-Hellman Group 14	*2048 bits*	*FIPS 140-2*
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	*128 bits* *160 bits* *256 bits* *384 bits* *512 bits*	*FIPS 140-2, FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard"*
SHA-1, SHA-256. SHA-512	*160 bits* *256 bits* *512 bits*	*FIPS 140-2,* *FIPS PUB 186-3, "Digital Signature Standard"*

5.4.2.2 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2 requirements stated in Annex A Table 30*].

5.4.2.3 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [*See "cryptographic operations" in Table 18*] in accordance with a specified cryptographic algorithm [*See "algorithm" in Table 18*] and cryptographic key sizes [*See "key size" in Table 18*] that meet the following: [*See "list of standards" in Table 18*].

Table 18 Cryptographic Operations

Cryptographic Operation	Algorithm	Key Size	List of Standards
Encryption/Decryption	*AES (CBC, CTR, GCM)*	*128 bits* *192 bits* *256 bits*	*FIPS 140-2, FIPS PUB 197, NIST SP 800-38A, NIST SP 800-38D*
Cryptographic signature	*DSA*	*1024-bits* *2048-bits* *3072-bits*	*FIPS 140-2,* *FIPS PUB 186-3, "Digital Signature Standard"*
Cryptographic signature	*ECDSA*	*P-256* *P-384* *P-521*	*FIPS 140-2,* *FIPS PUB 186-3, "Digital Signature Standard"*
Cryptographic signature and key transport	*RSA (rDSA)*	*1024-bits* *2048-bits* *3072-bits*	*FIPS 140-2, FIPS PUB 186-2 or FIPS PUB 186-3, "Digital Signature Standard"*
Cryptographic Hashing Services	*SHA-1, SHA-256, SHA-512*	*160 bits* *256 bits* *512 bits*	*FIPS 140-2, FIPS PUB 186-3, "Digital Signature Standard"*
Keyed-hash message	*HMAC-SHA-1, HMAC-*	*128 bits*	*FIPS 140-2, FIPS Pub 198-1, "The Keyed-*

Cryptographic Operation	Algorithm	Key Size	List of Standards
authentication	*SHA-256, HMAC-SHA-384, HMAC-SHA-512*	*160 bits* *256 bits* *384 bits* *512 bits*	*Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard"*

5.4.2.4 FCS_SSH_EXT.1 SSH

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254.

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3 The TSF shall ensure that the SSH transport implementation supports the following encryption algorithms: AES-CTR-128, AES-CTR-256.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses SSH_RSA and [no other public key algorithms] as its public key algorithm(s).

FCS_SSH_EXT.1.5 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [hmac-sha1].

5.4.2.1 FCS_TLS_EXT.1 TLS

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [TLS1.1, TLS1.2].

5.4.3 User data protection (FDP)

5.4.3.1 FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [*Virtual and Distributed Switch Information Flow Control SFP*] on [
Subject:
a) *physical and virtual network interfaces*
Information:
b) *network packets*
c) *operations: permit/deny/redirect/deny-and-log layer two and layer three communications*.]

5.4.3.2 FDP_IFF.1 Simple security attributes

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

- *Subjects: physical network interfaces and virtual network interfaces*
- *Subject security attributes: interface identifier (within EPG), VxLAN identifier (if applicable), tenant (VRF) identifier (if applicable)*
- *Information: network packets*
- *Information security attributes: IP address source identifier, IP address destination identifier, protocol, packet length, Precedence, DSCP Value, DHCP Server and interfaces configured as trusted*].

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 configured access control lists permit the information flow based on a combination of subject security attributes and information security attributes, 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 when the IP address of the 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; or*
- *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*].

5.4.3.3 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 [<u>deallocation of the resource from</u>] all objects.

5.4.4 Identification and authentication (FIA)

5.4.4.1 FIA_PMG_EXT.1 Password Management

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

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

5.4.4.2 FIA_UIA_EXT.1 User Identification and Authentication

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [no other services.]

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

5.4.4.3 FIA_UID.2 User identification before any action

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

5.4.4.4 FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [*remote password-based authentication via RADIUS or TACACS+*] to perform administrative user authentication.

5.4.4.5 FIA_UAU.7: Protected authentication feedback

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

5.4.5 Security Management (FMT)

5.4.5.1 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [*TSF Management SFP*] to restrict the ability to [[read, write]] the security attributes [*defined within administratively configured ACLs policy rules and Traffic Storm Inspection policies as described in* Table 19] to [*the roles/operations defined in Table 19 below*].

Table 19: TSF Management SFP

Role	Operations
aaa	*Used for configuring authentication, authorization, accounting, and import/export policies.*
admin	*read, write operations for all security attributes defined within administratively configured ACLs policy rules and Traffic Storm Inspection.* *read, write operations for all security attributes defined within administratively configured ACLs policy rules Traffic Storm Inspection policies. .*
access-admin	*Layer 1, Layer 2, Layer 3 configuration under infra. Fabric wide policies for NTP, SNMP, DNS, and image management. Management infra policies*
fabric-admin	*Layer 1, Layer 2, Layer 3 configuration under fabric. Fabric wide policies for NTP, SNMP, DNS, and image management. Management fabric policies*
nw-svc-admin	*managing Layer 4 to Layer 7 service devices, shared service devices, orchestration*
nw-svc-params	*managing Layer 4 to Layer 7 service policies.*
ops	*Used for operational policies including monitoring and troubleshooting policies such as atomic counter, SPAN, TSW, tech support, traceroute, analytics, and core policies.*
read-all	*Read only for infra and fabric policies and ops*
tenant-admin	*Layer 1, Layer 2, Layer 3 configuration under infra and fabric. Fabric wide policies for NTP, SNMP, DNS, and image management. Management infra and fabric policies for their assigned tenant*
tenant-ext-admin	*Used for managing network policies that affect the external to the tenant network. Layer 1, 2, and 3 protocols such as Used for managing tenant external Layer 3 protocols such as BGP, OSPF, PIM, and IGMP*
vmm-admin	*Read all objects in APIC's VMM and managing VMM policies.*
Administrator defined role(s)	*read, write operations consistent with the role definitions.*

5.4.5.2 FMT_MSA.3 Static attribute initialisation

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

FMT_MSA.3.2 The TSF shall allow the [*no role*] to specify alternative initial values to override the default values when an object or information is created.

5.4.5.3 FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [[*read, write*]] the [*TSF Data described in the table below*] to [*the roles identified in the table below*].

Table 20: Roles and operations on TSF Data

Role	Operation	TSF Data
aaa	*Read, Write*	*Configuring authentication, authorization, accounting, and import/export policies.*
admin	*Read, Write*	*full access to all configuration data*
access-admin	*Read, Write*	*Layer 1, Layer 2, Layer 3 configuration under infra. Fabric wide policies for NTP, SNMP, DNS, and image management. Management infra policies*
fabric-admin	*Read, Write*	*Layer 1, Layer 2, Layer 3 configuration under fabric. Fabric wide policies for NTP, SNMP, DNS, and image management. Management fabric policies*
nw-svc-admin	*Read, Write*	*Managing Layer 4 to Layer 7 service devices, shared service devices, orchestration*
nw-svc-params	*Read, Write*	*Managing Layer 4 to Layer 7 service policies.*
ops	*Read, Write*	*Operational policies including monitoring and troubleshooting policies such as atomic counter, SPAN, TSW, tech support, traceroute, analytics, and core policies.*
read-all	*Read only*	*Infra and fabric policies and ops*
tenant-admin	*Read, Write*	*Layer 1, Layer 2, Layer 3 configuration under infra and fabric. Fabric wide policies for NTP, SNMP, DNS, and image management. Management infra and fabric policies for their assigned tenant*
tenant-ext-admin	*Read, Write*	*Used for managing network policies that affect the external to the tenant network. Layer 1, 2, and 3 protocols such as Used for managing tenant external Layer 3 protocols such as BGP, OSPF, PIM, and IGMP*
vmm-admin	*Read, Write*	*Read all objects in APIC's VMM and managing VMM policies.*
Administrator defined role(s)	*Read, Write*	*Operations consistent with the role definitions.*

5.4.5.4 FMT_SMF.1 Specification of Management Functions

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

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;*
- *Ability to configure the cryptographic functionality*.]

5.4.5.5 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [*aaa, admin, access-admin, fabric-admin, nw-svc-admin, nw-svc-params, ops, read-all, tenant-admin, tenant-ext-admin, vmm-admin, Administrator defined role(s).*]

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

5.4.6 Protection of the TSF (FPT)

5.4.6.1 FPT_APW_EXT.1 Extended: Protection of Administrator Passwords

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

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

5.4.6.2 FPT_STM.1 Reliable time stamps

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

5.4.6.3 FPT_TST_EXT.1: TSF Testing

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

5.4.7 TOE Access (FTA)

5.4.7.1 FTA_SSL.4 User-initiated Termination

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

5.4.7.2 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.

5.4.8 Trusted Path/Channels (FTP)

5.4.8.1 FTP_TRP.1 Trusted Path

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

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [[*all remote administrative actions*]].

5.5 TOE SFR Hierarchies and Dependencies

This section of the Security Target demonstrates that the identified TOE and IT 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.

Not applicable in the Rationale column means the Security Functional Requirement has no dependencies and therefore, no dependency rationale is required. Satisfied in the Rationale column means the Security Functional Requirements dependency was included in the ST.

Table 21: TOE Security Functional Requirements Dependency Rationale

SFR	Dependencies	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_STG.1	FAU_GEN.1	Met by FAU_GEN.1
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1]	Met by FCS_COP.1
	FCS_CKM.4	Met by FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Met by FCS_CKM.1
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Met by FCS_CKM.1
	FCS_CKM.4	Met by FCS_CKM.4
FCS_SSH_EXT.1	FCS_COP.1	Met by FCS_COP.1
FCS_TLS_EXT.1	FCS_COP.1	Met by FCS_COP.1
FDP_IFC.1	FDP_IFF.1	Met by FDP_IFF.1
FDP_IFF.1	[FDP_IFC.1 or FDP_IFC.1] FMT_MSA.3	Met by FDP_IFC.1 and FMT_MSA.3
FDP_RIP.2	No Dependencies	Not applicable.
FIA_PMG_EXT.1	No Dependencies	Not applicable.
FIA_UIA_EXT.1	FTA_TAB.1	Met by FTA_TAB.1
FIA_UID.2	No Dependencies	Not applicable.
FIA_UAU_EXT.2	No Dependencies	Not applicable.
FIA_UAU.7	FIA_UAU.1	Met by FIA_UAU_EXT.2 FIA_UAU_EXT.2 is modeled after FIA_UAU.2 which is hierarchical to FIA_UAU.1 and therefore meets the

SFR	Dependencies	Rationale
		dependency.
FMT_MSA.1	[FDP_ACC.1, or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	Not applicable as the TSF Management SFP is defined in Table 19 instead of in a separate SFR. Met by FMT_SMR.1 Met by FMT_SMF.1
FMT_MSA.3	FMT_MSA.1	Met by FMT_MSA.1
	FMT_SMR.1	Met by FMT_SMR.1
FMT_MTD.1	FMT_SMF.1	Met by FMT_SMF.1
	FMT_SMR.1	Met by FMT_SMR.1
FMT_SMF.1	No Dependencies	Not applicable.
FMT_SMR.1	FIA_UID.1	Met by FIA_UID.2
FPT_APW_EXT.1	No Dependencies	Not applicable.
FPT_STM.1	No Dependencies	Not applicable.
FPT_TST_EXT.1	No Dependencies	Not applicable.
FTA_SSL.4	No Dependencies	Not applicable.
FTA_TAB.1	No Dependencies	Not applicable.
FTP_TRP.1	No Dependencies	Not applicable.

5.6 Extended TOE Security Functional Components Definition

This Security Target includes Security Functional Requirements (SFR) that are not drawn from existing CC Part 2. The Extended SFRs are identified by having a label '_EXT' after the requirement name for TOE SFRs. The structure of the extended SFRs is modeled after the SFRs included in CC Part 2. The structure is as follows:

A. Class – The extended SFRs included in this ST are part of the identified classes of requirements.

B. Family – The extended SFRs included in this ST are part of several SFR families

C. Component – The extended SFRs are not hierarchical to any other components, though they may have identifiers terminating on other than "1". The dependencies for each extended component are identified in the TOE SFR Dependencies section of this ST below.

D. The management requirements, if any, associated with the extended SFRs are incorporated into the Security management SFRs defined in this ST.

E. The audit requirements, if any, associated with the extended SFRs are incorporated into the Security audit SFRs defined in this ST.

F. The dependency requirements, if any, associated with the extended SFRs are identified in the dependency rationale and mapping section of the ST (Table 21).

Table 22 Extended Components Rationale

Component	Rationale
FCS_SSH_EXT.1	This SFR was modeled from the NDPP – where it is defined as a requirement specific to SSH protocol supported by the TOE. The SSH protocol is used to secure communications between the TOE and the endpoints; mainly remote administration. Securing the communication channel provides interoperability and resistance to cryptographic attack by means of two-way authentication of each endpoint. Compliance to the NDPP is not being claimed and the SFR has been adapted in this ST to support the TOE's implementation of the protocol as well as the specifics detailed in the NDPP. Given that this is a validated US Government Protection Profile the rationale for use of this extended requirement is deemed acceptable.
FCS_TLS_EXT.1	This SFR was modeled from the NDPP – where it is defined as a requirement specific to the TLS protocol supported by the TOE. The TLS protocol is used to secure communications between the TOE and the endpoints; mainly remote administration using the GUI. Securing the communication channel provides interoperability and resistance to cryptographic attack by means of two-way authentication of each endpoint. Compliance to the NDPP is not being claimed and the SFR has been adapted in this ST to support the TOE's implementation of the protocol as well as the specifics detailed in the NDPP. Given that this is a validated US Government Protection Profile the rationale for use of this extended requirement is deemed acceptable.
FIA_PMG_EXT.1	This SFR was modeled from the NDPP – where it is defined as a requirement for TSF password complexity rules for TOE administrators. FIA_PMG_EXT.1 was used to distinguish that the password quality parameters are required for *administrator* passwords and not *user* passwords. The FIA_SOS.1 SFR in the CC Part 2 does not distinguish between administrator and user password quality parameters. In addition, this extended SFR provides for password management capabilities of administrative passwords that the CC Part 2 SFR does not provide. Compliance to the NDPP is not being claimed and the SFR has been adapted in this ST to support the TOE's authentication security functionality. Given this is a validated US Government Protection Profile the rationale for use of this extended requirement is deemed acceptable.
FIA_UIA_EXT.1	This SFR was modeled from the NDPP – where it is defined as a requirement for TSF actions allowed prior to identification and authentication of an authorized administrator. Compliance to the NDPP is not being claimed and the SFR has been adapted in this ST to support the TOE's identification and authentication security functionality. Given this is from a validated US Government Protection Profile the rationale for use of this extended requirement is deemed acceptable.
FIA_UAU_EXT.2	This SFR was modeled from the NDPP – where it is defined as a requirement for TSF user authentication. Compliance to the NDPP is not being claimed and the SFR has been adapted in this ST to support the TOE's authentication security functionality. Given this is from a validated US Government Protection Profile the rationale for use of this extended requirement is deemed acceptable.
FPT_APW_EXT.1	This SFR was modeled from NDPP – where it is defined as a requirement for the TSF to not store passwords in plaintext. Compliance to the NDPP is not being claimed and the SFR has been adapted in this ST to support the TOE's authentication security functionality. Given this is a validated US Government Protection Profile the rationale for use of this extended requirement is deemed acceptable.
FPT_TST_EXT.1	This SFR was modeled from NDPP – where it is defined as a requirement for TSF self-tests of the TOE during initialization (on bootup) that allows for the detection of failures of the underlying security mechanisms prior to the TOE becoming operational. Compliance to the NDPP is not being claimed and the SFR has been adapted in this ST to support the TOE's comprehensive set of self-tests. Given this is from a validated US Government Protection Profile the rationale for use of this extended requirement is deemed acceptable.

5.6.1 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. 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.

5.7 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 23: Assurance Measures for EAL2

Component	How 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).it'
ADV_FSP.2	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.
ADV_TDS.1	The TOE design describes the TOE security functional (TSF) boundary and how the TSF implements the security functional requirements. The design description includes the decomposition of the TOE into subsystems, thus providing the purpose of the subsystem, the behavior of the subsystem and the actions the subsystem performs. The description also identifies the subsystem 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; thus providing a description of what the TOE is doing and how.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.2	The Configuration Management (CM) document(s) describes how the consumer (end-user) of

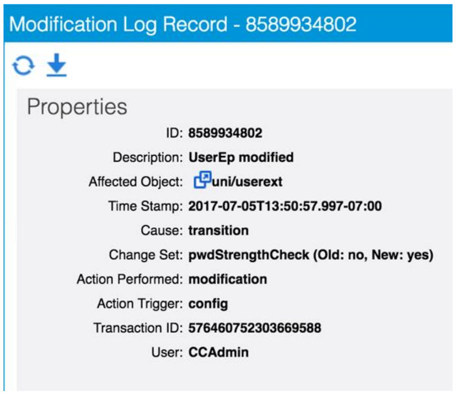
Component	How requirement will be met
ALC_CMS.2	the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s), identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that 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. Cisco uniquely identifies configuration items and each release of the TOE has a unique reference. The Configuration Management documentation contains a configuration item list.
ALC_DEL.1	Cisco documents the delivery procedure 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	The Test document(s) consist of a test plan describes the test configuration, the approach to testing, and how the TOE security functionality interfaces (TSFI) has been tested against its functional specification 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_FUN.1	
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 chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 24 How TOE SFRs are Met

TOE SFRs	How the SFR is Met
FAU_GEN.1	The TOE generates an audit record that is stored internally within the TOE whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, events related to the enforcement of information flow policies, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in Table 16. Each of the events is specified in the syslog which is stored internal to the TOE in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. The administrative configuration of contracts (RACL or VACL) and EPG to EPG contain an option to enable auditing. By default auditing is enabled. More verbose logging can be configured for contracts on the Nexus 9000 Series switch. This verbose logging results in packets that match deny rules in the contract being logged. A full list of the contents of the generated audit information can be found in the table associated with FAU_GEN.1. Each time an administrative user logs into or off of the Nexus 9000 Series switch or APIC, an audit record is generated. The audit record contains the Day of Week, the Date, the Action, the User ID, and terminal information (where applicable) of the user logging into the Nexus 9000 Series switch. Whenever an administrative user make a configuration change to the Nexus 9000 Series switch, an audit record is generated on a per-command basis. Likewise, the audit record contains the Day of Week, the Date, the Action, the User ID, the outcome of the event, and terminal information (where applicable) of the user making the configuration change. All SSH and TLS login accounting records are aggregated and stored in the controller. Auditing cannot be globally disabled and is automatically available upon the startup of the TOE. As a result, there is no auditable event that captures the startup and shutdown of the audit function. Therefore, the first audit event on startup and the last audit event on shutdown of the TOE are the designated startup and shutdown audit events. Example audit event is included below:  Modification Log Record - 8589934802 Properties ID: 8589934802 Description: UserEp modified Affected Object: uni/userext Time Stamp: 2017-07-05T13:50:57.997-07:00 Cause: transition Change Set: pwdStrengthCheck (Old: no, New: yes) Action Performed: modification Action Trigger: config Transaction ID: 576460752303669588 User: CCAdmin

TOE SFRs	How the SFR is Met
FAU_GEN.2	The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result they are traceable to a specific user. For example a human user, user identity, or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented.
FAU_STG.1	Access to the audit records stored on the TOE is only through a TSF Mediated interface. Only users explicitly authorized to access the audit records are given access to the audit records. There is no interface which may be used to perform audit record modification. In addition, logs can be cleared by an authorized administrator via the configured log retention policies. A summary of logs can also be viewed from the APIC. For the Nexus 9000 Series, logs are written to a database. The following commands show the audit logs: show accounting log show audits show sessions The logs may be viewed through the APIC GUI interface also. Audit records are objects that are created by the system to log user-initiated actions, such as login/logout and configuration changes. They contain the name of the user who is performing the action, a timestamp, a description of the action and, if applicable, the FQDN of the affected object. Audit records are never modified after creation and are deleted when their number exceeds the maximum value specified in the audit retention policy. The AAA logs that audit administrator actions on the TOE are stored separately in the AAA accounting log. All log locations are protected from modification and unauthorized deletion through the roles assigned to authorized administrators. By default, the logs are circular and once the log data reach capacity of the data storage, they are overwritten. With NX-OS, there is logging of event-histories that run in the background by default. The event-history log size is configurable.
FCS_CKM.1	The TOE generates cryptographic keys for Diffie-Hellman key establishment (conformant to NIST SP 800-56A) and for ECDSA and RSA key establishment schemes (conformant to NIST SP 800-56B). Diffie-hellman is used to generate the key that will secure the SSH sessions. The TOE complies with section 5.6 and all subsections regarding asymmetric key pair generation and key establishment in the NIST SP 800-56A. The TOE complies with section 6 and all subsections regarding RSA key pair generation and key establishment in the NIST SP 800-56B. The HMAC-SHA1 is used for the key generation in authenticating the RADIUS communications. HMAC-1 is also used to ensure data integrity during SSH sessions. The TOE can create a RSA and ECDSA public-private key pair that can be used to generate a Certificate Signing Request (CSR). Through use of Simple Certificate Enrollment Protocol (SCEP), the TOE can: send the CSR to a Certificate Authority (CA) for the CA to generate a certificate; and receive its certificate (including X.509v3) from the CA. Integrity of the CSR and certificate during transit are assured through use of digitally signatures (encrypting the hash of the TOE's public key contained in the CSR and certificate). The TOE can store and distribute the certificate to external entities including Registration Authorities (RA). X.509v3 certificates are used for administrator authentication using the APIC GUI and for device-level authentication of the Nexus 9k in ACI mode switches and the APIC.
FCS_CKM.4	The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs) in that none of the symmetric keys, pre-shared keys, or private keys are stored in plaintext form.

TOE SFRs	How the SFR is Met
	Through the implementation of cryptographic module, the TOE zeroizes all of the cryptographic keys used within the TOE after the key is no longer of use to the TOE. The key and CSP zeroization capabilities of the TOE have been verified as part of the TOE's FIPS 140-2 validation. See Table 6 and Table 30 for more information. The cryptographic key destruction is used as follows: • After TOE administration via SSH/SFTP is completed, the tunnel is torn down and the session key is overwritten. • After TLS session is completed, the tunnel is torn down and the session key is overwritten.
FCS_COP.1	The TOE provides symmetric encryption and decryption capabilities using AES in CBC, GCM, and CTR modes (128, 192, and 256 bits) as described in FIPS PUB 197, NIST SP 800-38A and NIST SP 800-38D. In addition, digital signature and verification are performed using DSA, ECDSA, and RSA. Image digital signature verification is performed on bootup of the TOE. AES is implemented in the following protocols: SSHv2 and TLS. The TOE provides AES encryption and decryption in support of SSHv2 and TLS for secure communications. Management of the cryptographic algorithms is provided through the CLI and GUI with auditing of those commands. AES data encryption is the encryption/ decryption option that is used within SSHv2 and TLS session communications. AES - Provides data protection using symmetric encryption and decryption for SSH/SFTP and TLS communications. SHA- hashing - Provides the hashing protection required by the SSH/TLS protocol and SHA256 is used for password hashing. RSA: This provides the asymmetric encryption used as part of the session setup process for SSH and TLS communications. DSA: Provides data protection using symmetric encryption and decryption for SSH/SFTP communications. HMAC-SHA: Is used to ensure the integrity of the SSHv2 and TLS session.
FCS_SSH_EXT.1	The TOE implements SSHv2 (telnet is disabled in the evaluated configuration). SSHv2 sessions are limited to an administrator configurable session timeout period, and will be rekeyed upon request from the SSH client. The key exchange methods used by the TOE is a configurable option.. The TOE implementation of SSHv2 supports the following: • local password-based authentication for administrative users accessing the TOE through SSHv2, and optionally supports deferring authentication to a remote AAA server. • public key based authentication using SSH keys. • encryption algorithms, AES-CTR-128, AES-CTR-256 to ensure confidentiality of the session. • hashing algorithms HMAC-SHA-1 to ensure the integrity of the session.
FCS_TLS_EXT.1	An authorized administrator can initiate inbound TLSv1.1 and TLSv1.2 connections using the web based GUI for remote administration of the TOE. TLS is also used to protect the TLS sessions between the APIC and Nexus 9000 switches in the ACI mode.
FDP_IFC.1	The TOE enforces the *Virtual and Distributed Switch Information Flow Control* policies on network traffic (IPv4, IPv6 and non-IP) received by the Nexus 9000 Series interfaces

TOE SFRs	How the SFR is Met
	including any Nexus Layer 3 interface, VLAN interfaces, Physical Layer 3 interfaces, Layer 3 Ethernet subinterfaces, Layer 3 Ethernet port-channel interfaces, Layer 3 Ethernet port-channel subinterfaces, Tunnels, Management interfaces, Layer 2 interfaces, or Layer 2 Ethernet port-channel interfaces. Each information flow is controlled by the supervisor (permit, drop, ignore) via the ACLs while the network traffic is mediated via the I/O network module ports. The TOE makes an information flow decision to Permit traffic flow, Deny traffic flow, Redirect the traffic to an interface, Deny traffic flow and log a copy of the traffic, or Disable the ingress interface. Whenever an endpoint device attempts to send network traffic to the TOE protected network, the TOE verifies that the posture, or state, of 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 TOE either denies the traffic flow or quarantines the Traffic flow to access to the TOE protected network that is sufficient only for remediation. After remediation the TOE checks the posture of the device again.
FDP_IFF.1	Whenever network traffic (both IP and non-IP traffic) is received by one of the Nexus 9000 Series interfaces, the TOE applies administratively configured information flow policies. All traffic within the ACI fabric is whitelisted by allowing traffic to flow between defined Endpoint Groups (EPGs). EPGs provide a logical grouping for objects that require similar policy. Because ACI is not like the standard NX-OS switch in a Data Center (DC), in ACI the EPG endpoints are fully isolated from each other within a subnet when an authorized administrator enables intra-EPG isolation. The Inter-EPG communication always goes through a whitelist firewall. No traffic is allowed to flow unless a contract is created that says this protocol can flow from this EPG to another EPG. As a result, the DHCP snooping and Dynamic ARP are not required in the Nexus 9k in ACI mode fabric. The following rules are applied through the abstraction of the Software Defined Networking level. For example configuring the tenant, contracts, and intra and inter Endpoint Group Configurations creates the ACLs. 1. Port Security 2. Traffic Storm Inspection (all applied at the same time) 3. Context (VRFs) 4. Contracts (VACL IP ACLs) 5. Contracts (RACL IP ACLs) The specific rules associated with each policy are, as follows: **Port Security** An administrator can configure the Nexus 9000 Series switch to allow inbound traffic from only a restricted set of MAC addresses. This policy can be applied to Layer 2 Access Ports, Layer 2 Trunk Ports, or Layer 2 SPAN Source Ports. The Nexus 9000 Series switch makes an information flow decision to permit, deny, or disable the port whenever traffic is received on the port. The TOE makes the information decision based on the following, ▪ The source MAC address is administratively configured as secure for the Nexus 9000 Series interface, or, ▪ The source MAC address is dynamically identified as secure by the TOE. A source MAC address is considered secure if the following criteria is met, o The Nexus 9000 Series has not reached any connection maximums;

TOE SFRs	How the SFR is Met
	○ The source MAC address has not already been secured for another port within the same VxLAN ▪ And, the network traffic flow is not denied by any Traffic Storm Inspection policies **Traffic Storm** Traffic storm control allows an administrator to monitor the levels of the incoming traffic to a Nexus 9000 Series switch layer 2 interface over a 1-second interval. During this interval, the traffic level, which is a percentage of the total available bandwidth of the port, is compared with the administratively configured traffic storm control level. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control denies the traffic flow until the interval ends. The TOE enforces the following traffic storm rules, ▪ Network traffic flow is permitted if the bandwidth used by the combination of Broadcast, Unicast, and Multicast Traffic on a given port does not exceed the administratively configured threshold of available bandwidth for that interface port over a one second time frame ▪ Network traffic flow is denied when the bandwidth used by the combination of Broadcast, Unicast, and Multicast Traffic on a given port exceeds the administratively configured threshold of available bandwidth for that interface port over a one second time frame **Contract (PACLs)** When non-IP network traffic that meets an administratively configured PACL is received on Layer 2 interfaces or Layer 2 Ethernet port-channel interfaces, the Nexus 9000 Series switch makes an information flow decision to either permit or deny the traffic. Traffic is permitted or denied, as follows, ▪ Ingress Non-IP traffic with security attributes that match an administratively configured PACL permit policy for non-IP traffic rule is allowed to flow, or, ▪ Ingress Non-IP traffic with security attributes that match an administratively configured deny policy rule is not permitted. The PACL permit/deny policies for non-IP traffic are comprised of a combination of information attributes and a permit/deny operation. The information attributes that are available for the creation of PACL permit/deny policies for non-IP traffic include: Protocol, Class of Service (COS), VLAN ID **Tenant (VRFs)** At the top level, the Cisco APIC policy model is built on a series of one or more tenants that allow segregation of the network infrastructure administration and data flows. These tenants can be used for customers, business units, or groups, depending on organizational needs. Tenants further break down into private Layer 3 networks, which directly relate to a Virtual Route Forwarding (VRF) instance or separate IP space. Each tenant may have one or more private Layer 3 networks depending on their business needs. Private Layer 3 networks provide a way to further separate the organizational and forwarding requirements below a given tenant. The Nexus 9000 Series switch provides the ability for an administrative user to configure VRFs for incoming IP traffic. For IP traffic that is received by the Nexus 9000 Series interfaces, the Nexus 9000 Series switch verifies which VRF the traffic is associated with and forwards the traffic in a manner consistent with the routing table associated with the VRF. There is no way for the user to circumvent the configured VRFs. The following VRF related rules are applied to Network traffic.

TOE SFRs	How the SFR is Met
	▪ IP traffic with security attributes that map to a configured VRF will be forwarded through the Nexus 9000 Series switch TOE component per the VRF routing table **Contract (VACL IP)** When network traffic that meets an administratively configured VACL IP ACL is received on VLAN interfaces, the Nexus 9000 Series switch makes an information flow decision to forward the traffic, redirect the traffic, drop the traffic, or drop the packet and create a log of the dropped traffic. Traffic is forwarded, redirected, dropped, or dropped and logged, as follows, ▪ IP traffic with security attributes that match an administratively configured permit policy rule is allowed to flow, or, ▪ IP traffic with security attributes that match an administratively configured deny policy rule is not permitted to flow. IP traffic with security attributes that match an administratively configured redirect policy rule is redirected to the specified interface, or, ▪ IP traffic with security attributes that match an administratively configured deny-and-log policy rule is not permitted to flow and a copy of the traffic is logged by the TOE. The permit/deny/redirect/deny-and-log policies (defined in VACL IP) for IP traffic described above are comprised of a combination of subject security attributes and information attributes and a permit/deny/redirect/deny-and-log operation. The subject attributes that are available for the creation of permit/deny/redirect/deny-and-log policies include: vlan-ID. The information attributes that are available for the creation of permit/deny/redirect/deny-and-log policies include: Source IP address, Destination IP address, Source port number, Destination port number, Protocol, ICMP message type, ICMP message code, IGMP message type, Packet length, Precedence, DSCP Value ▪ Non-IP traffic with security attributes that match an administratively configured permit policy rule is allowed to flow, or, ▪ Non-IP traffic with security attributes that match an administratively configured deny policy rule is not permitted to flow. Non-IP traffic with security attributes that match an administratively configured redirect policy rule is redirected to the specified interface, or, ▪ Non-IP traffic with security attributes that match an administratively configured deny-and-log policy rule is not permitted to flow. The permit/deny/redirect/deny-and-log policies (defined in VACL IP) for non-IP traffic described above are comprised of a combination of subject security attributes and information attributes and a permit operation. The subject attributes that are available for the creation of these permit/deny/redirect/deny-and-log policies include: vlan-ID. The information attributes that are available for the creation of these permit/deny/redirect/deny-and-log policies include: Source IP address, Destination IP address, Protocol, Class of Service (COS), or VLAN ID **Contracts (RACL IP)** When network traffic that meets an administratively configured RACL or PACL IP ACL is received on VLAN interfaces, Physical Layer 3 interfaces, Layer 3 Ethernet subinterfaces, Layer 3 Ethernet, port-channel interfaces, Layer 3 Ethernet port-channel subinterfaces, Tunnels, or Management interfaces, the Nexus 9000 Series switch makes an information flow decision to either permit or deny the traffic. Traffic is permitted or denied, as follows, ▪ Ingress or egress IP traffic with security attributes that match an administratively configured RACL permit policy rule is allowed to flow, or,

TOE SFRs	How the SFR is Met
	▪ Ingress or egress IP traffic with security attributes that match an administratively configured RACL deny policy for IP traffic rule is not permitted. The RACL permit/deny policies for IP traffic are comprised of a combination of information attributes and a permit/deny operation. The information attributes that are available for the creation of RACL permit/deny policies include: Source IP address, Destination IP address, Source port number, Destination port number, Protocol, ICMP message type, ICMP message code, IGMP message type, Packet length, Precedence, DSCP Value Note: RACLs are applied to both ingress and egress traffic. Additionally, the following explicit authorize rules are enforced on information flows. ▪ ARP traffic received on interfaces configured as trusted is always allowed to pass. The following explicit deny rules are enforced on information flows. For IP Network Traffic Flows: ▪ The TOE denies IP traffic flow when the IP address of the traffic is not identified as a valid combination either through administrative configuration, or, ▪ For IP traffic, if the security attributes do not match an administratively configured RACL or VACL, the traffic flow is denied, or, ▪ If the IP traffic security attributes do not map to a configured 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 and application profile the traffic flow is denied.
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 use zeros for padding. Residual data is never transmitted from the TOE. 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_PMG_EXT.1	The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “%”, “^”, “&”, “*”, “(“, and “)”.

TOE SFRs	How the SFR is Met
FIA_UIA_EXT.1 FIA_UAU_EXT.2 FIA_UID.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 Nexus 9000 Series APIC GUI and CLI. The TOE mediates all administrative actions through the APIC GUI and CLI. Once a potential administrative user attempts to access the GUI of the TOE through TLS or the CLI of the TOE through either a directly connected console or remotely through an SSHv2 connection, 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: • Remote authentication (facilitated by RADIUS or TACACS+ (provided by the IT environment)); • Authentication against a local database.
FIA_UAU.7	When a user enters their password at the local console, CLI via SSH, and APIC GUI via TLS and web browser the TOE does not echo any of the characters of the password or any representation of the characters.
FMT_MSA.1	The TOE allows authenticated and authorized administrative users of the APIC to manage the policies of the ACI fabric and infrastructure. The authorized administrator manages the Nexus 9000 Series switches in the ACI mode TOE component to Read, write Contracts (ACLs) policy and the Inspection policies as well as the attributes contained within the policy rules. The TOE allows access to the policy rules based on the permissions defined for the user's administratively assigned roles. Only users assigned a role with appropriate access privileges in the policy rules are allowed to have any access. All other administrative users have no visibility into the existence of the policy rules.
FMT_MSA.3	There are no default ACLs for the information flow control on the Nexus 9000 Series switch TOE component. Without default ACLs and/or RACLS, packet flows are not allowed. This is a restrictive default policy. The TOE does allow other policies to be created. However, when the policies are removed, the default TOE information flow control policy is still restrictive.
FMT_MTD.1	The TOE provides the ability for administrators of the Nexus 9000 Series to access TOE configuration and audit data. Each of the predefined and administratively configured roles has either read or write access to the configuration and audit data. See the SFR definition in section 5 for details regarding the specific access available to each user role.
FMT_SMF.1	Through the administrative interface of the Nexus 9000 Series APIC GUI and CLI, the TOE facilitates the following administrative functions: ▪ Configuration of Contracts (RACL, IP ACLs) within the ACLs SFP – This functionality allows the configuration of RACL and IP ACLs by an administrative user. ▪ Configuration of Contracts VACL IP ACLs within the ACLs SFP – This functionality allows the configuration of VACL IP ACLs by an administrative user. ▪ Configuration of RBACs - This functionality allows the configuration of RBACs by an administrative user. ▪ Configuration of Port Security within the ACLs SFP - This functionality allows the configuration of Port Security by an administrative user. ▪ Configuration of Traffic Storm within the ACLs SFP - This functionality allows the configuration of Traffic Storm by an administrative user. ▪ Configuration of Control Plane Policing within the Control Plane Policing/Rate Limiting SFP - This functionality allows the configuration of Control Plan Policing

TOE SFRs	How the SFR is Met
	by an administrative user. ▪ Configuration of Rate Limiting within the Control Plane Policing/Rate Limiting SFP - This functionality allows the configuration of Rate limiting by an administrative user. ▪ Reviewing audit records – This functionality allows Nexus 9000 Series audit records to be viewed by an administrative user. ▪ Configuration of Nexus 9000 Series cryptographic services - This functionality allows the configuration of Nexus 9000 Series cryptographic by an administrative user. ▪ Management of Users – This functionality allows the creation and configuration of users and the ability to assign roles to a specific user. ▪ Review Nexus 9000 Series configuration - This functionality allows the administrative user to review the Nexus 9000 Series configuration.
FMT_SMR.1	Cisco NX-OS devices uses role-based access control (RBAC) for authorization. The APIC provides access according to a user’ s role through role-based access control (RBAC). An ACI fabric user is associated with the following: • A set of roles • For each role, an associated privilege type can be assigned: no access, read-only, or read-write For example, because an “ admin” role is configured with privilege bits for “fabric-equipment” and “ tenant-security,” the “ admin” role has access to all objects that correspond to equipment of the fabric and tenant security. Creating a user and assigning a role to that user does not enable access rights. It is necessary to also assign the user to one or more security domains. By default, the ACI fabric includes two special pre-created domains: • All— allows access to the entire MIT • Infra— allows access to fabric infrastructure objects/subtrees, such as fabric access policies The permissions associated with the predefined administrative roles cannot be modified.
FPT_APW_EXT.1	The TOE prevents reading of passwords. The TOE does not store the password, it only stores the AES encrypted value of the password, so the password is unreadable in configuration files or via the GUI. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators.
FPT_STM.1	The Nexus 9000 Series switch can provide hardware based timestamp that are used to provide that timestamp in audit records. The TOE provides the option to either use the internally generated time stamps or at the discretion of the administrator use an external time server to provide the time stamp. The TOE provides a source of date and time information for the router, used in audit timestamps. This function can only be accessed from within the configuration exec mode via the privileged mode of operation of the TOE. The clock function is reliant on the system clock provided by the underlying hardware. The TOE can optionally be set to receive time from an NTP server.
FPT_TST_EXT.1	The TOE runs a suite of self-tests during initial start-up to verify its correct operation. Refer to the FIPS Security Policy for available options and management of the cryptographic self-test.

TOE SFRs	How the SFR is Met
	For testing of the TSF, the TOE automatically runs checks and tests at startup and during resets to ensure the TOE is operating correctly. Refer to the Guidance documentation for installation configuration settings and information and troubling shooting if issues are identified. When the system is booted up in FIPS mode, the FIPS power-up self-tests run on the supervisor and line card modules. If any of these FIPS self-tests fail, the whole system is moved to the FIPS error state. In this state, as per the FIPS requirement, all cryptographic keys are deleted, and all line cards are shut down. This mode is exclusively meant for debugging purposes. Once the switch is in the FIPS error state, any reload of a line card moves it to the failure state. To move the switch back to FIPS mode, it has to be rebooted. However, once the switch is in FIPS mode, any power-up self-test failure on a subsequent line card reload or insertion affects only that line card, and only the corresponding line card is moved to the failure state. 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.
FTA_SSL.4	An administrator is able to exit out of both local and remote administrative sessions.
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	All remote administrative communications take place over a secure encrypted SSH or TLS session. The SSH/TLS session is encrypted using AES encryption. A remote authorized administrator is able to initiate SSH/TLS communications with the TOE.

6.2 TOE Bypass and interference/logical tampering Protection Measures

The Nexus 9000 Series switch is a hardware appliance untrusted subjects. All administration and configuration operations are performed within the physical boundary of the TOE. Also, all TSP enforcement functions must be invoked and succeed prior to functions within the TSC proceeding.

The TOE has been designed so that all locally maintained TSF data can only be manipulated via the secured management interfaces, including the CLI and GUI interfaces. There are no undocumented interfaces for managing the product. The CLI interface achieves a trusted path via SSH public key authentication and is recommended for remote authorized administrator access. The GUI interface is a trusted path via TLS client authentication for remote authorized administrator access.

All sub-components included in the TOE hardware rely on the main Nexus 9000 Series switch for power, memory management, and access control. In order to access any portion of the Nexus 9000 switch, the Identification & 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 provide 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 UCS. 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 UCS hardware and is protected by the mechanisms described above.

This design, combined with the fact that only an administrative user with the appropriate role may access the TOE security functions, provides a distinct protected domain for the TOE that is logically protected from interference and is not bypassable.

6.3 Rationale for requirements/TOE Objectives

The security requirements are derived according to the general model presented in Part 1 of the Common Criteria. Specifically, the tables below illustrate the mapping between the security requirements and the security objectives and the relationship between the threats, policies and IT security objectives. This section identifies each Security Functional Requirement identified in Section 5, the TOE security objective(s) identified in Section 4 that addresses it, Table 25 and Table 26 provide the mapping and rationale for inclusion of each SFR in this ST.

6.4 Rationale for TOE Security Objectives

Table 25: SFR/Objectives Mappings

	O.DATA_FLOW_CONTROL	O.DISPLAY_BANNER	O.PROTECTED_COMMUNICATIONS	O.RESIDUAL_INFORMATION_CLEARING	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION	O.TSF_SELF_TEST
FAU_GEN.1					X		
FAU_GEN.2					X		
FAU_STG.1					X		
FCS_CKM.1			X				
FCS_CKM.4			X				
FCS_COP.1			X				
FCS_SSH_EXT.1			X				
FCS_TLS_EXT.1			X				
FDP_IFC.1	X						
FDP_IFF.1	X						
FDP_RIP.2				X			
FIA_PMG_EXT.1						X	
FIA_UIA_EXT.1						X	
FIA_UID.2						X	
FIA_UAU_EXT.2						X	
FIA_UAU.7						X	

	O.DATA_FLOW_CONTROL	O.DISPLAY_BANNER	O.PROTECTED_COMMUNICATIONS	O.RESIDUAL_INFORMATION_CLEARING	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION	O.TSF_SELF_TEST
FMT_MSA.1						X	
FMT_MSA.3	X					X	
FMT_MTD.1						X	
FMT_SMF.1						X	
FMT_SMR.1						X	
FPT_APW_EXT.1						X	
FPT_STM.1					X		
FPT_TST_EXT.1							X
FTA_SSL.4						X	
FTA_TAB.1		X					
FTP_TRP.1			X				

The inspection of Table 25 shows that:

- Each SFR traces back to at least one security objective;
- Each security objective for the TOE has at least one SFR tracing to it.

6.4.1.1 Justification of SFR tracing

The justification demonstrates that the SFRs address all security objectives of the TOE.

Table 26 SFR Tracing Justification

Objective	Rationale
O.DATA_FLOW_CONTROL	The SFRs, FDP_IFC.1, and FDP_IFF.1 meet this objective by ensuring the TOE mediates the flow of all information between clients and servers located on internal and external networks governed by the TOE. The TOE is required to identify the subject attributes and information attributes necessary to enforce the Virtual and Distributed Switch Information Flow Control SFP. The policy is defined by rules defining the conditions for which information is permitted or denied to flow. The SFR, FMT_MSA.3, ensures the TOE provides the capability for administrators to define default deny rules, though the default policy for the information flow control security rules is restrictive where no explicit rules exist until created and applied by an Authorized Administrator. The TOE enforces information flow policies on network traffic (both IPv4 and v6 and non-IP) received by the Nexus 9000 Series interfaces including any Nexus Layer 3 interface, VLAN interfaces, Physical Layer 3 interfaces, Layer 3 Ethernet subinterfaces, Layer 3 Ethernet port-channel interfaces, Layer 3 Ethernet port-channel subinterfaces, Tunnels, Management interfaces, Layer 2 interfaces, or Layer 2 Ethernet port-channel interfaces. The TOE makes an information flow decision to Permit traffic flow, Deny traffic flow, Redirect the traffic to an interface, Deny traffic flow and log a copy of the traffic, or Disable the ingress interface. Whenever an endpoint device attempts to send network traffic to the TOE protected network, the TOE verifies that the posture, or state, of 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 TOE either denies the traffic flow or quarantines the Traffic flow to access to the TOE protected network that is sufficient only for remediation. After remediation the TOE checks the posture of the device again.
O.DISPLAY_BANNER	The SFR, FTA_TAB.1 meets this objective by displaying an advisory notice and consent warning message regarding unauthorized use of the TOE.
O.PROTECTED_COMMUNICATIONS	The SFRs, FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FCS_SSH_EXT.1, FCS_TLS_EXT.1, FTP_TRP.1 meet this objective by ensuring the communications between the TOE and endpoints are secure by implementing the encryption protocols as defined in the SFRs and as specified by the RFCs.
O.RESIDUAL_INFORMATION_CLEARING	The SFR, FDP_RIP.2 meets this objective by ensuring no left over user data from the previous transmission is included in the network traffic.
O.SYSTEM_MONITORING	The SFRs, FAU_GEN.1, FAU_GEN.2, FAU_STG.1, 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. The TOE writes audit events to NVRAM, DRAM and flash. All log locations are protected from modification and deletion.

Objective	Rationale
	Logs can only be cleared by an authorized administrator through the CLI. The logs can also be sent to a configured syslog server.
O.TOE_ADMINISTRATION	The SFRs, FIA_UIA_EXT.1, FIA_PMG_EXT.1, FIA_UAU_EXT.2, FIA_UID.2, FIA_UAU.7, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FPT_APW_EXT.1, FTA_SSL.4 meet this objective by ensuring the TOE supports a password-based authentication mechanism with password complexity enforcement such as, strong passwords, password life-time constraints, providing current password when changing the password, obscured password feedback when logging in, and passwords are not stored in plaintext. The objective is further met by ensuring restrictive default values are enforced on the SFPs (authorization and flow control), that only Authorized Administrators can override the default values. The TOE provides the management and configuration features to securely manage the TOE and that those functions are restricted to the Authorized Administrator. In addition, the TOE provides the ability for an Authorized Administrator to exit or logoff an administrator session.
O.TSF_SELF_TEST	The SFR, FPT_TST_EXT.1 meets this objective by performing self-test to ensure the TOE is operating correctly and all functions are available and enforced.

6.5 Security objectives rationale

The security objectives rationale shows how the security objectives correspond to assumptions, threats, and organizational security policies and provide a justification of that tracing.

6.5.1 Tracing of security objectives to SPD

The tracing shows how the security objectives OT.* and OE.* trace back to assumptions A.*, threats T.*, and organizational security policies OSP.* defined by the SPD.

Table 27 Tracing of security objectives to SPD

	A.NO_GENERAL_PURPOSE	A.FIREWALL	A.PHYSICAL	A.REMOTE_SERVERS	A.TRUSTED_ADMIN	T. NET_TRAFFIC	T.TSF_FAILURE	T.UNAUTHORIZED_ACCESS	T.UNDETECTED_ACTIONS	T.USER_DATA_REUSE	P.ACCESS BANNER
O.DATA_FLOW_CONTROL						X					
O.DISPLAY_BANNER											X
O.PROTECTED_COMMUNICATIONS								X			
O.RESIDUAL_INFORMATION_CLEARING										X	

O.SYSTEM_MONITORING									X		
O.TOE_ADMINISTRATION								X			
O.TSF_SELF_TEST							X				
OE.NO_GENERAL_PURPOSE	X										
OE.FIREWALL		X				X					
OE.PHYSICAL			X			X					
OE.REMOTE_SERVERS				X							
OE.TRUSTED_ADMIN					X						

6.5.2 Justification of tracing

The justification demonstrates that the tracing of the security objectives to assumptions, threats, and OSPs is effective and all the given assumptions are upheld, all the given threats are countered, and all the given OSPs are enforced.

6.5.2.1 Tracing of threats and OSPs

Table 28 Threat and OSP Rationale

Objective	Rationale
O.DATA_FLOW_CONTROL	This security objective is necessary to counter the threat T.NET_TRAFFIC to ensure that information flow control policies are enforced to limit access to an attacker (unauthorized user) sending malicious traffic through/to the TOE and to mitigate attacks between the EPGs.
O.DISPLAY_BANNER	This security objective is necessary to address the Organizational Security Policy P.ACCESS_BANNER to ensure an advisory notice and consent warning message regarding unauthorized use of the TOE is displayed before the session is established.
O.PROTECTED_COMMUNICATIONS	This security objective is necessary to counter the threat: T.UNAUTHORIZED_ACCESS to ensure remote communications with the TOE are not compromised. O.PROTECTED_COMMUNICATIONS ensures that the administrator remote communications path is encrypted; therefore, providing a secured remote communications session to the TOE CLI preventing unauthorized users from viewing credentials or other TSF data passed in the session communications.
O.RESIDUAL_INFORMATION_CLEARING	This security objective is necessary to counter the threat T.USER_DATA_REUSE so that data traversing the TOE could inadvertently be sent to a user other than that intended by the sender of the original network traffic.
O.SYSTEM_MONITORING	This security objective is necessary to counter the T.UNDETECTED_ACTIONS to ensure activity is monitored so the security of the TOE is not compromised.
O.TOE_ADMINISTRATION	This security objective is necessary to counter the threat: T.UNAUTHORIZED_ACCESS to ensure administrators must identify and authenticate themselves before gaining access to the TOE's management interface.
O.TSF_SELF_TEST	This security objective is necessary to counter the threat T.TSF_FAILURE to ensure failure of mechanisms do not lead to a compromise in the TSF.

6.5.2.2 Tracing of assumptions

Table 29: Threat/Policies/TOE Objectives Rationale

Environment Objective	Rationale
OE.NO_GENERAL_PURPOSE	This security objective is necessary to address the assumption A.NO_GENERAL_PURPOSE by ensuring there are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) capabilities on the TOE.
OE.FIREWALL	This security objective is necessary to address the assumption A.FIREWALL by ensuring the TOE is protected by the firewall against unauthorized traffic through/to the TOE. This security objective is also necessary to counter the threat T.NET_TRAFFIC to ensure malicious and unauthorized traffic from outside the TOE is prevented from traversing the network and the TOE by the firewall.
OE.PHYSICAL	This security objective is necessary to address the assumption A.PHYSICAL by ensuring the TOE and the data it contains is physically protected from unauthorized access. This security objective is necessary to counter the threat T.NET_TRAFFIC to ensure that access is limited to the Nexus 9k ACI mode data center fabric to limit access to an attacker (unauthorized user) sending malicious traffic through/to the TOE and to mitigate attacks between the EPGs.
OE.REMOTE_SERVERS	This security objective satisfies A. REMOTE_SERVERS by the administrator ensuring the communications session between the TOE and NTP server as well as optional remote servers is secured.
OE.TRUSTED_ADMIN	This security objective is necessary to address the assumption A.TRUSTED_ADMIN by ensuring the administrators are non-hostile and follow all administrator guidance.

7 ANNEX A: KEY ZEROIZATION

7.1 Key Zeroization

The following table describes the FIPS 140-2 key zeroization referenced by FCS_CKM.4 provided by the TOE.

Table 30: TOE Key Zeroization

Name	Description	Zeroization
Diffie-Hellman Shared Secret	The value is zeroized after it has been given back to the consuming operation. The value is overwritten by 0's.	Automatically after completion of DH exchange. Overwritten with: 0x00
Diffie Hellman private exponent	The function returns the value to the RP and then calls the function to perform the zeroization of the generated key pair (p_dh_kepair) and then calls the standard Linux free (without the poisoning). These values are automatically zeroized after generation and once the value has been provided back to the actual consumer.	Zeroized upon completion of DH exchange. Overwritten with: 0x00
RADIUS secret	The function calls aaa_free_secret, which uses the poisoned free operation to zeroize the memory from the secret structure by overwriting the space with 0x0d and releasing the memory.	Zeroized using the following command: # no radius-server key Overwritten with: 0x0d
TACACS+ secret	The function calls aaa_free_secret, which uses the poisoned free operation to zeroize the memory from the secret structure by overwriting the space with 0x0d and releasing the memory.	Zeroized using the following command: # no tacacs-server key Overwritten with: 0x0d
SSH Private Key	Once the function has completed the operations requiring the RSA key object, the module over writes the entire object (no matter its contents) using memset. This overwrites the key with all 0's.	Zeroized using the following command: # crypto key zeroize rsa Overwritten with: 0x00
AES Key	The results zeroized using the poisoning in free to overwrite the values with 0x00. Zeroization for both SSH and TLS is done by the OPENSSL_cleanse function.	Automatically when the SSH/TLS session is terminated. Overwritten with: 0x00

8 ANNEX B: REFERENCES

The following documentation was used to prepare this ST:

Table 31: 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 4, CCMB-2012-009-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 4, CCMB-2012-009-004
[NDPP]	Protection Profile for Network Devices, version 1.1, June 8, 2012
[800-38A]	NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001
[800-56A]	NIST Special Publication 800-56A, March, 2007 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
[800-56B]	NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009 Key Establishment Schemes Using Integer Factorization Cryptography
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001
[FIPS PUB 186-2]	FIPS PUB 186-2 Federal Information Processing Standards Publication 2000 January 27
[FIPS PUB 186-3]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2009
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[800-90]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2012
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008