Nexus 5000 Series Switch Security Target

Revision 1.2

March, 2013

Table of Contents

List of Tables

DOCUMENT INTRODUCTION

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Nexus 5000 Series Switch with 2000 Series Fabric Extenders, NX-OS, and Cisco Secure Access Control Server (ACS) solution. 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.

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 3, Chapter 4.

1.1 ST and TOE Reference

This section provides information needed to identify and control this ST and its TOE. This ST targets Evaluation Assurance Level EAL4 augmented with ALC_FLR.2.

Table 1-1: ST and TOE Identification

ST Title	Nexus 5000 Series Switch Security Target
ST Version	Version 1.2
Publication Date	March, 2013
Vendor	Cisco Systems, Inc.
ST Author	Cisco Systems, Inc.
TOE Reference (short)	Nexus 5000 Series Switch with 2000 Series Fabric Extenders, NX-OS, and Cisco Secure Access Control Server (ACS)
TOE Reference (long)	Nexus 5000 Series Switches (5010, 5020, 5548P, 5548UP, 5596UP, and 5596T) with Nexus 2000 Series Fabric Extenders (2148T, 2224TP, 2248TP, 2248TP-E, 2232PP, 2232TM, 2232TM-E, B22F, and B22HP), running NX-OS 5.2(1)N1(2a), and Cisco Secure Access Control Server (ACS) Solution Engine Appliances (1120 and 1121) running ACS 5.2 Patch 10
TOE Software Version	NX-OS 5.2(1)N1(2a), ACS version 5.2 Patch 10
Security Target Evaluation Status	In Evaluation
Keywords	Switch, Data Protection, Authentication, Cryptography

1.2 Acronyms and Abbreviations

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

Table 1-2: Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control List
ACS	Access Control Server
AD	Active Directory
AES	Advanced Encryption Standard

Acronyms / Abbreviations	Definition
ARP	Address Resolution Protocol
ASIC	Application-Specific Integrated Circuit
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
COS	Class of Service
DGT	Destination Group Tag
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DSCP	Differentiated Services Code Point
EAC	Endpoint Admission Control
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GbE	Gigabit Ethernet
Gbps	Gigabits per second
HBA	Host Bus Adapters
HTTPS	Hyper-Text Transport Protocol Secure
IT	Information Technology
ICMP	Internet Control Message Protocol
IDG	Identity Group
IGMP	Internet Group Management Protocol
LDAP	Lightweight Directory Access Protocol
MTU	Maximum Transmission Unit
OS	Operating System
PACL	Port Access Control List
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RPF	Reverse Path Forwarding
RSA	Rivest, Shamir, Adleman
SAN	Storage Area Network
SHS	Secure Hash Standard
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
TACACS+	Terminal Access Controller Access-Control System Plus
Tbps	Terabits per Second
TCP	Transport Control Protocol
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
TTL	Time To Live
UDP	User Datagram Protocol
VACL	VLAN Access Control List
VDC	Virtual Device Context (Only one VDC exists on a Nexus 5000 or 2000 Series switch, whereas Nexus 7000 support multiple VDCs, which allow switches to be virtualized at the device level.)
VLAN	Virtual Local Area Network
VRF	Virtual routing and forwarding

1.3 TOE Overview

1.3.1 TOE Product Type

The Nexus 5000 Series TOE offers a unified fabric with high-capacity 10GbE, Fibre-Channel over Ethernet (FCoE) with low-latency, together with Data Center Ethernet (DCE). In addition to the Nexus 5000 Series Switch itself, the solution provided by the TOE includes the CISCO Nexus 2000 Series Fabric Extender, the NX-OS software and the Cisco Secure Access Control Server (ACS), which provides a scalable GbE and 10GbE Data Center access solution in addition to providing classical Ethernet.

The ACS Server component of the TOE provides authentication services and supports the implementation of information flow policies by the Nexus 5000 switch TOE component. The AAA services provided by the ACS server include RADIUS and TACACS for authentication and maintains the authentication credentials.

1.3.2 Required non-TOE Hardware/ Software/ Firmware

The TOE requires (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 1-3: IT Environment Components

IT Environment Component	Required	Usage/Purpose Description for TOE performance
Web browser	YES	Administrators will use to communicate with the ACS TOE component; GUI administrative web interface. Any web browser may be used. Examples include, Internet Explorer, Firefox, Chrome
SSH Client	YES	Administrators to communicate with ACS and Nexus 5000 switch TOE components via CLI administrative interfaces. Any SSH client may be used. Examples include, PuTTy
SNMP Server	YES	SNMP administrative configuration of the TOE is facilitated by an IT environment SNMP server. Any SNMP may be used that supports SNMPv3 with AES 128 bit encryption.
Time Server	OPTIONAL	Optionally provide time stamps in deployment scenarios in which an external time source is desirable.
RADIUS	OPTIONAL	Optionally used to perform authentication
External Authentication Server	OPTIONAL	The TOE may interact with an external Active Directory, LDAP, or another ACS server for authentication decisions.

1.4 TOE DESCRIPTION

This section provides an overview of the TOE including the Nexus 5000 Series Switch with 2000 Series Fabric Extenders and the Cisco Secure Access Control Server (ACS). This section also defines the TOE components included in the evaluated configuration of the TOE.

Table 1-4: TOE Component Descriptions

TOE Component	TOE-Subcomponent	Description
Nexus 5000 Series	Cisco Nexus 5548P	Supporting 32 fixed 1 and 10 Gigabit Ethernet ports(Ports 1 to 16 Can Run at 1 Gigabit Ethernet),

TOE Component	TOE-Subcomponent	Description
Switch		FCoE, and 1 Expansion Module Slot
	Cisco Nexus 5548UP	Supporting 32 unified ports (each can be Gigabit Ethernet, FCoE, or Fiber Channel), and 1 Expansion Module Slot.
	Cisco Nexus 5596T	The Cisco Nexus 5596T is a 2RU switch, with 32 fixed ports of 10G BASE-T and 16 fixed ports of SFP+, and supports up to three expansion slots.
	Cisco Nexus 5596UP	A 2RU switch supporting 48 1/10 Gigabit Ethernet fixed enhanced Small Form-Factor Pluggable (SFP+) Ethernet/FCoE or 1/2/4/8-Gbps native FC unified ports and three expansion slots.
	Cisco Nexus 5020	Supporting 40 Fixed Ports of 10 Gigabit Ethernet (Ports 1 to 16 Can Run at 1 Gigabit Ethernet), FCoE, and 2 Expansion Module Slots
	Cisco Nexus 5010	Supporting 20 Fixed Ports of 10 Gigabit Ethernet (Ports 1 to 16 Can Run at 1 Gigabit Ethernet), FCoE, and 1 Expansion Module Slot
Cisco Nexus 2000 Series Fabric Extenders	Cisco Nexus 2148T, 2224TP, 2248TP, 2248TP-E, 2232PP, 2232TM, 2232TM-E, B22F, and B22HP Fabric Extenders.	The Cisco Nexus 2000 Series sits on top of a server rack and essentially acts as a remote line card for an upstream switch and becomes an extension of the switch, so software, configuration, and policy are all inherited from the upstream switch; even advanced features such as FCoE and Cisco VN-Link support are inherited. Designed specifically to give customers a means of granularly transitioning from Gigabit Ethernet to 10 Gigabit Ethernet and Unified Fabric; and supporting up to 48 Gigabit Ethernet downlinks and 4 10 Gigabit Ethernet uplinks.
NX-OS	Software image running on N5k and N2k components.	NX-OS 5.2(1)N1(2a)
Cisco Secure Access Control Server (ACS) v5.2 Patch 10	Cisco Secure ACS Solution Engine appliance models 1120, or 1121, or virtual machine.	Cisco Secure ACS is an access control server that operates as a centralized authentication server.

The Cisco Nexus™ 5000 Series Switches comprise a family of line-rate, low-latency, lossless 10 Gigabit Ethernet and Fibre Channel over Ethernet (FCoE) switches for data center applications.

The Cisco Nexus 5000 Series consolidates multiple networks-LAN, SAN, and server cluster-onto a single unified fabric, making multiple parallel networks, switching infrastructure, and cabling unnecessary.. The Cisco Nexus 5000 Series Switches are compatible with third-party consolidated I/O adapters (Consolidated Network Adapters or CNAs) that present separate Ethernet NICs and Fibre Channel HBAs to the server operating system. This allows existing drivers and Fibre Channel management software to work transparently with FCoE. Upstream, two different expansion modules support direct connections from the Cisco Nexus 5000 Series to existing native Fibre Channel SANs.

1.5 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the Nexus 5000 Series Switch with 2000 Series Fabric Extenders, NX-OS and Cisco Secure Access Control Server (ACS) TOE. The TOE is comprised of the following:

Table 1-5: Physical Scope of the TOE

TOE Component	Hardware (within the TOE)	Software (within the TOE)
Nexus 5000 Series Switch	Cisco Nexus 5020 Supporting 40 Fixed Ports of 10 Gigabit Ethernet (Ports 1 to 16 Can Run at 1 Gigabit Ethernet), FCoE, and 2 Expansion Module Slots	NX-OS 5.2(1)N1(2a) This includes a hardened version of Linux Kernel 2.6.
	Cisco Nexus 5010 Supporting 20 Fixed Ports of 10 Gigabit Ethernet (Ports 1 to 16 Can Run at 1 Gigabit Ethernet), FCoE, and 1 Expansion Module Slot	
	Cisco Nexus 5596T, with 32 fixed ports of 10G BASE-T and 16 fixed ports of SFP+, and support for up to three expansion slots.	
	Cisco Nexus 5596UP supporting 48 1/10 Gigabit Ethernet fixed enhanced Small Form-Factor Pluggable (SFP+) Ethernet/FCoE or 1/2/4/8-Gbps native FC unified ports and three expansion slots.	
	Cisco Nexus 5548UP supporting 32 unified ports (each can be Gigabit Ethernet, FCoE, or Fiber Channel), and 1 Expansion Module Slot.	
	Cisco Nexus 5548P Supporting 32 fixed 1 and 10 Gigabit Ethernet ports(Ports 1 to 16 Can Run at 1 Gigabit Ethernet), FCoE, and 1 Expansion Module Slot	
	Cisco Nexus 5000 Series Expansion Modules	
Cisco Nexus 2000 Series Fabric Extenders	Cisco Nexus 2148T, 2224TP, 2248TP, 2248TP-E, 2232PP, 2232TM, 2232TM-E, B22F, and B22HP Fabric Extenders	NX-OS 5.2(1)N1(2a) This includes a hardened version of Linux Kernel 2.6.
Cisco Secure Access Control Server (ACS)	Cisco Secure ACS hardware appliance or virtual machine	ACS Software version 5.2 Patch 10

Product Architecture

Each Cisco Nexus 5000 Series Switch contains a single unified crossbar fabric ASIC and multiple unified port controllers to support fixed ports and expansion modules within the switch.

The unified port controller provides an interface between the unified crossbar fabric ASIC and the network media adapter and makes forwarding decisions for Ethernet, Fibre Channel, and FCoE frames. The ASIC supports the switch by transmitting packets to the unified crossbar fabric before the entire payload has been received. The unified crossbar fabric ASIC is a single-stage, nonblocking crossbar fabric capable of meshing all ports at wire speed; and of improving traffic flow performance with its scheduling for unicast and multicast traffic functionality. In addition, the tight integration of the unified crossbar fabric with the unified port controllers helps ensure low-latency lossless fabric for ingress interfaces requesting access to egress interfaces.

Cisco Nexus 5548P 32-Port Switch

The Cisco Nexus 5548P Switch is a 1RU, 10 Gigabit Ethernet/FCoE access-layer switch built to provide more than 960 Gigabits per second (Gbps) throughput with very low latency. It has:

- Thirty-two, 1/10-Gigabit Ethernet, Cisco Data Center, and FCoE Small Form Factor Pluggable Plus (SFP+) ports.
- One expansion module slot that can be configured to support up to 16 additional 10-Gigabit Ethernet, Cisco Data Center Ethernet, and FCoE SFP+ ports or up to 8 Fibre Channel switch ports, or a combination of both.
- Serial console port and an out-of-band 10/100/1000-Mbps Ethernet management port.
- 1+1 redundant, hot-pluggable power supplies.
- 1+1 redundant, hot-pluggable fan modules to provide reliable front-to-back cooling.

Cisco Nexus 5548UP

The Cisco Nexus 5548UP is a 1RU, 1 Gigabit and 10 Gigabit Ethernet switch offering up to 1.92 terabits per second (Tbps) throughput and scaling up to 48 ports. It has:

- Thirty-two 1/10 Gigabit Ethernet fixed enhanced Small Form-Factor Pluggable (SFP+) Ethernet/FCoE or 1/2/4/8-Gbps native FC unified ports and one expansion slot..
- Unified ports support traditional Ethernet, Fibre Channel (FC),and Fibre Channel over Ethernet (FCoE)
- Connectivity options include 1 Gigabit Ethernet, 10 Gigabit Ethernet, 10 Gigabit Ethernet with FCoE, and 1/2/4/8G Native Fibre Channel
- Switch supports all Cisco Nexus 2000 Series Fabric Extenders

Cisco Nexus 5596T

The Cisco Nexus 5596T is a 2RU, 10 Gigabit Ethernet switch offering up to 1920 Gbps of throughput and up to 96 ports.

- 32 fixed ports of 10G BASE-T
- 16 fixed ports of SFP+
- Connectivity options include 10 Gigabit Ethernet (fiber and copper), Fibre Channel, and FCoE,

Cisco Nexus 5596UP

The Cisco Nexus 5596UP is a 2RU, 1 Gigabit and 10 Gigabit Ethernet switch offering up to 1.92 terabits per second throughput and scaling up to 96 ports. It has:

- Forty-eight 1/10 Gigabit Ethernet fixed enhanced Small Form-Factor Pluggable (SFP+) Ethernet/FCoE or 1/2/4/8-Gbps native FC unified ports and three expansion slots. These slots have a combination of Ethernet/FCoE and native FC ports.
- Unified ports support traditional Ethernet, Fibre Channel (FC),and Fibre Channel over Ethernet (FCoE)
- Connectivity options include 1 Gigabit Ethernet, 10 Gigabit Ethernet, 10 Gigabit Ethernet with FCoE, and 1/2/4/8G Native Fibre Channel
- Switch supports all Cisco Nexus 2000 Series Fabric Extenders

Cisco Nexus 5020 56-Port Switch

The Cisco Nexus 5020 Switch is a two rack-unit (2RU), 10 Gigabit Ethernet/FCoE access-layer switch built to provide 1.04 terabits per second (Tbps) throughput with very low latency. It has:

- Forty fixed 10-Gigabit Ethernet, Cisco Data Center Ethernet, and FCoE Small Form Factor Pluggable Plus (SFP+) ports. Sixteen of the forty fixed ports support both Gigabit Ethernet and 10-Gigabit Ethernet. The default is 10-Gigabit Ethernet.
- Two expansion module slots that can be configured to support up to 12 additional 10-Gigabit Ethernet, Cisco Data Center Ethernet, and FCoE SFP+ ports, up to 16 Fibre Channel switch ports, or a combination of both.
- Serial console port and an out-of-band 10/100/1000-Mbps Ethernet management port.
- 1+1 redundant, hot-pluggable power supplies.
- 4+1 redundant, hot-pluggable fan modules to provide reliable front-to-back cooling.

Cisco Nexus 5010 28-Port Switch

The Cisco Nexus 5010 Switch is a 1RU, 10 Gigabit Ethernet/FCoE access-layer switch built to provide more than 500 Gigabits per second (Gbps) throughput with very low latency. It has:

- Twenty fixed 10-Gigabit Ethernet, Cisco Data Center Ethernet, and FCoE Small Form Factor Pluggable Plus (SFP+) ports. Eight of the Twenty fixed ports support both Gigabit Ethernet and 10-Gigabit Ethernet.
- One expansion module slots that can be configured to support up to 6 additional 10-Gigabit Ethernet, Cisco Data Center Ethernet, and FCoE SFP+ ports, up to 8 Fibre Channel switch ports, or a combination of both.

- Serial console port and an out-of-band 10/100/1000-Mbps Ethernet management port.
- 1+1 redundant, hot-pluggable power supplies.
- 1+1 redundant, hot-pluggable fan modules to provide reliable front-to-back cooling.

Cisco Nexus 5000 Series Expansion Modules

The Cisco Nexus 5000 Series is equipped to support three expansion module options that can be used to increase the number of 10 Gigabit Ethernet/FCoE ports, connect to Fibre Channel SANs, or both. The Cisco Nexus 5010 supports a single module, with the Cisco Nexus 5020 supporting any combination of two modules from the following offerings:

- An Ethernet module that provides 6 10 Gigabit Ethernet/FCoE ports using an SFP+ interface.
- A Fibre Channel plus Ethernet module that provides 4 10 Gigabit Ethernet/FCoE ports using an SFP+ interface, and 4 ports of 1/2/4-Gbps native Fibre Channel connectivity using an SFP interface.
- A Fibre Channel module that provides 8 ports of 1/2/4-Gbps native Fibre Channel using an SFP interface for transparent connectivity with existing Fibre Channel networks.

Physical Specifications

SFP+ Optics

Cisco Nexus 5000 Series products support 10 Gigabit Ethernet SFP+ copper Twinax cables for short distances and SFP+ optics (10GBASE-SR and 10GBASE-LR) for longer distances. SFP+ has several advantages compared to other 10 Gigabit Ethernet connectivity options:

- Smallest 10 Gigabit Ethernet form-factor
- Optical interoperability with XENPAK, X2, and XFP interface types
- Lowest power consumption
- Hot-swappable device

SFP Optics

- Cisco Nexus 5000 Series products support Gigabit Ethernet SFP for Gigabit Ethernet connectivity options. The following SFP transceiver modules are supported in ports 1 to 8 of the Cisco Nexus 5010 and ports 1 to 16 of the Cisco Nexus 5020:
  - Cisco 1000BASE-T SFP
  - Cisco 1000BASE-SX SFP
  - Cisco 1000BASE-LX/LR SFP
- Cisco Nexus 5000 Series products support 4-Gbps Fibre Channel-compatible SFP for native Fibre Channel connectivity options; 4-Gbps Fibre Channel-compatible short-reach and 10-km long-reach SFP transceiver modules operate at 4/2/1 Gbps and are supported in the native Fibre Channel ports on expansion modules.

Fabric Extenders
The TOE includes the Cisco Nexus 2000 Series Fabric Extenders (2148T 2224TP, 2248TP, 2248TP-E, 2232PP, 2232TM, 2232TM-E, B22F, and B22HP Fabric Extenders). Each of these FEX models, when connected to a Nexus 5000 Series system, acts as a single managed entity, with the Cisco Nexus 5000 Series system providing the supervisory functions of the control plane and the Cisco FEX inheriting the characteristics of connected Cisco Nexus 5000 Series ports. The Cisco FEX supports the following features:

- Operation as a remote I/O module, extending the internal fabric of the Cisco Nexus 5010 and 5020 Switches for low-cost port-count expansion
- Zero-touch provisioning, including configuration and upgrade
- 48 Gigabit Ethernet server access ports with RJ-45 connectors
- Four 10 Gigabit Ethernet uplink ports using SFP+ short-reach (SR) and long-reach (LR) optical or CX1 directattach copper interconnects
- Compact 1RU form factor
- Front-to-back cooling compatible with data center hot-aisle and cold-aisle designs, with all switch ports at the rear of the unit in close proximity to server ports
- 1+1 redundant, hot-pluggable, dual-sensing power supplies
- Hot-swappable fan trays
- All user-serviceable components accessible from the front panel

Cisco Secure ACS
Cisco Secure Access Control Server (ACS) v5.2 Patch 10 is an access control server that operates as a centralized authentication server. The Cisco Secure ACS is an appliance that provides an identity-based access policy system for Cisco intelligent information networks. It is the integration and control platform for managing access policy for network resources. Cisco Secure ACS provides central management of access policies for both network access and device administration and supports a wide range of access scenarios including wireless LAN, 802.1x wired, and remote access. Cisco Secure ACS provides an authentication, authorization, and accounting (AAA) platform.

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. Data Plane Information Flow Control
    a. PACLs
    b. VACLs
    c. VRFs
2. Data Plane Information Flow Accountability
3. Secure Management
    a. Administrator Identification and Authentication
    b. Administrative Auditing

c. Administrative Authorization
d. Secure Management Communication
e. Authentication, Authorization, and Accounting (AAA)

4. Availability
   a. IP Source Guard
   b. Traffic Storm Control
   c. Control Plane Policing
   d. Rate Limiting
   e. DHCP Snooping – Dynamic ARP Inspection
   f. Cisco Fabric Services (CFS) provisioning

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

1.6.1 Data Plane Information Flow Control

The TOE provides the ability to control traffic flow into or out of the Nexus 5000 switch. The following types of traffic flow may be able to be controlled:

- Layer 2 Traffic – PACLs
- VLAN Traffic – VACLs
- VRFs

A PACL is an administratively configured access control list that is applied to Layer 2 traffic that is routed into Nexus 5000 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.

PACLs can filter ingress traffic filtered 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, Source MAC address, Destination MAC address, Protocol, Class of Service (COS), VLAN ID, Precedence, Packet Length, TTL, 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, Source MAC address, Destination MAC address, Protocol, Class of Service (COS), VLAN ID, Precedence, Packet Length, TTL, or DSCP value.

The TOE supports Virtual Routing and Forwarding (VRF). VRFs allow multiple instances of routing tables to exist within the Nexus 5000 switch TOE component simultaneously. The TOE implements two VRFs (management and default). 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.

1.6.1.1 ACL Hit Counters

An ACL consists of Access Control Entries (ACEs), each ACE specifying a traffic flow based on a filter (e.g. including Source IP address, Destination IP address) and whether or not to permit or deny that traffic flow. To determine if the traffic should be allowed or denied, each ACE is examined in the order as presented in the ACL. The first ACE that matches the attempted flow of traffic is considered a "hit" and determines whether or not the traffic is allowed or denied. Nexus 5000 has the ability to maintain counters on the hits encountered by each ACE.

These ACL hit counters can then be used by Nexus 5000 to optimize ACLs such that ACEs are re-ordered based upon the most popular hits bringing the most likely ACEs to encounter hits to the front of the ACL, thus improving performance by reducing the time it takes to encounter an hit in the ACL.. In performing this optimization, Nexus 5000 ensures the logic of the original order is not disturbed meaning that the re-ordering does not permit traffic to flow that would have not been permitted by the original order. If optimization analysis determines that the re-ordering would violate the logic of the original order, the ACL is not optimized.

1.6.2 Management Security

The TOE provides the ability to be securely administered.

1.6.2.1 Administrator Identification and Authentication

Users must be authenticated prior to gaining access to the administrative functionality of the Nexus 5000 switch TOE component. Administrative authentication options include remote authentication facilitated by the ACS TOE component as well as authentication against a database local to the Nexus 5000 appliance.

Users must be authenticated prior to gaining access to the administrative functionality of the ACS TOE component. ACS administrative users are authenticated by the ACS TOE component against a local ACS authentication database.

The ACS TOE component may optionally interface with an external LDAP, Active Directory, or another ACS server for authentication verification. Even in these cases, the ACS TOE component still provides the access decision and enforcement.

1.6.2.1.1 Authentication, Authorization, and Accounting (AAA)

To implement the use of external servers for authentication purposes, Nexus 5000 includes Authentication, Authorization, and Accounting (AAA) services. The AAA feature allows for external user verification, authority, and logging (can send audit information to the server).

The ACS TOE component is an AAA server that provides authentication services. The AAA services provided by the ACS server include local authentication as well as the use of external servers such as RADIUS and TACACS.

Authentication is verification of a user's identity and authorization determines what a user can do. The Nexus 5000 switch can be configured to perform one or both locally or by using one or more AAA servers. A preshared secret key provides security for communication between the Nexus 5000 switch and AAA servers. A common secret key can be configured for all AAA servers or for only a specific AAA server.

Microsoft Challenge Handshake Authentication Protocol (MSCHAP) is the Microsoft version of CHAP and can be used in the evaluated configuration for user logins to a Nexus 5000 Series switch through a remote authentication server (RADIUS or TACACS+).

The commands used to configure AAA can optionally be restricted on a user basis.

1.6.2.2 Administrative Auditing

The Nexus 5000 switch TOE component provides the ability to audit the actions taken by authorized administrators. Audited events include Start-up and shutdown, Configuration Changes, Administrative Authentication, and Administrative Log-off.

The ACS TOE component provides the ability to audit the actions taken by authorized administrators. Audited events include Start-up and shutdown, Configuration Changes, Administrative Authentication, and Administrative Log-off.

The TOE provides the capability for authorized administrators to review the audit records stored within the TOE. This is available with both the Nexus 5000 and ACS TOE components.

1.6.2.3 Administrative Authorization

The Nexus 5000 switch TOE component implements Role-based Access Control (RBAC) in providing a granular administration authorization framework for defining the exact Nexus 5000 administrative capabilities available to the user based on assigned role(s). Users may be assigned multiple roles. The Nexus 5000 switch supports two predefined roles, as follows:

- network-admin (aka superuser) – complete read and write access to the entire Nexus 5000 Series switch
- network-operator (aka operator) – complete read access to the Nexus Series switch

Authorized administrators of the Nexus 5000 and the ACS TOE component perform the user account management and user configuration for the users of each respective TOE component.

The ACS TOE component supports ten predefined GUI administrative role types as follows: ChangeAdminPassword, ChangeUserPassword, NetworkDeviceAdmin, PolicyAdmin, ReadOnlyAdmin, ReportAdmin, SecurityAdmin, SystemAdmin, UserAdmin, and SuperAdmin. The ACS TOE component also supports two CLI administrative roles, Admin and Operator.

1.6.2.4 Secure Management Communication

The TOE supplies secure communication channels through which the TOE is administered. The following table reflects the secure management channels provided by the TOE:

Table 1-6: Secure Management Communication

TOE Component	Secure Management Protocol
Nexus 5000 Switch TOE component	Secure Shell (SSH) Protocol version 2
	Simple Network Management Protocol version 3 (SNMPv3)
ACS TOE component	Secure Shell (SSH) Protocol version 2
	Transport Layer Security (TLS) 1.0
	Simple Network Management Protocol version 3 (SNMPv3)

The claimed cryptographic mechanism used to support the secure communication channels are not FIPS 140-2 validated. The vendor asserts the TOE implementation is compliant with the specific algorithms and methods specified. See Table 6-2 for further detail of the claimed cryptographic mechanisms.

1.6.3 Virtualization and Availability

The TOE provides several measures to help assure that Nexus 5000 switch is able to constantly provide the desired switching services. The TOE also provides several traffic control policies specifically to ensure that the TOE services are available to legitimate traffic.

1.6.3.1 Traffic Storm Control

Traffic Storm Control allows an administrative user to monitor the levels of the incoming traffic 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. When the ingress traffic reaches the Traffic Storm Control level that is configured on the port, Traffic Storm Control drops the traffic until the interval ends.

1.6.3.2 Control Plane Protection

The Control Plan Protection feature allows policing of control-plane traffic by classifying traffic into different categories. This feature requires no configuration and is statically implemented to protect the CPU ensuring the CPU is not overwhelmed as excessive traffic could overload the CPU and slow down the performance of the entire TOE.

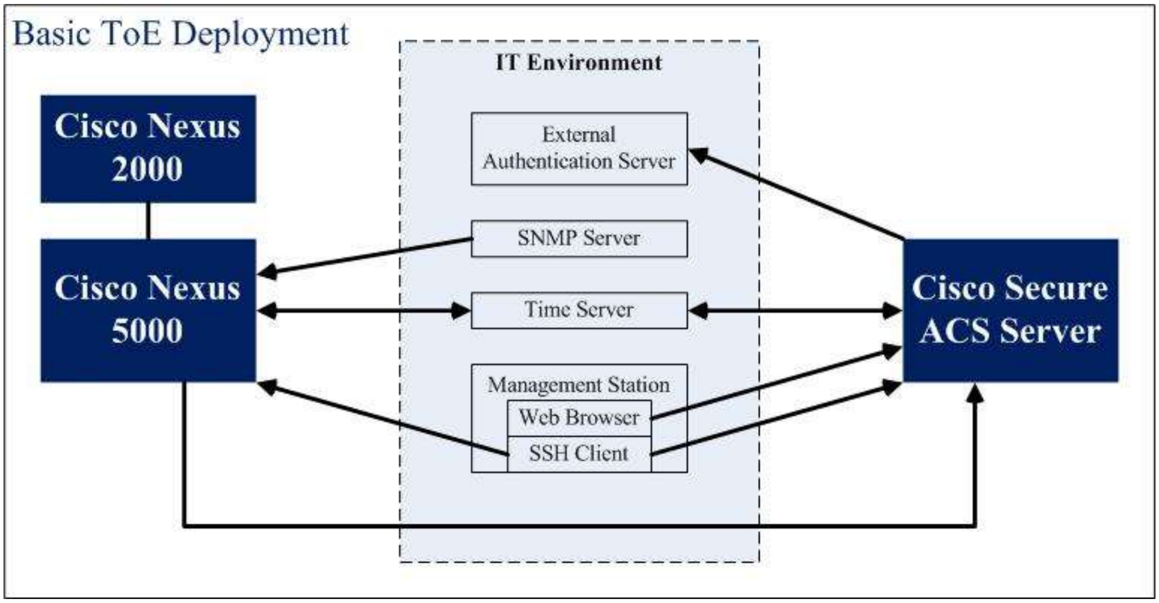
1.6.3.3 Private VLANs (PVLANs)

A VLAN on a network is a broadcast domain. All of the hosts on that VLAN can communicate with the other members of the same VLAN. PVLANs allow traffic to be segmented at the data-link layer (layer 2) of the OSI model, limiting the size of the broadcast domain. This additionally adds the ability to deny communications between hosts. PVLANs provide a mechanism to control which devices can communicate within a single subnet.

1.7 TOE Evaluated Configuration

The following figure provides a visual depiction of a typical TOE deployment:

Figure 1 TOE Deployment



The figure above includes the following:

- One or more Nexus 5000 switch (TOE components)
- ACS (TOE component)
- 2000 Series Fabric Extender Appliance (ToE Component)
- Management Station (IT environment)
- Web Browser (IT environment)
- SSH Client (IT environment)
- SNMP Server (IT environment)

1.7.1 Excluded Functionality

No functionality is excluded from the evaluation.

1.8 TOE Bypass and interference/logical tampering Protection Measures

Both the Nexus 5000 switch and ACS TOE components are hardware platforms in which all operations in the TOE scope are protected from interference and tampering by untrusted subjects. All administration and configuration operations are performed within the physical boundary of the TOE. 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 CLI, GUI, or SNMPv3 interfaces. There are no undocumented interfaces for managing the product.

All cards included in the TOE rely on the main Nexus 5000 switch for power, memory management, and access control. In order to access any portion of the Nexus 5000 switch, the Identification & Authentication mechanisms of the Nexus 5000 switch must be invoked and succeed. The same is true for the ACS portion of the TOE.

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 5000 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 5000 switch TOE component are not able to affect.

The Nexus 5000 switch provides a secure domain for each VRF to operate within. The TOE has two VRFs (management and default). Each VRF has its own resources that other VRFs within the same Nexus 5000 switch TOE component are not able to affect.

Finally, the Nexus 5000 switch enforces ACLs and applies other network traffic security at its interfaces before traffic passes into or out of the switch. The TOE controls every ingress and egress traffic flow. Policies are applied to each traffic flow. The TOE includes protections against various attacks, including traffic burst. The information flow defenses built into the TOE to counter this type of attack Traffic Storm Policies.

There are no unmediated traffic flows into or out of either component of the TOE (Nexus 5000 switch or ACS). The information flow policies identified in the SFRs are applied to all traffic received and sent by the Nexus 5000 TOE component. The ACS TOE component only accepts mediated administrative traffic and AAA related traffic. Each communication including data plane communication, control plane communications, and administrative communications are mediated by the TOE. There is no opportunity for unaccounted traffic flows to flow into or out of the TOE.

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.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

This TOE conforms to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 2, September 2007.
    - Part 2 conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, Revision 2, September 2007.
    - Part 3 conformant
- Package Conformance:
    - Evaluation Assurance Level 4 (EAL 4) augmented with ALC_FLR.2

2.2 Protection Profile Conformance

This ST does not claim compliance to any Common Criteria validated Protection Profiles.

3 SECURITY PROBLEM DEFINITION

This chapter identifies the following:

- Significant assumptions about the TOE's operational environment.
- IT related threats to the organisation countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.
- Organisational 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. Policies are identified as P.policy with "policy" specifying a unique name.

3.1 Assumptions

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

Table 3-1: TOE Assumptions

Assumption Name	Assumption Definition
A.PROTCT	The TOE hardware and software will be protected from unauthorized physical modification.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be physically accessed by authorized users.

3.2 Threats

Table 3-2 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 3-2: Threats

Threat Name	Threat Definition
T.AVAIL	An attacker may prevent the availability of Nexus 5000 switch services by attacking the switch using network based attacks.
T.NETTRAFFIC	An unauthorized user may send network traffic to unauthorized destinations

Threat Name	Threat Definition
	through the Nexus 5000 switch without detection.
T.IMPCONF	The TOE may be susceptible to improper configuration by an authorized or unauthorized person causing potential intrusions to go undetected.
T.ADMINAUTHOR	An authorized administrative user may either intentionally or unintentionally gain access to the configuration services for which the user is not authorized.
T.ADMINAUDIT	An authorized or unauthorized administrative user may make configuration changes to the Nexus 5000 switch without being detected.
T.AUDITCOMP	An attacker may compromise the integrity of the TOE audit data.
T.ADMINTRAF-C&I	An attacker may view or modify TOE administrative traffic without detection.
T.VRFCOMP	An attacker may be able to cause traffic to be forwarded inappropriately through the TOE by sending traffic through the VRFs on the Nexus 5000 switch.

3.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. Table 11: Organizational Security Policies identifies the organizational security policies

Table 3-3: Organizational Security Policies

Policy Name	Policy Definition
P.ACCOUNTABLE	Users shall be accountable for their actions on the protected network and 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 table below 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 4-1: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.Nexus5KAvail	The TOE shall ensure the availability of its services even when subjected to network traffic based attacks.
O.DataFlowControl	The TOE shall ensure that only authorized traffic is permitted to flow through the TOE to its destination.
O.Admin	The TOE shall include a set of functions that allow effective management of its functions and data.
O.AdminAuth	The TOE shall be able to identify and authenticate authorized administrators prior to allowing access to TOE functions and data.
O.AdminAccess	The TOE shall allow authorized administrative users to access only appropriate TOE functions and data.
O.Audit	The TOE shall record audit records for PACLs, VACLs and administrative actions.
O.AuditIntegrity	The TOE shall ensure the integrity of all audit data.
O.SecureMgtComm	The TOE shall ensure that management communication to the TOE is protected from unauthorized disclosure or modification.
O.VRFSec	The TOE shall provide VRFs and ensure that traffic received by the Nexus 5000 switch is only forwarded in a manner consistent with the VRF for which the traffic is associated.

4.2 Security Objectives for the Environment

The assumptions identified in Section 3.1 are incorporated as security objectives for the environment. They levy additional requirements on the environment, which are largely satisfied through procedural or administrative measures. Table 4-2: Security Objectives for the Environment identifies the security objectives for the environment.

Table 4-2: Security Objectives for the Environment

Environment Security Objective Name	IT Environment Security Objective Definition
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE (includes the Nexus 5000 switch, 2000 Fabric Extenders and ACS TOE components).
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE. PHYCAL	Those responsible for the TOE must ensure that the TOE is protected from any physical attack.
OE.TIME	The environment shall optionally provide reliable timestamps to the TOE.

4.3 Security Objectives Rationale

This section demonstrates that the identified security objectives are covering all aspects of the security needs. This includes showing that each threat, assumption, or policy is addressed by a security objective. Table 14 and Table 15 provide the mapping and rationale for the security objectives identified in Chapter 4 and the assumptions, threats and policies identified in Chapter 3.

Table 4-3: How Security Objectives Map to Threats, Assumptions, and OSPs

	O.Nexus5KAvail	O.DataFlowControl	O.Admin	O.AdminAuth	O.AdminAccess	O.Audit	O.AuditIntegrity	O.SecureMgtComm	OE.PERSON	OE.INSTALL	OE. PHYCAL	OE.TIME	O.VRFSec
A.PROTCT										X	X		
A.LOCATE										X	X		
A.MANAGE									X				
A.NOEVIL									X				
A.NOTRST											X		
T.AVAIL	X												
T.NETTRAFFIC		X				X							
T.IMPCONF			X		X								
T.ADMINAUTHOR			X	X	X								
T.ADMINAUDIT						X							
T.AUDITCOMP							X						
T.ADMINTRAF-C&I								X					
T.VRFCOMP													X
P.ACCOUNTABLE						X						X	

Table 4-4: Security Objectives Map to Threats, Assumptions, and OSPs Rationale

Threat/Assumption	Objective	Rationale
A.PROTCT	OE. PHYCAL	This objective helps to cover the assumption by having the administrators in charge of the ongoing deployment of the TOE ensure that it is protected.
	OE.INSTALL	This objective helps to cover the assumption by having the administrators in charge of the installation of the TOE ensure that it is protected during the installation process.
A.LOCATE	OE. PHYCAL	This objective helps to cover the assumption because the responsible administrators will work to maintain the physical security of the TOE after installation.
	OE.INSTALL	This objective helps to cover the assumption because the responsible administrators will choose a physically secure location to deploy the TOE.
A.MANAGE	OE.PERSON	This objective will cover the assumption because the criteria used to select the TOE administrator will be consistent with that of a competent individual.
A.NOEVIL	OE.PERSON	This objective will cover the assumption because the criteria used to select the TOE administrator will be consistent with that of a careful individual that is not careless, willfully negligent, or hostile.
A.NOTRST	OE. PHYCAL	The objective will cover the assumption because the personnel who are choosing the location of the TOE will select a location that only allows access by authorized administrators.
T.AVAIL	O.Nexus5KAvail	This threat is countered because this objective provides a series of measures implemented by the TOE to protect against attacks that would compromise the availability of Nexus 5000 switch services.
T.NETTRAFFIC	O.DataFlowControl	This objective helps to counter this threat by providing control over the data plane information flows to and from the Nexus 5000. This prevents unauthorized traffic flows.
	O.Audit	This objective helps to counter this threat by providing audit records that are viewable by the administrative users of the TOE. These audit records include records of when network traffic matches a configured ACL. This allows the administrator to view attempts by unauthorized entities to send information to unauthorized destinations.
T.IMPCONF	O.Admin	This objective helps to mitigate this threat by providing all of the functionality necessary to securely manage the TOE.
	O.AdminAccess	This object helps to mitigate this threat by ensuring that administrators do not have access to administrative resources they should not have access to. This prevents an authorized administrator from accidentally misconfiguring a

Threat/Assumption	Objective	Rationale
		functionality for which they should not have access.
T.ADMINAUTHOR	O.Admin	This objective helps to counter this threat by providing the administrative functions needed to securely manage the TOE.
	O.AdminAccess	This objective helps to counter this threat by providing that TOE administrator only have access to the administrative functionality associated with his or her assigned role. This prevents administrators from misconfiguring portions of the TOE for which they should not have access.
	O.AdminAuth	This objective helps to counter this threat by providing identification and authentication functionality to determine who the potential administrator is. After the administrator is identified and authenticated, the TOE can ensure that the administrator is only granted access to the administrative functionality consistent with his or her assigned role.
T.ADMINAUDIT	O.Audit	This objective counters this threat by providing that the TOE generates audit records for each configuration change. There is no way for anyone to make changes without others knowing because there is an audit record reflecting the change.
T.AUDITCOMP	O.AuditIntegrity	This objective counters this threat by providing that the TOE has mechanisms that will protect the integrity of the audit records stored internally to the TOE.
T.ADMINTRAF-C&I	O.SecureMgtComm	This objective counters this threat by providing that the TOE provides a mechanism for secure management communications. These protected management communications prevent unauthorized disclosure or modification of administrative traffic.
T.VRFCOMP	O.VRFSec	This objective counters this threat by ensuring that VRFs operate in a self-contained environment. This prevents compromise of one VRF to affect the operation of another VRF.
P.ACCOUNTABLE	O.Audit	This objective upholds this policy by providing the TOE with the means to create audit records that record actions made on the network. The administrators of the TOE can review these audit records to learn the actions of network entities.
	OE.TIME	This objective upholds this policy by providing an optional environment supplied time stamp that can be used in the audit records generated by the TOE. These timestamps give the administrators of the TOE an understanding of when events occurred.

5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived verbatim from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 2* and all National Information Assurance Partnership (NIAP) and international interpretations.

5.1 Conventions

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

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

5.2 Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in Table 5-1 are described in more detail in the following subsections.

Table 5-1: Security Functional Requirements

Functional Component	
SFR Component ID	**Component Name**
Security Functional Requirements Directly Drawn from CC Part 2	
FAU_GEN.1	Audit data generation
FAU_SAR.1(1)	Audit review-Nexus 5000 Related Logging
FAU_SAR.1(2)	Audit review- ACS Administrative Auditing
FAU_STG.1	Protected audit trail storage
FCS_CKM.1(1)	Cryptographic key generation-RSA
FCS_CKM.1(2)	Cryptographic key generation-SNMPv3
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1(1)	Cryptographic operation-RSA E/D
FCS_COP.1(2)	Cryptographic operation-AES E/D
FCS_COP.1(3)	Cryptographic operation- Triple DES E/D
FCS_COP.1(4)	Cryptographic operation-SHS Hashing
FCS_COP.1(5)	Cryptographic operation- MD5 Hashing
FCS_COP.1(6)	Cryptographic operation-DSA Signature Services
FCS_COP.1(7)	Cryptographic operation- Diffie-Hellman Key Establishment
FDP_IFC.1(1)	Subset information flow control/ACLs
FDP_IFC.1(2)	Subset information flow control /PVLAN
FDP_IFF.1(1)	Simple security attributes /ACLs
FDP_IFF.1(2)	Simple security attributes /PVLAN
FIA_UAU.1(1)	Timing of authentication /N5K Switch administrator
FIA_UAU.1(2)	Timing of authentication /ACS Administrator
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.1(1)	Timing of identification/ N5K Switch administrator
FIA_UID.1(2)	Timing of identification /ACS Administrator

Functional Component	
FMT_MSA.1(1)	Management of security attributes-ACLs Policy
FMT_MSA.1(2)	Management of security attributes-PVLAN Policy
FMT_MSA.3(1)	Static attribute initialisation-ACLs Policy
FMT_MSA.3(2)	Static attribute initialisation - PVLAN Policy
FMT_MTD.1(1)	Management of TSF data-N5K data
FMT_MTD.1(2)	Management of TSF data-ACS-Data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_STM.1	Reliable time stamps

5.2.1 TOE Security Functional Requirements

5.2.1.1.1 FAU_GEN.1 Audit data generation

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

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [not specified] level of audit; and
c) [

- *Configuration Changes on the Nexus 5000 switch;*
- *Administrative Authentication on the Nexus 5000 switch;*
- *Administrative Log-off on the Nexus 5000 switch;*
- *Configuration Changes on the ACS TOE component;*
- *Administrative Authentication on the ACS TOE component;*
- *Administrative Log-off on the ACS TOE component*].

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, [*audit relevant information defined in the table below*].

Table 5-2: ACL Audit Information

Audited Action	Recorded Information
Configuration Changes on the Nexus 5000 switch	Day of Week, Date, Action, User, status of the configuration change, terminal information (when applicable)
Administrative Authentication on the Nexus 5000 switch	Day of Week, Date, Action, User, terminal information (when applicable)
Administrative Log-off on the Nexus 5000 switch	Day of Week, Date, Action, User, terminal information (when applicable)
Configuration Changes on ACS	User ID, Interface on which the action took place (CLI or GUI), Time and Date, the action that took place, the new value for configuration changes (except when the new

Audited Action	Recorded Information
	value is security relevant – for example, passwords)
Administrative Authentication on ACS	User ID, Interface on which the action took place (CLI or GUI), Time and Date, the action that took place,
Administrative Log-off ACS	User ID, Interface on which the action took place (CLI or GUI), Time and Date, the action that took place,

Hierarchical to: No other components.
Dependencies: FPT_STM.1

5.2.1.1.2 FAU_SAR.1(1) Audit review – Nexus 5000 Related Logging

FAU_SAR.1.1(1) The TSF shall provide [*network-admin, network-operator, Administrator defined role(s)*] with the capability to read [*the following:*

- *network-admin and network-operator can read all information within the audit records stored within the Nexus 5000.*
- *Administrator defined role(s) can read all information within the audit records (consistent with the role definition)*]

from the audit records.

FAU_SAR.1.2(1) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Hierarchical to: No other components.
Dependencies: FAU_GEN.1

5.2.1.1.3 FAU_SAR.1(2) Audit review – ACS Administrative Auditing

FAU_SAR.1.1(2) The TSF shall provide *[SuperAdmin (ACS Predefined role), MachineAdmin (ACS Predefined role), and any administratively defined ACS role with audit read capabilities*] with the capability to read [*the ACS Administrative Audit Records*] from the audit records.

FAU_SAR.1.2(2) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Hierarchical to: No other components.
Dependencies: FAU_GEN.1

5.2.1.1.4 FAU_STG.1 Protected audit trail storage

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

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

Hierarchical to: No other components.

Dependencies: FAU_GEN.1

5.2.1.1.5 FCS_CKM.1(1) Cryptographic key generation – RSA

FCS_CKM.1.1(1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*RSA key generation*] and specified cryptographic key sizes [*1024-bits, and 2048-bits*] that meet the following: [*FIPS 186-3*].

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 or FCS_COP.1], FCS_CKM.4

Application Note: The TOE provides RSA Key Generation for the following purposes:

Table 5-3: Cryptographic Key Generation Provided by the TOE (RSA)

Usage	Purpose
TLS Key Generation (ACS)	Key used to protect a TLS session.
SSH Key Generation (both)	Key used to protect a SSH session.

5.2.1.1.6 FCS_CKM.1(2) Cryptographic key generation - SNMPv3

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*password to key using the SHA algorithm discussed in RFC 3414*] and specified cryptographic key sizes [*64, 128, 192, and 256 bits*] that meet the following: [*RFC 3414*].

Hierarchical to: No other components.
Dependencies: [FCS_CKM.2 or FCS_COP.1], FCS_CKM.4

Application Note: The TOE provides SHA Key Generation for the following purposes:

Table 5-4: Cryptographic Key Generation Provided by the TOE (SNMPv3)

Usage	Purpose
SNMPv3 Tunnel Teardown (N5k)	Key used to protect a SNMPv3 session.

5.2.1.1.7 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 [*overwrite*] that meets the following: [*FIPS 140-2 key zeroization requirements*]

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]

Application Note: The TOE provides cryptographic key destruction for the following purposes:

Table 5-5: Cryptographic Key Destruction Provided by the TOE

Usage	Purpose
SSH Tunnel Teardown (both)	After TOE administration via SSH is completed, the tunnel is torn down and the session key is overwritten.

Usage	Purpose
SNMPv3 Tunnel Teardown (N5k)	After TOE administration via SNMPv3 is completed, the tunnel is torn down and the key is overwritten.
TLS Tunnel Teardown (ACS)	After TOE administration via TLS is completed, the tunnel is torn down and the session key is overwritten.

5.2.1.1.8 FCS_COP.1(1) Cryptographic operation – RSA E/D

FCS_COP.1.1(1) The TSF shall perform [*Encryption/Decryption*] in accordance with a specified cryptographic algorithm [*RSA*] and cryptographic key sizes [*1024-bits and 2048-bits*] that meet the following: *[FIPS 186-2*].

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4

Application Note: The TOE provides RSA encryption and decryption for the following purposes:

Table 5-6: RSA Encryption/Decryption Provided by the TOE

Usage	Purpose
TLS (ACS)	This provides the asymmetric encryption used as part of the session setup process for TLS communications.
SSH (both)	This provides the asymmetric encryption used as part of the session setup process for SSH communications.

5.2.1.1.9 FCS_COP.1(2) Cryptographic operation – AES E/D

FCS_COP.1.1(2) The TSF shall perform [*Encryption/Decryption*] in accordance with a specified cryptographic algorithm [*Advanced Encryption Standard (AES in CBC mode)*] and cryptographic key sizes [*128-bits*] that meet the following: [*FIPS 197*].

Application Note: The TOE provides AES encryption and decryption for the following purposes:

Table 5-7: AES Encryption/Decryption Provided by the TOE

Usage	Purpose
SSH (both)	This provides the protection for SSH based administrative communication.
SNMPv3 (N5k)	Provides data protection using symmetric encryption and decryption for SNMPv3 communications.
TLS (ACS)	Provides data protection using symmetric encryption and decryption for TLS communications.

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4

5.2.1.1.10 FCS_COP.1(3) Cryptographic operation –Triple-DES E/D

FCS_COP.1.1(3) The TSF shall perform [*Encryption/Decryption*] in accordance with a specified cryptographic algorithm [*Triple-DES in CBC mode*] and cryptographic key sizes [*168-bits*] that meet the following: [*FIPS 46-3*].

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4

Application Note: The TOE provides Triple-DES encryption and decryption for the following purposes:

Table 5-8: Triple-DES Encryption/Decryption Provided by the TOE

Usage	Purpose
SSH (both)	Provides data protection using symmetric encryption and decryption for SSH communications.
SNMPv3 (N5k)	Provides data protection using symmetric encryption and decryption for SNMPv3 communications.
TLS (ACS)	Provides data protection using symmetric encryption and decryption for TLS communications.

5.2.1.1.11 FCS_COP.1(4) Cryptographic operation - SHS Hashing

FCS_COP.1.1(4) The TSF shall perform [*Hashing*] in accordance with a specified cryptographic algorithm [*Secure Hash Standard (SHS)*] and cryptographic key sizes [*N/A*] that meet the following: [*FIPS 180-2*].

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4

Application Note: The TOE provides SHS hashing for the following purposes:

Table 5-9: SHS Hashing Provided by the TOE

Usage	Purpose
TLS (ACS)	Provides the hashing required as part of the TLS session establishment protocol.
SNMPv3 (N5k)	Provides the hashing required as part of the SNMPv3 session establishment.

5.2.1.1.12 FCS_COP.1(5) Cryptographic operation – MD5 Hashing

FCS_COP.1.1(5) The TSF shall perform [*secure hash (message digest)*] in accordance with a specified cryptographic algorithm: [*MD5*] and cryptographic key sizes [*128-bit hash value*] that meet the following: [*RFC 1321*].

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4

Application Note: The TOE provides MD5 Hashing for the following purposes:

Table 5-10: MD5 Hashing Provided by the TOE

Usage	Purpose
TACACS+ (both)	Provides the hashing protection required by the TACACS+ protocol
RADIUS (both)	Provides the hashing protection required by the RADIUS protocol
SNMPv3 (N5k)	Provides the hashing for SNMPv3 communication.

5.2.1.1.13 FCS_COP.1(6) Cryptographic operation – DSA Signature Services

FCS_COP.1.1(6) The TSF shall perform [*cryptographic signature services*] in accordance with a specified cryptographic algorithm [*DSA*] and cryptographic key sizes [*1024-bits*] that meet the following: [*FIPS 186-2*].

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4
Application Note: The TOE provides DSA signature services for the following purposes:

Table 5-11: DSA Encryption/Decryption Provided by the TOE

Usage	Purpose
SSH (N5k)	This provides the signature services used as part of the session setup process for SSH communications.

5.2.1.1.14 FCS_COP.1(7) Cryptographic operation – Diffie-Hellman Key Establishment

FCS_COP.1.1(7) The TSF shall perform [key agreement] in accordance with a specified cryptographic algorithm [Diffie-Hellman] and cryptographic key sizes [*768-bits to 2048-bits*] that meet the following: [*RFC 2631*].

Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4

Application Note: The TOE provides Diffie-Hellman Key Agreement for the following purposes:

Table 5-12: Diffie-Hellman Key Agreement Provided by the TOE

Usage	Purpose
DH-CHAP (ACS)	Diffie-Hellman Challenge Handshake Authentication Protocol.

5.2.1.1.15 FDP_IFC.1(1) Subset information flow control/ACLs

FDP_IFC.1.1(1) The TSF shall enforce the [*ACLs Policy*] on
[*Subjects:*

- *Nexus 5000 interfaces*
    - *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*
    - *Management interfaces*
    - *Layer 2 interfaces*
    - *Layer 2 Ethernet port-channel interfaces*
- *Source Network Device*

- ♦ *Destination Network Device*

Information:

- ♦ *Network Traffic*
  - ▪ *IP Packets*
  - ▪ *Non-IP Packets*

Operations:

- ♦ *pass information*].

Hierarchical to: No other components.
Dependencies: FDP_IFF.1

5.2.1.1.16 FDP_IFC.1(2) Subset information flow control/PVLAN

FDP_IFC.1.1(2) The TSF shall enforce the [*PVLAN Policy*] on
[*Subjects:*

- ♦ *Nexus 5000 interfaces*
  - ▪ *PVLAN interfaces*

Information:

- ♦ *Network Traffic*
  - ▪ *IP Packets*

Operations:

- ♦ *pass information*].

Hierarchical to: No other components.
Dependencies: FDP_IFF.1

5.2.1.1.17 FDP_IFF.1(1) Simple security attributes

FDP_IFF.1.1(1) The TSF shall enforce the [*ACLs Policy*] based on the following types of subject and information security attributes:

[*Subject security attributes:*

- ♦ *Nexus 5000 interfaces*
  - ▪ *Traffic Storm threshold, PACL/VACL policies, and minimal access policy configured for the Nexus 5000 interfaces*

Information security attributes: Network Traffic

- ♦ *IP Packets*
  - ▪ *Source IP address*
  - ▪ *Destination IP address*
  - ▪ *Source port number*
  - ▪ *Destination port number*
  - ▪ *Protocol*
  - ▪ *ICMP message type*
  - ▪ *ICMP message code*
  - ▪ *IGMP message type*

- *Precedence*
- *DSCP Value*

- *Non-IP Packets*
  - *Source MAC address*
  - *Destination MAC address*
  - *Protocol*
  - *Class of Service (COS)*
  - *VLAN ID*
  - *Traffic Type: Broadcast Traffic, Unicast Traffic, Multicast Traffic].*

FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*Network traffic is processed by the TOE according to administratively configured policies in the following order:*

1. *Traffic Storm*
2. *PACL MAC ACLs*
3. *VRFs*
4. *VACL IP/MAC ACLs*

The specific information flow control rules associated with each policy are as follows:

- *Traffic Storm*
  - *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*
- *PACL MAC ACLs*
  - *Ingress IP traffic with security attributes that match an administratively configured PACL permit policy rule is allowed to flow, or,*
  - *Ingress IP traffic with security attributes that match an administratively configured PACL deny policy rule is not permitted.*

    The PACL permit/deny polices for IP traffic are comprised of a combination of subject security attributes and information attributes and a permit/deny operation. The subject attributes that are available for the creation of PACL permit/deny policies include: slot, port, and port-channel. The information attributes that are available for the creation of PACL permit/deny policies for IP traffic include: Source IP address, Destination IP address, Source port *number, Destination port number, Protocol, ICMP message type, ICMP message code, IGMP message type, Precedence, DSCP Value.*

  - *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 polices for non-IP traffic are comprised of a combination of subject security attributes and information attributes and a permit/deny operation. The subject attributes that are available for the creation of PACL permit/deny policies include: slot, port, and port-channel. The information attributes that are available for the creation of PACL permit/deny policies for non-IP traffic include: Source MAC address, Destination MAC address, Protocol, Class of Service (COS), VLAN ID, and traffic type.

- ♦ *VRFs*
  - *IP traffic with security attributes that map to a configured VRF will be forwarded through the Nexus 5000 switch TOE component per the VRF routing table*
- ♦ *VACL IP/MAC ACLs*
  - *IP traffic with security attributes that match an administratively configured permit policy rule is allowed to flow*
  - *IP traffic with security attributes that match an administratively configured deny policy rule is not permitted to flow.*
  - *The permit/deny polices for IP traffic are comprised of a combination of subject security attributes and information attributes and a permit/deny operation. The subject attributes that are available for the creation of permit/deny policies include: vlan-ID. The information attributes that are available for the creation of 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, Precedence, DSCP Value*
  - *Non-IP traffic with security attributes that match an administratively configured permit policy rule is allowed to flow,*
  - *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 deny policy rule is not permitted to flow.*

    The permit/deny polices for non-IP traffic 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 policies include: vlan-ID. The information attributes that are available for the *creation of these permit/deny policies include: Source MAC address, Destination MAC address, Protocol, Class of Service (COS), or VLAN ID***]**

FDP_IFF.1.3(1) The TSF shall enforce the **[***following:*

- *DHCP requests are allowed to flow through the TOE during authentication***]**

FDP_IFF.1.4(1) The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on the following rules: [

For IP Network Traffic Flows:

- *For IP traffic, if the security attributes do not match an administratively configured 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 PACL or VACL, the traffic flow is denied*].

Hierarchical to: No other components.
Dependencies: FDP_IFC.1, FMT_MSA.3

5.2.1.1.18 FDP_IFF.1(2) Simple security attributes/PVLAN

FDP_IFF.1.1(2) The TSF shall enforce the [*PVLAN policy*] based on the following types of subject and information security attributes:
[*Nexus 5000 Interfaces (subject) security attributes:*

- *Receiving/transmitting PVLAN port*

Information security attributes:

- *PVLAN port designation]*

FDP_IFF.1.2(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 transmitting and receiving port type allow the information flow as follows:

- *A promiscuous port will forward traffic from any port on the same PVLAN.*
- *A community port can forward traffic to a promiscuous port or a port on the same community.*
- *An Isolated port can only forward traffic to promiscuous ports***].**

FDP_IFF.1.3(2) The TSF shall enforce the [*none*].

FDP_IFF.1.4(2) The TSF shall explicitly authorise an information flow based on the following rules: [*none*].

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on the following rules: [*none*].

Hierarchical to: No other components.
Dependencies: FDP_IFC.1, FMT_MSA.3

5.2.1.1.19 FIA_UAU.1(1) Timing of authentication – Nexus 5000 Switch Administrator Authentication

FIA_UAU.1.1(1) The TSF shall allow [*establishment of a secure remote session between the administrative user and the Nexus 5000 Switch TOE component*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2(1) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Hierarchical to: No other components.
Dependencies: FIA_UID.1

5.2.1.1.20 FIA_UAU.1(2) Timing of authentication – ACS Administrator Authentication

FIA_UAU.1.1(2) The TSF shall allow [*establishment of a secure remote session between the administrative user and the ACS TOE Component*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2(2) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Hierarchical to: No other components.
Dependencies: FIA_UID.1

5.2.1.1.21 FIA_UAU.5 Multiple authentication mechanisms – Nexus 5000 Switch Administrator

FIA_UAU.5.1 The TSF shall provide [*the following authentication mechanisms:*

a) Remote authentication (facilitated by RADIUS or TACACS+ (provided by the ACS TOE component));

b) Authentication against a database local to the Nexus 5000 switch]

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **following: [**

a) *For Remote authentication facilitated by RADIUS or TACACS+, and Authentication scheme;*

b) *For Authentication against a database local to the Nexus 5000 switch, the TSF will authenticate the administrator based on the administratively configured Identification and Authentication scheme*].

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

5.2.1.1.22 FIA_UID.1(1) Timing of identification – Nexus 5000 Switch Administrator Identification

FIA_UID.1.1(1) The TSF shall allow [*establishment of a secure remote session between the administrative user and the Nexus 5000 Switch TOE component*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2(1) The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

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

5.2.1.1.23 FIA_UID.1(2) Timing of identification – ACS Administrator Identification

FIA_UID.1.1(2) The TSF shall allow [*establishment of a secure remote session between the administrative user and the ACS TOE component*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2(2) The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

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

5.2.1.1.24 FMT_MSA.1(1) Management of security attributes – ACLs Policy

FMT_MSA.1.1(1) The TSF shall enforce the [*ACLs Policy*] to restrict the ability to [*read, write*] the security attributes [*defined within administratively configured ACLs policy rules*] to [*the roles/operations defined in the following table*].

Table 5-13: Role/Operations Associated with ACLs

Role	Operations
network-admin (Resident on the Nexus 5000 Switch)	read, write operations for all security attributes defined within administratively configured ACLs policy rules.

network-operator (Resident on the Nexus 5000 Switch)	Read operations for all security attributes defined within administratively configured ACLs policy rules.
Administrator defined role(s) (Resident on the Nexus 5000 Switch)	read, write operations consistent with the role definitions.
Administrator defined role(s) (Resident on the ACS TOE component)	Query, modify, and delete operations consistent with the role definitions (GUI).

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1

5.2.1.1.25 FMT_MSA.1(2) Management of security attributes – PVLAN Policy

FMT_MSA.1.1(2) The TSF shall enforce the [*PVLAN Policy*] to restrict the ability to [*read, write*] the security attributes [*defined within administratively configured PVLAN*] to [*the roles/operations defined in the following table*].

Table 5-14: Role/Operations Associated with PVLAN

Role (Resident on the Nexus 5000 Switch)	Operations
network-admin	read, write operations for all role definitions associated with commands, features, and groups .
network-operator	read operations for all role definitions associated with commands, features, and groups.
Administrator defined role(s)	Read, write operations consistent with the role definitions.

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_SMR.1, FMT_SMF.1

5.2.1.1.26 FMT_MSA.3(1) Static attribute initialisation – ACLs Policy

FMT_MSA.3.1(1) The TSF shall enforce the [*ACLs Policy*] to provide [restrictive] default values for security attributes that are used to enforce the Policy.

FMT_MSA.3.2(1) The TSF shall allow the [*network-admin*] to specify alternative initial values to override the default values when an object or information is created.

Hierarchical to: No other components.
Dependencies: FMT_MSA.1, FMT_SMR.1

5.2.1.1.27 FMT_MSA.3(2) Static attribute initialisation –PVLAN Policy

FMT_MSA.3.1(2) The TSF shall enforce the [*PVLAN Policy*] to provide [restrictive] default values for security attributes that are used to enforce the Policy.

FMT_MSA.3.2(2) The TSF shall allow the [*network-admin*] to specify alternative initial values to override the default values when an object or information is created.

Hierarchical to: No other components.
Dependencies: FMT_MSA.1, FMT_SMR.1

5.2.1.1.28 FMT_MTD.1(1) Management of TSF data – Nexus 5000 Data

FMT_MTD.1.1(1) The TSF shall restrict the ability to [[read, write]] the *[the TSF Data described in the table below*] to [*the roles identified in the table below*].

Table 5-15: Role/Operations/TSF Data

Role	Operation	TSF Data
network-admin	Read, write	All Nexus 5000 configuration data. This includes cryptographic related Nexus 5000 configuration data.
network-operator	read	All Nexus 5000 configuration data. This includes cryptographic related Nexus 5000 configuration data.
Administratively configured Nexus 5000 roles with “read” privileges	Read	Nexus 5000 configuration data which can be read by the commands, features, and feature groups for which the role is authorized to access. This includes cryptographic related Nexus 5000 configuration data.
Administratively configured Nexus 5000 roles with “write” privileges	Write	Nexus 5000 configuration data which can be written by the commands, features, and feature groups for which the role is authorized to access. This includes cryptographic related Nexus 5000 configuration data.

Hierarchical to: No other components.
Dependencies: FMT_SMR.1, FMT_SMF.1

5.2.1.1.29 FMT_MTD.1(2) Management of TSF data – ACS Data

FMT_MTD.1.1(2) The TSF shall restrict the ability to [query, modify, delete] the *[the TSF Data described in the table below*] to [*the roles identified in the table below*].

Table 5-16: Role/Operations/TSF Data

Role	Operation	TSF Data
ChangeAdminPassword	Query	Administrator data
	Modify	Administrator passwords
ChangeUserPassword	Query	User data
	Modify	User passwords
NetworkDeviceAdmin	Query, Modify, Delete	Network Device Configuration Data on the ACS TOE component; Definition of external servers and RADIUS servers.
	Query,	ACS Network Device Group Configuration Data

Role	Operation	TSF Data
		on the ACS TOE component
Policy Admin (GUI role)	Query, Modify, Delete	Policy related Configuration Data on the ACS TOE component
	Query, Modify, Delete	Services related Configuration Data on the ACS TOE component NOTE: Services refer to which authentication services are available (or unavailable).
ReadOnlyAdmin (GUI role)	Query	All ACS Configuration Data on the ACS TOE component
ReportAdmin (GUI role)	Query	Audit logs on the ACS TOE component
SecurityAdmin (GUI role)	Query, Modify, Delete	ACS administrative user configuration related Configuration Data on the ACS TOE component.
System Admin (GUI role)	Query, Modify, Delete	ACS system administration related Configuration Data on the ACS TOE component NOTE: ACS system administration refers to authentication service (RADIUS and TACACS+) settings, audit log configuration, ACS licensing, and cryptographic related ACS configuration data.
	Query, Modify, Delete	ACS instances related Configuration Data on the ACS TOE component NOTE: ACS instances refer to deployments that include multiple instances of the ACS TOE component
User Admin (GUI role)	Query, Modify, Delete	Network user and host related Configuration Data on the ACS TOE component
	Query	Network user Identity Group (IDG) related Configuration Data on the ACS TOE component NOTE: Network user identity group is used to configure groups of Network users at the same time.
SuperAdmin (GUI role)	Query, Modify, Delete	All ACS Configuration Data on the ACS TOE component
Admin (CLI role)	Query, Modify, Delete	All ACS Configuration Data on the ACS TOE component
Operator (CLI role)].	Query, Modify, Delete	All ACS Configuration Data on the ACS TOE component that can be accessed with the following commands: exit, nslookup, ping, show acs-logs, show, acs-migration-interface, show cdp, show clock, show, cpu, show disks, show icmp_status, show interface, show logging, show logins, show memory, show ntp, show ports, show process, show terminal, show timezone, show udi, show uptime, show version, ssh, ssh keygen, ssh rmkey, telnet, terminal, and traceroute

Hierarchical to: No other components.
Dependencies: FMT_SMR.1, FMT_SMF.1

5.2.1.1.30 FMT_SMF.1 Specification of Management Functions

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

- *Nexus 5000 Switch TOE component related management functions:*
  - *Configuration of PACL IP ACLs within the ACLs Policy;*
  - *Configuration of VACL IP ACLs within the ACLs Policy;*
  - *Configuration of PACL MAC ACLs within the ACLs Policy;*
  - *Configuration of VACL MAC ACLs within the ACLs Policy;*
  - *Configuration of role definitions within the RBAC Policy;*
  - *Configuration of PVLAN port designation within the PVLAN Policy*
  - *Configuration of IP Source Guard within the ACLs Policy;*
  - *Configuration of Traffic Storm within the ACLs Policy;*
  - *Review audit records;*
  - *Configuration of Nexus 5000 cryptographic services;*
  - *Management of Users;*
  - *Review Nexus 5000 configuration*
  - *Optimize ACLs (using ACL Hit Counters).*

- *ACS TOE component related management functions*
  - *Configuration of ACS cryptographic services;*
  - *Configuration of ACS system settings;*
  - *Management of Administrative Users;*
  - *Review audit records*].

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

5.2.1.1.31 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [

- *Nexus 5000 Switch TOE component related roles:*
  - *network-admin (CLI role)*
  - *network-operator(CLI role)*
  - *administrator-defined roles (CLI roles)*
- *ACS TOE component related roles:*
  - ChangeAdminPassword (GUI role)
  - ChangeUserPassword (GUI role)
  - NetworkDeviceAdmin (GUI role)
  - *PolicyAdmin (GUI role)*
  - *ReadOnlyAdmin (GUI role)*
  - *ReportAdmin (GUI role)*
  - *SecurityAdmin (GUI role)*
  - *System Admin (GUI role)*
  - *UserAdmin (GUI role)*
  - *SuperAdmin (GUI role)*
  - *Admin (CLI role)*
  - *Operator (CLI role)*].

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

Hierarchical to: No other components.
Dependencies: FIA_UID.1

5.2.1.1.32 FPT_STM.1 Reliable time stamps

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

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

5.2.2 Extended Components

This Security Target only contains SFRs drawn from existing CC part 2 Security Function Requirements. This Security Target does not contain explicitly stated SFRs.

5.3 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.

N/A in the Rationale column means the Security Functional Requirement has no dependencies and therefore, no dependency rationale is required. Satisfied in the Rationale column means the Security Functional Requirements dependency was included in the ST. When a dependency is not met, rationale is provided in the Rationale column.

Table 5-17: TOE Security Functional Requirements Dependency Rationale

SFR	Dependencies	Rationale
FAU_GEN.1	FPT_STM.1	Met by FPT_STM.1
FAU_SAR.1(1)	FAU_GEN.1	Met by FAU_GEN.1
FAU_SAR.1(2)	FAU_GEN.1	Met by FAU_GEN.1
FAU_STG.1	FAU_GEN.1	Met by FAU_GEN.1
FCS_CKM.1(1)	[FCS_CKM.2 or FCS_COP.1]	Met by FCS_COP.1(1)
	FCS_CKM.4	Met by FCS_CKM.4
FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1]	Met by FCS_COP.1(6)
	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(1) Met by FCS_CKM.1(2)
FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Met by FCS_CKM.1(1)
	FCS_CKM.4	Met by FCS_CKM.4
FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2	Met by FCS_CKM.1(1)

SFR	Dependencies	Rationale
	or FCS_CKM.1]	Met by FCS_CKM.1(1)
	FCS_CKM.4	Met by FCS_CKM.4
FCS_COP.1(3)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Met by FCS_CKM.1(1)
	FCS_CKM.4	Met by FCS_CKM.4
FCS_COP.1(4)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Not applicable – The cryptographic operation Hashing does not require or use keys.
	FCS_CKM.4	Not applicable – The cryptographic operation Hashing does not require or use keys.
FCS_COP.1(5)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Not applicable – The cryptographic operation Hashing does not require or use keys.
	FCS_CKM.4	Not applicable – The cryptographic operation Hashing does not require or use keys.
FCS_COP.1(6)	[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_COP.1(7)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Not applicable. This SFR specifies key establishment and is not dependent upon key generation 1)
	FCS_CKM.4	Met by _FCS_CKM.4
FDP_IFC.1(1)	FDP_IFF.1	Met by FDP_IFF.1(1)
FDP_IFC.1(2)	FDP_IFF.1	Met by FDP_IFF.1(2)
FDP_IFF.1(1)	FDP_IFC.1,	Met by FDP_IFC.1(1)
	FMT_MSA.3	Met by FMT_MSA.3(1)
FDP_IFF.1(2)	FDP_IFC.1,	Met by FDP_IFC.1(2)
	FMT_MSA.3	Met by FMT_MSA.3(2)
FIA_UAU.1(1)	FIA_UID.1	Met by FIA_UID.1(1)
FIA_UAU.1(2)	FIA_UID.1	Met by FIA_UID.1(2)
FIA_UAU.5(1)	No Dependencies	Not applicable.
FIA_UAU.5	No Dependencies	Not applicable.
FIA_UID.1(1)	No Dependencies	Not applicable.
FIA_UID.1(2)	No Dependencies	Not applicable.
FMT_MSA.1(1)	[FDP_ACC.1 or FDP_IFC.1]	Met by FDP_IFC.1(1)
	FMT_SMR.1	Met by FMT_SMR.1
	FMT_SMF.1	Met by FMT_SMF.1
FMT_MSA.1(2)	[FDP_ACC.1 or FDP_IFC.1]	Met by FDP_IFC.1(2)
	FMT_SMR.1	Met by FMT_SMR.1
	FMT_SMF.1	Met by FMT_SMF.1
	FMT_SMR.1	Met by FMT_SMR.1
	FMT_SMF.1	Met by FMT_SMF.1
FMT_MSA.3(1)	FMT_MSA.1	Met by FMT_MSA.1(1)
	FMT_SMR.1	Met by FMT_SMR.1

SFR	Dependencies	Rationale
FMT_MSA.3(2)	FMT_MSA.1	Met by FMT_MSA.1(2)
	FMT_SMR.1	Met by FMT_SMR.1
	FMT_SMR.1	Met by FMT_SMR.1
	FMT_SMR.1	Met by FMT_SMR.1
FMT_MTD.1(1)	FMT_SMF.1	Met by FMT_SMF.1
	FMT_SMR.1	Met by FMT_SMR.1
FMT_MTD.1(2)	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.1(3) Met by FIA_UID.1(4)
FPT_STM.1	No Dependencies	Not applicable.

5.4 Rationale for SFRs/TOE Objectives

This section provides rationale for the Security Functional Requirements demonstrating that the Security Functional Requirements are suitable to address the security objectives. It identifies each Security Functional Requirement identified in Section 5, the TOE security objective(s) identified in Section 4 that addresses it, Table 31 and Table 32 provides the mapping and rationale for inclusion of each SFR in this ST

Table 5-18: Objective to SFR Mappings

	O.Nexus5KAvail	O.DataFlowControl	O.Admin	O.AdminAuth	O.AdminAccess	O.Audit	O.AuditIntegrity	O.SecureMgtComm	O.VRFSec
FAU_GEN.1						X			
FAU_SAR.1(1)			X						
FAU_SAR.1(2)			X						
FAU_STG.1							X		
FCS_CKM.1(1)								X	
FCS_CKM.1(2)								X	
FCS_CKM.4								X	
FCS_COP.1(1)								X	
FCS_COP.1(2)								X	
FCS_COP.1(3)								X	
FCS_COP.1(4)								X	
FCS_COP.1(5)								X	
FCS_COP.1(6)								X	
FCS_COP.1(7)								X	
FCS_COP.1(8)								X	
FDP_IFC.1(1)	X	X							X

FDP_IFC.1(2)	X	X							
FDP_IFF.1(1)	X	X							X
FDP_IFF.1(2)	X	X							
FIA_UAU.1(1)				X					
FIA_UAU.1(2)				X					
FIA_UAU.5									
FIA_UID.1(1)				X					
FIA_UID.1(2)				X					
FMT_MSA.1(1)			X		X				
FMT_MSA.1(2)			X		X				
FMT_MSA.3(1)			X						
FMT_MSA.3(2)			X						
FMT_MTD.1(1)					X				
FMT_MTD.1(2)					X				
FMT_SMF.1			X						
FMT_SMR.1					X				
FPT_STM.1						X			

Table 5-19: Objective to SFR Mapping Rationale

Objective	SFRs	Rationale
O.Nexus5KAvail	FDP_IFF.1(1)	This SFR applies Traffic Storm to traffic received by the Nexus 5000. This allows the Nexus 5000 switch to continue to provide its services even when attacked by an attacker trying to send traffic by preventing traffic that does not have a matching IP/MAC address combination by preventing devices from communicating with the TOE with an incorrect IP/MAC address combination, or by an attacker trying to overload a Nexus 5000 interface with traffic burst.
	FDP_IFF.1(2)	This SFR applies PVLAN policies controlling traffic within a PVLAN.
	FDP_IFC.1(1)	This SFR applies Traffic Storm to traffic received by the Nexus 5000. This allows the Nexus 5000 switch to continue to provide its services even when attacked by an attacker trying to send traffic to unused ports on the Nexus 5000 switch by preventing traffic to overload a Nexus 5000 interface with traffic burst.
	FDP_IFC.1(2)	This SFR applies PVLAN policies controlling traffic within a PVLAN and restricting traffic based upon PVLAN port designation.
O.DataFlowControl	FDP_IFF.1(1)	This SFR helps to ensure that only authorized traffic flows through the TOE to its destination by applying PACL IP ACLs to data plane traffic processed by the TOE. Traffic that meets a configured ACL is processed according to the specified rule-set and only flows through the TOE to its intended destination if allowed. If not allowed by a configured ACL rule, the TOE prevents the traffic from flowing to its intended destination. This SFR helps to ensure that only authorized traffic flows through the TOE to its destination by applying VACL IP ACLs to data plane traffic processed by the TOE. Traffic that meets a configured ACL is processed according to the specified rule-set and only flows through the TOE to its intended destination if allowed. If not allowed by a configured ACL rule, the TOE prevents the traffic from flowing to its intended destination.

Objective	SFRs	Rationale
		This SFR helps to ensure that only authorized traffic flows through the TOE to its destination by applying PACL MAC ACLs to data plane traffic processed by the TOE. Traffic that meets a configured ACL is processed according to the specified rule-set and only flows through the TOE to its intended destination if allowed. If not allowed by a configured ACL rule, the TOE prevents the traffic from flowing to its intended destination. . This SFR helps to ensure that only authorized traffic flows through the TOE to its destination by verifying that the traffic flowing through the Nexus 5000 TOE component is associated with a configured VRF. Traffic that is associated with a configured VRF is processed according to the VRFs routing table and only flows through the TOE to its intended destination. If the traffic is not associated with a configured VRF, the TOE prevents the traffic from flowing to its intended destination.
	FDP_IFF.1(2)	This SFR helps to ensure that only authorized traffic flows through the TOE to its destination by applying VACL MAC ACLs to data plane traffic processed by the TOE. Traffic that meets a configured ACL is processed according to the specified rule-set and only flows through the TOE to its intended destination if allowed. If not allowed by a configured ACL rule, the TOE prevents the traffic from flowing to its intended destination.
	FDP_IFC.1(1)	This SFR helps to ensure that only authorized traffic flows through the TOE to its destination by applying PACL IP ACLs to data plane traffic processed by the TOE. Traffic that meets a configured ACL is processed according to the specified rule-set and only flows through the TOE to its intended destination if allowed. If not allowed by a configured ACL rule, the TOE prevents the traffic from flowing to its intended destination. This SFR helps to ensure that only authorized traffic flows through the TOE to its destination by applying VACL IP ACLs to data plane traffic processed by the TOE. Traffic that meets a configured ACL is processed according to the specified rule-set and only flows through the TOE to its intended destination if allowed. If not allowed by a configured ACL rule, the TOE prevents the traffic from flowing to its intended destination. This SFR helps to ensure that only authorized traffic flows through the TOE to its destination by applying PACL MAC ACLs to data plane traffic processed by the TOE. Traffic that meets a configured ACL is processed according to the specified rule-set and only flows through the TOE to its intended destination if allowed. If not allowed by a configured ACL rule, the TOE prevents the traffic from flowing to its intended destination. This SFR helps to ensure that only authorized traffic flows through the TOE to its destination by verifying that the traffic flowing through the Nexus 5000 TOE component is associated with a configured VRF. Traffic that is associated with a configured VRF is processed according to the VRFs routing table and only flows through the TOE to its intended destination.

Objective	SFRs	Rationale
		If the traffic is not associated with a configured VRF, the TOE prevents the traffic from flowing to its intended destination.
	FDP_IFC.1(2)	This SFR helps to ensure that only authorized traffic flows through the TOE to its destination by applying VACL MAC ACLs to data plane traffic processed by the TOE. Traffic that meets a configured ACL is processed according to the specified rule-set and only flows through the TOE to its intended destination if allowed. If not allowed by a configured ACL rule, the TOE prevents the traffic from flowing to its intended destination.
O.Admin	FAU_SAR.1(1)	This SFR helps to ensure that the TOE provides the necessary functions to administer the TOE by requiring the TOE to provide secure administrative access to the, PACL, and VACL related audit records and configuration related audit records stored by the TOE.
	FAU_SAR.1(2)	This SFR helps to ensure that the TOE provides the necessary functions to administer the TOE by requiring the TOE to provide secure administrative access to the ACS TOE component configuration related audit records stored by the TOE.
	FMT_MSA.1(1)	This SFR helps to ensure that the TOE provides the necessary functions to administer the TOE by requiring the TOE to provide secure administrative control over the security attributes used to control ACLs Policy.
	FMT_MSA.1(2)	This SFR helps to ensure that the TOE provides the necessary functions to administer the TOE by requiring the TOE to provide secure administrative control over the security attributes used to control the PVLAN policy
	FMT_MSA.3(1)	This SFR helps to ensure that the TOE provides the necessary functions to administer the TOE by requiring the TOE to provide secure administrative control over the security attributes used to control ACLs Policy.
	FMT_MSA.3(2)	This SFR helps to ensure that the TOE provides the necessary functions to administer the TOE by requiring the TOE to provide secure administrative control over the security attributes used to control the PVLAN policies.
	FMT_SMF.1	This SFR helps to ensure that the TOE provides the necessary functions to administer the TOE by requiring the TOE to provide secure management features to support the security functionality provided by the TOE.
O.AdminAuth	FIA_UAU.1(1)	This SFR helps to ensure that only identified and authenticated administrators are allowed access to the administrative functions of the TOE by requiring that any administrative access to the Nexus 5000 may only occur after the TOE has authenticated the potential administrator. The only access allowed for the potential administrator prior to being authenticated is establishment of a secure channel to pass the authentication credentials to the TOE in a protected fashion.
	FIA_UAU.1(2)	This SFR helps to ensure that only identified and authenticated administrators are allowed access to the administrative functions of the TOE by requiring that any administrative access to the ACS TOE component may only occur after the TOE has authenticated the potential administrator. The only access allowed for the potential administrator prior to being

Objective	SFRs	Rationale
		authenticated is establishment of a secure channel to pass the authentication credentials to the TOE in a protected fashion.
	FIA_UAU.5	This SFR helps to ensure that only identified and authenticated administrators are allowed to access the administrative functions of the TOE by supporting multiple types of authentication for potential administrators attempting to access the administrative functions of the Nexus 5000 switch.
	FIA_UID.1(1)	This SFR helps to ensure that only identified and authenticated administrators are allowed access to the administrative functions of the TOE by requiring that any administrative access to the Nexus 5000 may only occur after the TOE has identified the potential administrator. The only access allowed for the potential administrator prior to being identified is establishment of a secure channel to pass the identification credentials to the TOE in a protected fashion.
	FIA_UID.1(2)	This SFR helps to ensure that only identified and authenticated administrators are allowed access to the administrative functions of the TOE by requiring that any administrative access to the ACS TOE component may only occur after the TOE has identified the potential administrator. The only access allowed for the potential administrator prior to being identified is establishment of a secure channel to pass the identification credentials to the TOE in a protected fashion.
O.AdminAccess	FMT_SMR.1	This SFR helps to ensure authorized administrators only have access to the appropriate administrative functions by requiring the TOE to maintain a set of administrative roles. These roles are used by the TOE to determine the authorization level of administrators.
	FMT_MSA.1(1)	This SFR helps to ensure that authorized administrators only have access to the appropriate administrative functions by requiring the TOE to limit the access to configuration of the ACLs Policy to only administrators with a role which allows ACLs Policy administration.
	FMT_MSA.1(2)	This SFR helps to ensure that authorized administrators only have access to the appropriate administrative functions by requiring the TOE to limit the access to configuration of the PVLAN policy
	FMT_MTD.1(1)	This SFR helps to ensure that authorized administrators only have access to the appropriate administrative functions by requiring the TOE to restrict access to TSF data to only administrators of the Nexus 5000 TOE component with the appropriate authorization.
	FMT_MTD.1(2)	This SFR helps to ensure that authorized administrators only have access to the appropriate administrative functions by requiring the TOE to restrict access to TSF data to only administrators of the ACS Server TOE component with the appropriate authorization.
O.Audit	FAU_GEN.1	This SFR helps to ensure that the TOE provides audit records for PACLs, VACLs and administrative actions by requiring that the TOE creates an audit record each time the TOE identifies traffic as meeting an administratively configured PACL, or VACL.
	FPT_STM.1	This SFR helps to ensure that the TOE provides audit records for PACLs, VACLs, and administrative actions by requiring that the TOE provides timestamps to be used with each audit record.

Objective	SFRs	Rationale
O.AuditIntegrity	FAU_STG.1	This SFR helps to ensure that the integrity of all TOE audit records by requiring that the TOE protect all audit records it stores.
O.SecureMgtComm	FCS_CKM.1(1)	This SFR also helps to ensure that management communications to the TOE are protected by providing a pseudo random number generator to create the key used in TLS communications. TLS is used for administrative GUI communications with the ACS TOE component.
	FCS_CKM.1(2)	This SFR helps to ensure that management communications to the TOE are protected by providing the key creation used in SNMPv3 communications. SNMPv3 is used for administrative SNMPv3 communications with the Nexus 5000 switch and the ACS TOE component.
	FCS_CKM.4	This SFR helps to ensure that management communications to the TOE are protected by providing the tunnel tear down used in SSH, SNMPv3, and TLS communications. SSH, SNMPv3, and TLS are used for administrative communications with the Nexus 5000 switch and the ACS TOE component.
	FCS_COP.1(1)	This SFR helps to ensure that management communications to the TOE are protected by providing RSA encryption and decryption used in TLS communications. TLS is used for administrative communications with the ACS TOE component.
	FCS_COP.1(2)	This SFR helps to ensure that management communications to the TOE are protected by providing AES encryption and decryption used in SSH, TLS, and SNMPv3 communications. SSH, TLS, and SNMPv3 are used for administrative communications with the TOE.
	FCS_COP.1(3)	This SFR helps to ensure that management communications to the TOE are protected by providing the Triple-DES encryption and decryption used in SSH, TLS, and SNMPv3 communications. SSH, TLS, and SNMPv3 are used for administrative communications with the TOE.
	FCS_COP.1(4)	This SFR helps to ensure that management communications to the TOE are protected by providing the hashing used in TLS communications. TLS is used for administrative GUI communications with the ACS TOE component.
	FCS_COP.1(5)	This SFR helps to ensure that management communications to the TOE are protected by providing the hashing used in SNMPv3 communications. SNMPv3 is used for administrative communications with the TOE.
	FCS_COP.1(6)	This SFR helps to ensure that management communications to the TOE are protected by providing DSA signature services used in TLS communications. TLS is used for administrative communications with the ACS TOE component.
	FCS_COP.1(7)	This SFR helps to ensure that management communications to the TOE are protected by providing the key establishment used in SSH communications. SSH is used for administrative CLI communications with the Nexus 5000 switch and the ACS TOE component. Additionally, SSH is also used for administration via XML for the Nexus 5000 Switch. This SFR also helps to ensure that management communications to the TOE are protected by providing the key establishment used in TLS communications. TLS is used for administrative GUI communications with the ACS TOE component.

Objective	SFRs	Rationale
O.VRFSec	FDP_IFC.1(1)	This SFR helps to ensure that only all traffic that flows through the TOE is forwarded to the correct destination by ensuring that IP traffic is forwarded in a manner consistent with the associated VRF routing table. If the traffic does not map to a configured VRF, the traffic is not permitted to flow.
	FDP_IFF.1(1)	This SFR helps to ensure that only all traffic that flows through the TOE is forwarded to the correct destination by ensuring that IP traffic is forwarded in a manner consistent with the associated VRF routing table. If the traffic does not map to a configured VRF, the traffic is not permitted to flow.

5.5 Security Assurance Requirements

5.5.1 SAR Requirements

The TOE satisfies CC EAL4 assurance requirements augmented with ALC_FLR.2 derived from Common Criteria Version 3.1, Revision 2. This section identifies the Configuration Management, Delivery and Operation, Development, Flaw Remediation, Guidance Documents, Testing, and Vulnerability Assessment assurance requirements.

Table 5-19: Assurance Measures

Assurance Class	Assurance components
CC EAL4 Assurance Requirements	
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_TDS.3 Basic modular design
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_REQ.2 Derived security requirements
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_IND.2 Independent testing - sample
	ATE_DPT.2 Testing: security enforcing modules
	ATE_FUN.1 Functional testing
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis
Augmented Assurance Requirements	

ALC: Life-cycle support	ALC_FLR.2 Flaw reporting procedures

5.5.2 Security Assurance Requirements Rationale

This Security Target claims an assurance rating of EAL 4 augmented with ALC_FLR.2. This assurance rating was chosen to ensure that the TOE has a moderate level of assurance in enforcing its security functions when instantiated in its intended environment which imposes no restrictions on assumed activity on applicable networks. Augmentation was chosen to provide the added assurances that result from having flaw remediation procedures and correcting security flaws as they are reported.

6 TOE SUMMARY SPECIFICATION

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

Table 6-1: How TOE SFRs are Met

TOE SFRs	How the SFR is Met
FAU_GEN.1	Each time an administrative user logs into or off of the Nexus 5000 switch, 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 5000 switch. Whenever an administrative user make a configuration change to the Nexus 5000 switch, an audit record is generated on a per-command basis. 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. Each time an administrative user logs into or off of the ACS, an audit record is generated. The audit record contains the user ID, the interface on which the action took place (CLI or GUI), the time and date, the action that took place, and the outcome of the event. Whenever an administrative user make a configuration change to the ACS, an audit record is generated by the ACS. The audit record contains the user ID, interface on which the action took place (CLI or GUI), time and date, the action that took place, the new value for configuration changes (except when the new value is security relevant – for example, passwords). Auditing cannot be globally disabled and is automatically available upon the startup of the TOE. Therefore, there is no auditable event that captures the startup and shutdown of the audit function
FAU_SAR.1(1)	Access to audit records stored on the Nexus 5000 switch is controlled by an Access Control Policy. There are several default roles which can access audit records, including, network-admin and network-operator. For other administratively defined roles, if access to the audit records is not specifically configured then no access is granted to users of that role.
FAU_SAR.1(2)	Access to audit records stored on the ACS TOE component is controlled per the capabilities of the user (and associated role) attempting to access the TOE. There ACS supports several predefined roles that allow audit review, including ReadOnlyAdmin (GUI role), ReportAdmin (GUI role), SuperAdmin (CLI role), and MachineAdmin (CLI role). Additionally, the ACS TOE component allows administratively created roles that may be created with audit review capabilities. All attempts to view audit records that do not originate from user with roles that include audit review permissions are denied. The TOE does not include any interfaces that allow unauthorised users to access audit records.
FAU_STG.1	Access to the audit records stored on the TOE are only stored in NVRAM and FLASH memory internal to the module. There is no way to access these audit records other than through a TSF Mediated interface. Only users explicitly authorized to access/modify the audit records are given access to the audit records. There is no interface which may be used to perform unauthorized audit record modification. The Nexus supports local logging of system events and AAA accounting events by default. Remote storage of system events can be achieved by configuring a syslog server, and remote AAA accounting can be configured when using a remote AAA server. ▪ System events are maintained in NVRAM, which stores the most recent

TOE SFRs	How the SFR is Met
	100 messages, and when the log is full oldest messages are over-written when new messages are generated. By default, messages of severity 0, 1, or 2 (emergency, alert, or critical) are logged to the NVRAM log. This setting cannot be changed. ▪ Locally stored AAA events (and system events if configured) are stored in a log that has a default size of 4194304 bytes, but can be configured from 4096 to 10485760 bytes, and when the log is full oldest messages are over-written when new messages are generated. The default severity level of logged events is 5, but can be configured from 0-7.
FCS_CKM.1(1)	A portion of the creating the session establishment includes RSA key generation. See Table 6-2 for the method of compliance to the algorithm standard.
FCS_CKM.1(2)	Administrative communication with the Nexus 5000 appliance can take place over SNMPv3. The first step to establishing an administrative session to the Nexus 5000 appliance using SNMPv3 is to establish a SNMPv3 session. The TOE establishes a SNMPv3 session with the remote administrator. A portion of the SNMPv3 session establishment includes key generation as specified in RFC 3414. See Table 6-2 for the method of compliance to the algorithm standard.
FCS_CKM.4	After each cryptographic session established with the TOE is finished being used, the session is torn down. The keying material associated the session is overwritten and is no longer retrievable. See Table 6-2 for the method of compliance to the algorithm standard.
FCS_COP.1(1)	As part of the TLS communications, the TOE performs RSA encryption and decryption. See Table 6-2 for the method of compliance to the algorithm standard.
FCS_COP.1(2)	As part of the SSH, SNMPv3, and TLS communications, the TOE performs AES encryption and decryption. See Table 6-2 for the method of compliance to the algorithm standard.
FCS_COP.1(3)	As part of the SSH, SNMPv3, and TLS communications, the TOE performs Triple-DES encryption and decryption. See Table 6-2 for the method of compliance to the algorithm standard.
FCS_COP.1(4)	Provides the SHS hashing required as part of the TLS session establishment protocols. See Table 6-2 for the method of compliance to the algorithm standard.
FCS_COP.1(5)	The TOE performs the necessary MD5 hashing as part of RADIUS, TACACS+, and SNMPv3 communications. .See Table 6-2 for the method of compliance to the algorithm standard.
FCS_COP.1(6)	As part of the TLS communications, the TOE performs DSA signature services. See Table 6-2 for the method of compliance to the algorithm standard.
FCS_COP.1(7)	As part of SSH and TLS communications, the TOE provides Diffie-Hellman Key Agreement. See Table 6-2 for the method of compliance to the algorithm standard.
FDP_IFC.1(1)	The TOE enforces information flow policies on network traffic (both IP and non-IP) received by the Nexus 5000 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, 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, Disable the ingress interface, or Create DHCP binding table.
FDP_IFF.1(1)	Whenever network traffic (both IP and non-IP traffic) is received by one of the Nexus 5000 interfaces, the TOE applies administratively configured information

TOE SFRs	How the SFR is Met
	flow policies to the traffic in the following order, 1. Traffic Storm/DHCP Snooping 2. PACL MAC ACLs 3. VRFs 4. VACL IP/MAC ACLs The specific rules associated with each policy are, as follows: Traffic Storm Traffic storm control allows an administrator to monitor the levels of the incoming traffic to a Nexus 5000 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 PACLs When non-IP network traffic that meets an administratively configured PACL MAC ACL is received on Layer 2 interfaces or Layer 2 Ethernet port-channel interfaces, the Nexus 5000 switch makes an information flow decision to either permit or deny the traffic. Traffic is permitted or denied, as follows, ▪ Ingress IP traffic with security attributes that match an administratively configured PACL permit policy rule is allowed to flow, or, ▪ Ingress IP traffic with security attributes that match an administratively configured PACL deny policy rule is not permitted. The PACL permit/deny polices for IP traffic are comprised of a combination of subject security attributes and information attributes and a permit/deny operation. The subject attributes that are available for the creation of PACL permit/deny policies include: slot, port, and port-channel. The information attributes that are available for the creation of PACL permit/deny policies for IP traffic include: Source IP address, Destination IP address, Source port number, Destination port number, Protocol, ICMP message type, ICMP message code, IGMP message type, Precedence, DSCP Value ▪ 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 polices for non-IP traffic are comprised of a combination of subject security attributes and information attributes and a permit/deny operation. The subject attributes that are available for the creation of PACL permit/deny policies include: slot, port, and port-channel. The information attributes that are available for the creation of PACL

TOE SFRs	How the SFR is Met
	permit/deny policies for non-IP traffic include: Source MAC address, Destination MAC address, Protocol, Class of Service (COS), VLAN ID VRFs The Nexus 5000 switch provides the ability for an administrative user to configure VRFs for incoming IP traffic. For IP traffic that is received by the Nexus 5000 interfaces, the Nexus 5000 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. ▪ IP traffic with security attributes that map to a configured VRF will be forwarded through the Nexus 5000 switch TOE component per the VRF routing table VACL IP/MAC ACLs When network traffic that meets an administratively configured VACL IP ACL is received on VLAN interfaces, the Nexus 5000 switch makes an information flow decision to forward the traffic, or drop the traffic. Traffic is forwarded, or dropped 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 deny policy rule is not permitted to flow. The permit/deny polices (defined in VACL IP/MAC ACLs) for IP traffic described above are comprised of a combination of subject security attributes and information attributes and a permit/deny operation. The subject attributes that are available for the creation of permit/deny policies include: vlan-ID. The information attributes that are available for the creation of 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, Precedence, and 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. ▪ The permit/deny polices (defined in VACL IP/MAC ACLs) 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 policies include: vlan-ID. The information attributes that are available for the creation of these permit/deny/redirect/deny-and-log policies include: Source MAC address, Destination MAC address, Protocol, Class of Service (COS), or VLAN ID The following information flow is allowed: • DHCP requests are allowed to flow through the TOE during authentication The following information flow is explicitly allowed: • None.

TOE SFRs	How the SFR is Met
	The following explicit deny rules are enforced on information flows. For IP Network Traffic Flows: ▪ For IP traffic, if the security attributes do not match an administratively configured RACL (5500 series only), PACL 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 RACL (5500 series only), PACL, or VACL, the traffic flow is denied.
FDP_IFC.1(2)	A regular VLAN is a single broadcast domain. The PVLAN policy partitions a larger VLAN broadcast domain into smaller sub-domains. Traffic can be controlled (permitted or denied) within the PVLAN based upon the PVLAN port interface.
FDP_IFF.1(2)	Within a private VLAN domain three separate port designations exist. Each port designation has its own unique set of rules which regulate a connected endpoint's ability to communicate with other connected endpoints within the same private VLAN domain. The three port designations are: promiscuous, isolated, and community. An endpoint connected to a promiscuous port has the ability to communicate with any endpoint within the private VLAN. Multiple promiscuous ports may be defined within a single private VLAN domain. In most networks, Layer 3 default gateways or network management stations are commonly connected to promiscuous ports. Isolated ports are typically used for those endpoints that only require access to a limited number of outgoing interfaces on a private-VLAN-enabled device. An endpoint connected to an isolated port will only possess the ability to communicate with those endpoints connected to promiscuous ports. Endpoints connected to adjacent isolated ports cannot communicate with one another. For example, within a web hosting environment, isolated ports can be used to connect hosts that require access only to default gateways. A community port is a port that is part of a private VLAN community, which is a grouping of ports connected to devices belonging to the same entity (for example, a group of hosts of the same ISP customer or a pool of servers in a data center). Within a community, endpoints can communicate with one another and can also communicate with any configured promiscuous port. Endpoints belonging to one community cannot instead communicate with endpoints belonging to a different community or with endpoints connected to isolated ports.
FIA_UAU.1(1)	Prior to being granted any administrative access to the Nexus 5000 switch, prospective administrative users must be authenticated by the TOE. The only action allowed to these users prior to authentication is establishing a secure remote session with the Nexus 5000 switch (SNMPv3, SSH) so that administrative credentials (e.g., username/password) can be sent in a protected form.
FIA_UAU.1(2)	Prior to being granted any administrative access to the ACS, prospective administrative users must be authenticated by the TOE. The only action allowed to these users prior to authentication is securing a secure remote session with the ACS so that administrative credentials can be sent in a protected form. NOTE: ACS administrative users are always authenticated by the ACS TOE component against a local ACS authentication database.

TOE SFRs	How the SFR is Met
FIA_UAU.5	The TOE supports several authentication techniques for administrative users attempting to access the Nexus 5000 switch administrative functions. The authentication techniques supported by the TOE for Nexus 5000 switch administrative users include the following, ▪ Remote authentication (facilitated by RADIUS or TACACS+ (provided by the ACS TOE component)); ▪ Authentication against a database local to the Nexus 5000 switch The TOE will perform authentication based on the following rules: ▪ For Remote authentication (facilitated by RADIUS or TACACS+), the TSF will authenticate the administrator based on the administratively configured Identification and Authentication scheme ▪ For Authentication against a database local to the Nexus 5000 switch, the TSF will authenticate the administrator based on the administratively configured Identification and Authentication scheme The administratively configured authentication scheme specifies the authentication method order in which the TOE will attempt to authenticate an entity. For example, the TOE may be configured to first attempt remote authentication through the ACS and then attempt local authentication on Nexus 5000. ACS may be configured to use an LDAP server, active directory server, or another ACS server for authentication verification. The ACS then enforces the decision provided by the server.
FIA_UID.1(1)	Prior to being granted any administrative access to the Nexus 5000 switch, prospective administrative users must be authenticated and identified by the TOE. The only action allowed to these users prior to authentication and identified is establishing a secure remote session with the Nexus 5000 switch (SSH, SNMPv3) so that administrative and identification credentials (e.g., username/password) can be sent in a protected form.
FIA_UID.1(2)	Prior to being granted any administrative access to the ACS, prospective administrative users must be authenticated and identified by the TOE. The only action allowed to these users prior to authentication or identification is establishing a secure remote session with the ACS so that authentication and identification credentials can be sent in a protected form.
FMT_MSA.1(1)	The TOE allows authenticated and authorized administrative users of the Nexus 5000 switch TOE component to Read, write ACLs policy rules and 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 access privileges to the policy rules have any access. All other administrative users have no visibility into the existence of the policy rules. The TOE provides two ways to manage the ACL policy rules and the security attributes within the policy rules, traditional rule configuration in which or new rules are applied and all connections are lost during configuration and atomic configuration which allows new configurations to be applied without losing current connections. The TOE allows authenticated and authorized administrative users of the ACS TOE component to query, modify or delete Nexus 5000 policy rules (defined within the ACLs Policy) and 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 access privileges to the policy rules have any access. All other administrative users have no visibility into the existence of the policy rules.
FMT_MSA.1(2)	The TOE allows authenticated and authorized administrative users of the Nexus

TOE SFRs	How the SFR is Met
	5000 switch TOE component to read, write PVLAN policy rules and the security 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 access privileges to the policy rules have any access. All other administrative users have no visibility into the existence of the policy rules. The default roles have the access as identified in table associated with FMT_MSA.1(2) requirement.
FMT_MSA.3(1)	By default (following the Common Criteria admin guidance), traffic flow is not permitted across any switchport (not applicable to management port). To allow traffic flow across switchports, an authorized administrator must enable each switchport after applying their custom configuration (which may include ACLs and/or PVLANs). Thus, the default configuration of traffic flow is restrictive, and can be modified by an authorized administrator.
FMT_MSA.3(2)	The default PVLAN policies are restrictive. PVLAN ports must be explicitly defined and designated to be a particular type (i.e. promiscuous, isolated, or community).
FMT_MTD.1(1)	The TOE provides the ability for administrators of the Nexus 5000 to access TOE configuration data. Each of the predefined and administratively configured roles has either read or write access to the configuration and audit data. See the table in the FMT_MTD.1(1) SFR definition for details regarding the specific access available to each user role.
FMT_MTD.1(2)	The TOE provides the ability for administrators of the ACS to access TOE configuration and audit data. Each of the predefined and administratively configured roles has query, modify, or delete access to the configuration and audit data. See the table in the FMT_MTD.1(2) SFR definition for details regarding the specific access available to each user role.
FMT_SMF.1	Through the administrative interface of the Nexus 5000 switch (CLI), the TOE facilitates the following administrative functions, ▪ Configuration of PACL IP ACLs within the ACLs Policy – This functionality allows the configuration of PACL IP ACLs by an administrative user. ▪ Configuration of VACL IP ACLs within the ACLs Policy – This functionality allows the configuration of VACL IP ACLs by an administrative user. ▪ Configuration of PACL MAC ACLs within the ACLs Policy – This functionality allows the configuration of PACL MAC ACLs by an administrative user. ▪ Configuration of VACL MAC ACLs within the ACLs Policy - This functionality allows the configuration of VACL MAC ACLs by an administrative user. ▪ Configuration of RBACs - This functionality allows the configuration of RBACs by an administrative user. ▪ Configuration of IP Source Guard within the ACLs Policy - This functionality allows the configuration of IP Source Guard by an administrative user. ▪ Configuration of Traffic Storm within the ACLs Policy - This functionality allows the configuration of Traffic Storm by an administrative user. ▪ Reviewing audit records – This functionality allows Nexus 5000 audit

TOE SFRs	How the SFR is Met
	records to be viewed by an administrative user. ▪ Configuration of Nexus 5000 cryptographic services - This functionality allows the configuration of Nexus 5000 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 5000 configuration - This functionality allows the administrative user to review the Nexus 5000 configuration. ▪ Configure ACL Optimization (the TOE uses ACL Hit Counters to re-order ACEs within the ACL to reduce the ACL examination time and increase performance only when the re-ordering does not change the logical order of the ACEs (see description in section 1 ACL Hit Counters). Through the administrative interface of the ACS TOE component (CLI and GUI), the TOE facilitates the following administrative functions, ▪ Configuration of ACS cryptographic services - This functionality allows the configuration of the ACS cryptographic services by an administrative user. ▪ Configuration of ACS system settings – This configuration allows the setting of system setting, including, RADIUS and TACACS+ settings, audit log configuration, configuring how many instances of ACS will run within a deployment, and ACS licensing. ▪ Management of Administrative Users – The functionality allows the creation and configuration of administrative accounts, view predefined roles, and the ability to assign roles to a specific user. ▪ Review audit records – This functionality allows ACS TOE component audit records to be viewed by an administrative user.
FMT_SMR.1	The Nexus 5000 switch supports the following predefined roles, ▪ network-admin – This role is a super administrative role. This role has read and write privileges for any configuration item on the Nexus 5000 switch and Nexus 2000 switch. ▪ network-operator - This role has read privileges for any configuration item on the Nexus 5000 switch and Nexus 2000 switch. The permissions associated with the predefined administrative roles cannot be modified. The TOE does allow, however, for the configuration of custom administrative roles on the Nexus 5000 switch. Access for the custom roles can be defined per command, feature (a group of commands), or feature group (a collection of features). Role definitions consists of Role-based access control (RBAC) rules that result in permitting or a denying access to a command, feature, or feature group. A single rule may either permit or deny invocation of a single command, command associated a feature, or command associated with a feature group. The TOE enforces role-based access restrictions on administrative access and authorization to the Nexus 5000 switch. Access to the administrative functionality of the Nexus 5000 switch is permitted based on the role assigned to the user attempting to access the functionality. One of four permissions (Permit Read Access, Permit Write Access, Deny Read Access, or Deny Write Access) can be administratively assigned on a per command, feature (a collection of commands), or feature group (a collection of features) basis. The decision to allow a user access to specific administrative functionality is based on the administratively configured

TOE SFRs	How the SFR is Met
	permission assigned to the role(s) for which the user is associated. The ACS TOE component supports several predefine roles, as follows: ▪ ChangeAdminPassword (GUI role) – This role entitles the administrator to change the password of other administrators. ▪ ChangeUserPassword (GUI role) – This role entitles the administrator to change the password of internal users. ▪ Network Device Admin (GUI role) – This role has privileges to Network Device Configuration Data. ▪ Policy Admin (GUI role) – This role has privileges to Policy and Services related Configuration Data ▪ ReadOnlyAdmin (GUI role) – This role has privileges to ACS administrative service related Configuration Data ▪ ReportAdmin (GUI role) – This role has privileges to Audit logs ▪ SecurityAdmin (GUI role) – This role has privileges to ACS administrative service related Configuration Data ▪ SystemAdmin (GUI role) – This role has privileges to ACS system administration and ACS instances related Configuration Data ▪ UserAdmin (GUI role) – This role has privileges to Network user and host related Configuration Data ▪ SuperAdmin (GUI role) – This role has complete access to every ACS administrative function. This is also the role assigned to the predefined ACSAdmin account. ▪ Admin (CLI role) – This role has privileges to all ACS Configuration Data and commands at the CLI. ▪ Operator (CLI role) – This role has privileges to all ACS Configuration Data on the ACS TOE component that can be accessed with the following commands: exit, nslookup, ping, show acs-logs, show, acs-migration-interface, show cdp, show clock, show, cpu, show disks, show icmp_status, show interface, show logging, show logins, show memory, show ntp, show ports, show process, show terminal, show timezone, show udi, show uptime, show version, ssh, ssh keygen, ssh rmkey, telnet, terminal, and traceroute NOTE: telnet is disabled by default and is to remain disabled in the evaluated configuration. The permissions associated with the predefined administrative roles cannot be modified. The TOE does allow, however, for the configuration of custom administrative roles on the ACS TOE component.
FPT_STM.1	Both the Nexus 5000 switch and the ACS TOE component can provide hardware based timestamp that are used to provide the 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 table below summarizes the method used to determine compliance to standards identified in the cryptographic related requirements.

Table 6-2: Cryptographic Functions and Method of Compliance

SFR/Algorithm	Key sizes	Standard Claimed	Method of Compliance

SFR/Algorithm	Key sizes	Standard Claimed	Method of Compliance
FCS_CKM.1(1)/RSA Key generation	1024-bits and 2048 bits	RFC 2246	Vendor assertion
FCS_CKM.1(2)/SNMPv3 Key generation	64, 128, 192, and 256 bits	RFC 3414	Vendor assertion
FCS_CKM.4 /Key zeroization		none	N/A
FCS_COP.1(1)/RSA encryption/decryption	1024-bits and 2048-bits	FIPS 186-2	Vendor assertion
FCS_COP.1(2)/AES encryption/decryption in CBC mode	128 bits	FIPS 197	Vendor assertion
FCS_COP.1(3)/Triple-DES encryption/decryption in CBC mode	168-bits	FIPS 46-3	Vendor assertion
FCS_COP.1(4)/SHS Hashing	N/A	FIPS 180-2	Vendor assertion
FCS_COP.1(5)/ MD5 hashing	128-bit	RFC 1321	Vendor assertion
FCS_COP.1(6)/DSA Signature Services	1024-bits	FIPS 186-2	Vendor assertion
FCS_COP.1(7)/Diffie-Hellman	768, to 2048- bits	RFC 2631	Vendor assertion

7 ANNEX A: REFERENCES/ACRONYMS/DEFINITIONS

7.1 References

The following documentation was used to prepare this ST:

[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2006, version 3.1, Revision 1, CCMB-2006-09-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2007, version 3.1, Revision 2, CCMB--2007-09-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2007, version 3.1, Revision 2, CCMB-2007-09-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2007, version 3.1, Revision 2, CCMB-2007-09-004
[PVLAN]	Cisco System's Private VLANs: Scalable Security in a Multi-Client Environment draft-sanjib-private-vlan-10.txt]