



Nexus 7000 Series Switch Security Target

Revision 0.23

August 2012

Table of Contents

Table of Contents.....	2
List of Tables.....	3
1 SECURITY TARGET INTRODUCTION.....	5
1.1 ST and TOE Reference.....	5
1.2 Acronyms and Abbreviations.....	5
1.3 TOE Overview.....	7
1.3.1 TOE Product Type.....	7
1.3.2 Required non-TOE Hardware/ Software/ Firmware.....	7
1.4 TOE DESCRIPTION.....	7
1.5 Physical Scope of the TOE.....	9
1.6 Logical Scope of the TOE.....	10
1.6.1 Data Plane Information Flow Control.....	10
1.6.2 Data Plane Information Flow Accountability.....	11
1.6.3 Cisco TrustSec (CTS).....	12
1.6.4 Management Security.....	13
1.6.5 Virtualization and Availability.....	15
1.7 TOE Evaluated Configuration.....	16
1.7.1 Excluded Functionality.....	17
2 Conformance Claims.....	19
2.1 Common Criteria Conformance Claim.....	19
2.2 Protection Profile Conformance.....	19
3 SECURITY PROBLEM DEFINITION.....	20
3.1 Assumptions.....	20
3.2 Threats.....	20
3.3 Organizational Security Policies.....	21
4 SECURITY OBJECTIVES.....	22
4.1 Security Objectives for the TOE.....	22
4.2 Security Objectives for the Environment.....	23
4.3 Security Objectives Rationale.....	23
5 SECURITY REQUIREMENTS.....	28
5.1 Conventions.....	28
5.2 Security Functional Requirements.....	28
5.2.1 TOE Security Functional Requirements.....	29
5.2.2 Extended Components.....	57
5.3 TOE SFR Hierarchies and Dependencies.....	57
5.4 Rationale for SFRs/TOE Objectives.....	60
5.5 Security Assurance Requirements.....	68
5.5.1 SAR Requirements.....	68
5.5.2 Security Assurance Requirements Rationale.....	69
6 TOE Summary Specification.....	70
6.1 TOE Security Functional Requirement Measures.....	70
6.2 TOE Bypass and interference/logical tampering Protection Measures.....	85
7 Annex A: References/Acronyms/Definitions.....	87
7.1 References.....	87

List of Tables

TABLE 1: ST AND TOE IDENTIFICATION	5
TABLE 2: ACRONYMS	5
TABLE 3: IT ENVIRONMENT COMPONENTS	7
TABLE 4: TOE COMPONENT DESCRIPTIONS	8
TABLE 5: PHYSICAL SCOPE OF THE TOE	9
TABLE 6: PC&I CRYPTOGRAPHIC METHODS	13
TABLE 7: SECURE MANAGEMENT COMMUNICATION	14
TABLE 8 TOE ASSUMPTIONS	20
TABLE 9 THREATS	20
TABLE 10 ORGANIZATIONAL SECURITY POLICIES	21
TABLE 11 SECURITY OBJECTIVES FOR THE TOE	22
TABLE 12 SECURITY OBJECTIVES FOR THE ENVIRONMENT	23
TABLE 13: HOW SECURITY OBJECTIVES MAP TO THREATS, ASSUMPTIONS, AND OSPS	24
TABLE 14: SECURITY OBJECTIVES MAP TO THREATS, ASSUMPTIONS, AND OSPS RATIONALE	24
TABLE 15 SECURITY FUNCTIONAL REQUIREMENTS	28
TABLE 16: ACL AUDIT INFORMATION	30
TABLE 17: CRYPTOGRAPHIC KEY GENERATION PROVIDED BY THE TOE (RSA)	32
TABLE 18: PAC KEY CREATION PROVIDED BY THE TOE	33
TABLE 19: HMAC-SHA1 BASED KEY GENERATION	33
TABLE 20: CRYPTOGRAPHIC KEY DESTRUCTION PROVIDED BY THE TOE	33
TABLE 21: RSA ENCRYPTION/DECRYPTION PROVIDED BY THE TOE	34
TABLE 22: AES ENCRYPTION/DECRYPTION PROVIDED BY THE TOE	34
TABLE 23: TRIPLE-DES ENCRYPTION/DECRYPTION PROVIDED BY THE TOE	35
TABLE 24: SHS HASHING PROVIDED BY THE TOE	35
TABLE 25: MD5 HASHING PROVIDED BY THE TOE	36
TABLE 26: GMAC MESSAGE AUTHENTICATION PROVIDED BY THE TOE	36
TABLE 27: DSA ENCRYPTION/DECRYPTION PROVIDED BY THE TOE	36
TABLE 28: ROLE/OPERATIONS ASSOCIATED WITH ACLS	50
TABLE 29: ROLE/OPERATIONS ASSOCIATED WITH CONTROL PLANE POLICING	51
TABLE 30: ROLE/OPERATIONS ASSOCIATED WITH RBAC	51
TABLE 31: ROLE/OPERATIONS ASSOCIATED WITH VRFS	52
TABLE 32: ROLE/OPERATIONS/TSF DATA	53
TABLE 33: ROLE/OPERATIONS/TSF DATA	54
TABLE 34: TOE SECURITY FUNCTIONAL REQUIREMENTS DEPENDENCY RATIONALE	57
TABLE 35: OBJECTIVE TO SFR MAPPINGS	60
TABLE 36: OBJECTIVE TO SFR MAPPING RATIONALE	61
TABLE 37: ASSURANCE MEASURES	68
TABLE 38: HOW TOE SFRS ARE MET	70

DOCUMENT INTRODUCTION

Prepared By:

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

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Nexus 7000 Series Switch 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.

REVISION HISTORY

<u>Rev</u>	<u>Date</u>	<u>Description</u>
0.01	December	Initial Draft
0.02	January	Revision based on team comments
0.03	January	Revision based on Internal BU comments
0.04	January	Continued revisions based on BU comments
0.05	January	Updated TOE identifier
0.06	March	Updated to reflect Lab Comments
0.07	March	Updated to reflect internal review
0.08	March	Updated to reflect Lab Comments 2
0.09	March	Minor update for clarity
0.10	March	Updated to reflect Lab Comments
0.11	March	One final updated for lab
0.12	March	Additional comment updated for lab
0.13	February 2010	Updates based on other document creation
0.14	February 2010	Updates based on ACS feedback
0.15	July 2010	Updates based on testing feedback
0.16	November 2010	Updates for AGD guide consistency
0.17	November 2010	Updates for ADV evidence
0.18	December 2010	Updates for ATE ETR
0.19	January 2011	Updates for tVOR and testing
0.20	February 2011	Updates for new ACS version with patch
0.21	February 2011	Updates for Validator comments
0.22	April 2011	Updates for FIPS certificate numbers
0.23	August 2012	Updates for Maintenance effort

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: ST and TOE Identification

ST Title	Nexus 7000 Series Switch Security Target
ST Version	Version 0.23
Publication Date	August 2012
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Nexus 7000 Series Switch and Cisco Secure Access Control Server (ACS)
TOE Software Version	NX-OS version 5.2(5), ACS version 5.2 patch 8
Keywords	Switch, Data Protection, Authentication, Cryptography

1.2 Acronyms and Abbreviations

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

Table 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
ARP	Address Resolution Protocol
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
COS	Class of Service
CTS	Cisco Trust Sec
DGT	Destination Group Tag
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service

Acronyms / Abbreviations	Definition
DSCP	Differentiated Services Code Point
EAC	Endpoint Admission Control
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
Gbps	Gigabits per second
GMAC	Galois Message Authentication Code
HMAC	Hash Message Authentication Code
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
NDAC	Network Device Admission Control
OS	Operating System
PACL	Port Access Control List
PC&I	Packet Confidentiality and Integrity
PP	Protection Profile
RACL	Router Access Control List
RADIUS	Remote Authentication Dial In User Service
RPF	Reverse Path Forwarding
RSA	Rivest, Shamir, Adleman
SAP	Security Association Protocol
SGACL	Security Group Access Control List
SGT	Security Group Tag
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
VLAN	Virtual Local Area Network
VRF	Virtual routing and forwarding

1.3 TOE Overview

1.3.1 TOE Product Type

The Nexus 7000 TOE component is a data center-class switch for 10 Gigabit Ethernet networks with a fabric architecture that scales to 15 terabits per second (Tbps). The Nexus 7000 TOE is both IPv4 and IPv6 capable.

The ACS TOE component is an AAA server that provided authentication services and supports the implementation of information flow policies by the Nexus 7000 switch TOE component. The AAA services provided by the ACS server include RADIUS and TACACs for authentication. The ACS server also maintains the authentication credentials for the Network Devices that are part of the TOE protected network and the authentication credentials for the Endpoints attempting to connect to the TOE protected network. Finally, the ACS TOE component creates the PAC Key used in the protection of packets on the TOE protected network.

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 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 7000 switch TOE components via CLI administrative interfaces. Any SSH client may be used. Examples include, PuTTY
Audit server or Configuration Collection SW resident on end point device	YES	Purpose is to collect configuration information from end-point devices attempting to access the protected network. This configuration is used by the TOE to determine whether the endpoint device meets the requirements to connect to the CTS network. An example of an Audit Server is, QualysGuard version 4.5. An example of, collection software is, Cisco Trust Agent version 2.1.103. These will be included in the evaluated configuration of the TOE.
CTS capable devices	OPTIONAL	The TOE interacts with devices in the IT environment [which have CTS capable network cards] via hop-to-hop encryption [CTS PC-1]. These devices are part of the CTS network.
Time Server	OPTIONAL	Optionally provide time stamps in deployment scenarios in which an external time source is desirable.
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 Nexus 7000 Series Switch and Cisco Secure Access Control Server (ACS) Target of Evaluation (TOE). This section also defines the TOE components included in the evaluated configuration of the TOE.

Table 4: TOE Component Descriptions

TOE Component	TOE-Subcomponent	Description
<p data-bbox="235 289 526 319">Nexus 7000 Series Switch</p> 	<p data-bbox="548 275 834 394">Cisco Nexus 7000 Series 10-Slot Chassis (Also referred to as the 7010 Switch)</p>	<p data-bbox="857 275 1383 352">The Cisco Nexus 7000 Series 10-Slot chassis with eight I/O module slots supports up to 256 10 Gigabit Ethernet or 384 Gigabit Ethernet ports.</p>
	<p data-bbox="548 401 834 520">Cisco Nexus 7000 Series 18-Slot Chassis (Also referred to as the 7018 Switch)</p>	<p data-bbox="857 401 1383 478">The Cisco Nexus 7000 Series 18-Slot chassis with sixteen I/O module slots supports up to 512 10 Gigabit Ethernet or 768 Gigabit Ethernet ports.</p>
	<p data-bbox="548 527 834 646">Cisco Nexus 7000 Series Supervisor Module (plugs into either the 10-Slot or 18-Slot chassis)</p>	<p data-bbox="857 527 1383 709">The Cisco Nexus 7000 Series Supervisor Module is designed to deliver scalable control plane and management functions for the Cisco Nexus 7000 Series chassis. The supervisor controls the Layer 2 and 3 services, redundancy capabilities, configuration management, status monitoring, power and environmental management.</p>
	<p data-bbox="548 716 834 863">Cisco Nexus 7000 10-Slot Chassis 46Gbps/Slot Fabric Module (plugs into the 10-Slot chassis)</p>	<p data-bbox="857 716 1383 905">The Cisco Nexus 7000 10-Slot Fabric Module is a fabric module that provides parallel fabric channels to each I/O and supervisor module slot. Up to five simultaneously active fabric modules work together delivering up to 230 Gbps per slot. The fabric module provides the central switching element for the fully distributed forwarding on the I/O modules.</p>
	<p data-bbox="548 911 834 1058">Cisco Nexus 7000 18-Slot Chassis 46Gbps/Slot Fabric Module (plugs into the 18-Slot chassis)</p>	<p data-bbox="857 911 1383 1100">The Cisco Nexus 7000 18-Slot Fabric Module is a fabric module that provides parallel fabric channels to each I/O and supervisor module slot. Up to five simultaneously active fabric modules work together delivering up to 230 Gbps per slot. The fabric module provides the central switching element for the fully distributed forwarding on the I/O modules.</p>
	<p data-bbox="548 1106 834 1283">Cisco Nexus 7000 Series 32-Port 10Gb Ethernet Module with 80Gbps Fabric (plugs into either the 10-Slot or 18-Slot chassis)</p>	<p data-bbox="857 1106 1383 1373">The Cisco Nexus 7000 Series 32-Port 10Gb Ethernet Module with 80 Gb of bandwidth to the fabric is a high-performance, high-density 10 Gigabit Ethernet module. This module delivers up to 256 ports of 10 Gigabit Ethernet. This module can also be used as a 10 Gigabit Ethernet uplink when employing the Cisco Nexus 7000 Series 48-port 10/100/1000 Module for the access layer. The physical interfaces on the Cisco Nexus 7000 32-Port 10Gb Ethernet Module support SFP+ pluggable optics.</p>
	<p data-bbox="548 1379 834 1556">Cisco Nexus 7000 Series 48-Port 10/100/1000 Ethernet Module with 46 Gbps Fabric (plugs into either the 10-Slot or 18-Slot chassis)</p>	<p data-bbox="857 1379 1383 1514">The Cisco Nexus 7000 48-Port 10/100/1000 Ethernet Module with 46 Gbps of bandwidth to the fabric is a high-performance, highly scalable module. This module delivers up to 384 ports of 10/100/1000 Ethernet.</p>
	<p data-bbox="548 1568 834 1745">Cisco Nexus 7000 Series 48-Port Gigabit Ethernet SFP Module with 46 Gbps Fabric (plugs into either the 10-Slot or 18-Slot chassis)</p>	<p data-bbox="857 1568 1383 1682">The Cisco Nexus 7000 48-Port Gigabit Ethernet SFP Module with 46 Gbps of bandwidth to the fabric is a high-performance, highly scalable module. This module delivers up to 384 ports of Gigabit Ethernet.</p>
	<p data-bbox="548 1757 834 1892">Cisco Nexus 7000 Series 8-Port 10Gigabit Ethernet X2 XL Module with 80 Gbps Fabric (plugs into either the 10-</p>	<p data-bbox="857 1757 1383 1892">The Cisco Nexus® 7000 Series 8-Port 10 Gigabit Ethernet Module with XL Option is a cost-effective, highly scalable, high-performance module designed for mission-critical Ethernet networks. The module uses two M1-XL forwarding engines that feature a</p>

TOE Component	TOE-Subcomponent	Description
	Slot or 18-Slot chassis)	larger Forwarding Information Base (FIB). The module also supports a wide range of X2 optics, allowing deployment flexibility in various type of networking environment.
	Cisco Nexus 7000 Series 48-Port Gigabit Ethernet XL SFP Module with 46 Gbps Fabric (plugs into either the 10-Slot or 18-Slot chassis)	The Cisco Nexus® 7000 Series 48-Port Gigabit Ethernet Module with XL Option is a highly scalable module designed for performance-driven, mission-critical Ethernet networks. The module uses the M1-XL forwarding engine, providing a throughput of up to 60 million packets per seconds (Mpps); 48 high-density Gigabit Ethernet ports; and a larger Forwarding Information Base (FIB), making it ideal for deployment at an Internet exchange point (IXP), a service provider, or a large enterprise.
Cisco Secure Access Control Server (ACS) 	Not Applicable. There are no subcomponents. The ACS TOE component is made of one component the Cisco CAM25 appliance – 1120 or 1121 running the ACS software.	Cisco Secure ACS is a highly scalable, high-performance access control server that operates as a centralized authentication server.

1.5 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the Nexus 7000 Series Switch and Cisco Secure Access Control Server (ACS) TOE. The TOE is comprised of the following:

Table 5: Physical Scope of the TOE

TOE Component	Hardware (within the TOE)	Software (within the TOE)
Nexus 7000 Series Switch	Cisco Nexus 7000 Series 10-Slot Chassis	NX-OS version 5.2(5) This includes a hardened version of Linux Kernel 2.6.
	Cisco Nexus 7000 Series 18-Slot Chassis	
	Cisco Nexus 7000 Series Supervisor Module	
	Cisco Nexus 7000 10-Slot Chassis 46Gbps/Slot Fabric Module	
	Cisco Nexus 7000 18-Slot Chassis 46Gbps/Slot Fabric Module	
	Cisco Nexus 7000 Series 32-Port 10Gb Ethernet Module with 80Gbps Fabric	
	Cisco Nexus 7000 Series 48-Port Gigabit Ethernet SFP Module with 46Gbps Fabric	
	Cisco Nexus 7000 Series 48-Port 10/100/1000 Ethernet Module with 46Gbps Fabric	
	Cisco Nexus 7000 Series 8-Port Gigabit Ethernet X2 XL Module with 80Gbps Fabric	

TOE Component	Hardware (within the TOE)	Software (within the TOE)
	Cisco Nexus 7000 Series 48-Port Gigabit Ethernet SFP Module with 46Gbps Fabric XL Module	
Cisco Secure Access Control Server (ACS)	Cisco CAM25 appliance – 1120 or 1121	ACS Software version 5.2 patch 10 This includes a hardened version of Linux Kernel 2.4.

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. RACLs
 - b. PACLs
 - c. VACLs
 - d. VRFs
2. Data Plane Information Flow Accountability
3. Cisco TrustSec (CTS)
 - a. NDAC
 - b. PC&I
 - c. SGACL
4. Secure Management
 - a. Administrator Identification and Authentication
 - b. Administrative Auditing
 - c. Administrative Authorization
 - d. Secure Management Communication
5. Availability
 - a. Virtual Device Context (VDC) Security
 - b. Port Security
 - c. IP Source Guard
 - d. Traffic Storm Control
 - e. Control Plane Policing
 - f. Rate Limiting
 - g. DHCP Snooping – Dynamic ARP Inspection

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 7000 switch. The following types of traffic flow may be able to be controlled for both IPv4 and IPv6 traffic:

- ◆ Layer 3 Traffic – RACLs
- ◆ Layer 2 Traffic – PACLs

- ◆ VLAN Traffic – VACLs
- ◆ VRFs

A RACL is an administratively configured access control list that is applied to Layer 3 traffic that is routed into or out of a Nexus 7000 switch. A PACL is an administratively configured access control list that is applied to Layer 2 traffic that is routed into a Nexus 7000 switch. A VACL is an administratively configured access control list that is applied to packets that are routed into or out of a VLAN or are bridged within a VLAN. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces.

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

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

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

The TOE supports Virtual Routing and Forwarding (VRF). VRFs allow multiple instances of routing tables to exist within the Nexus 7000 switch TOE component simultaneously. This increases functionality by allowing network paths to be segmented without using multiple devices. Each VRF instance uses a single routing table. These tables prevent traffic from being forwarded outside a specific VRF path and also keep out traffic that should remain outside the VRF path.

1.6.2 Data Plane Information Flow Accountability

The Nexus 7000 switch TOE component provides the ability to audit the information flow decisions associated with RACLs, PACLs, and VACLs. Audited events include when a packet matches a configured RACL, PACL IP ACLs rule, when a packet matches a configured VACL IP ACLs rule, when a packet is dropped as the result of matching a configured VACL IP ACLs rule, when a packet matches a configured PACL MAC ACLs rule, when a packet matches a configured VACL MAC ACLs rule, or when a packet is dropped as the result of matching a configured VACL MAC ACLs rule.

1.6.3 Cisco TrustSec (CTS)

The Cisco TrustSec security architecture builds secure networks by establishing clouds of trusted network devices. Each device in the cloud is authenticated by its neighbors. Communication on the links between devices in the cloud is secured with a combination of encryption and message integrity checks. Cisco TrustSec also uses the device and user identification information acquired during authentication for classifying traffic as it enters the network. This traffic classification is maintained by tagging packets on ingress to the Cisco TrustSec network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path.

As traffic enters the Cisco TrustSec network, the format of the packet is altered to include a source identification tag. The tag is included within the packet for the duration of the time the packet is within the Cisco TrustSec network. The tag is a unique 16-bit tag, called the security group tag (SGT), allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic. The SGT is a single label that indicates the privileges of the source within the entire enterprise. Its scope is global within a Cisco TrustSec network.

The exit endpoint of the Cisco TrustSec network identifies the tag embedded in the traffic exiting the Cisco TrustSec network and decides whether to allow or not allow the traffic to exit the network and reach its final destination. Cisco TrustSec uses ingress tagging and egress filtering to enforce access control policy in as a conversation.

1.6.3.1 Network Device Admission Control (NDAC)

Network Device Admission Control is designed to enforce a trust relationship between network devices and their trusted peers. Network devices entering the Cisco TrustSec Network are initially considered untrusted and assigned limited access. When a network device enters the Cisco TrustSec network the Network Device is immediately authenticated using 802.1x methods. After the network device is authenticated, the device is assigned the appropriate security group tag and access to the network is based on the permissions associated with the security group tag. The Nexus 7000 uses key-based authentication. Based on the send and accept lifetimes of a key, keychain management provide a secure mechanism to handle key rollover of the authentication keys. The Nexus 7000 uses the lifetimes of keys to determine which keys in a keychain are active.

1.6.3.2 Packet Confidentiality & Integrity (PC&I)

The TOE provides port level encryption, decryption, and integrity verification of traffic entering and exiting the Nexus 7000 switch. As packets leave the Nexus 7000 switch they are encrypted at line rate. The traffic flows across the Cisco TrustSec network in encrypted format preventing tampering and spoofing. As encrypted traffic enters the Nexus 7000 switch, the packets are decrypted. In addition to the encryption and decryption capabilities, the TOE also provides integrity verification on the packets to

ensure that the frame was not tampered with. This feature is based on the 802.11i modified for wired networks. The following table identifies the cryptographic methods implemented by the TOE for use in PC&I.

Table 6: PC&I Cryptographic Methods

Cryptographic Method	Purpose
SAP Session Establishment	Establishes a secure connection between devices on in the Cisco TrustSec network.
SAP Re-Keying	Establishes a secure connection between devices on in the Cisco TrustSec network by creating a new shared key between devices on in the Cisco TrustSec network.
AES	Data plane packet encryption and decryption.
GMAC	Data plane packet integrity check.

1.6.3.3 SGACL

In security group access lists (SGACLs), an administrator can control the operations that users can perform based on assigned security groups. SGACL rules are crafted around the presumed source and destination of traffic packets. As the administrator adds packet sources to the Nexus 7000, the packet sources are assigned to one or more security groups and they immediately receive the appropriate permissions.

Cisco TrustSec assigns a unique 16-bit tag, called the security group tag (SGT), to a security group. The SGT is a single label that indicates the privileges of the source within the entire enterprise. Its scope is global within a Cisco TrustSec network.

Once authenticated, Cisco TrustSec tags any packet that originates from a device with the SGT that represents the security group to which the device is assigned. The packet carries this SGT throughout the network within the Cisco TrustSec header. Because this tag represents the group of the source, the tag is referred to as the source SGT. At the egress edge of the network, Cisco TrustSec determines the group that is assigned to the packet destination device and applies the access control policy.

1.6.4 Management Security

The TOE provides the ability to be securely administered.

1.6.4.1 Administrator Identification and Authentication

Users must be authenticated prior to gaining access to the administrative functionality of the Nexus 7000 switch TOE component. Administrative authentication options include remote authentication facilitated by (RADIUS or TACACS+ (provided by the ACS TOE component)), and authentication against a database local to the Nexus 7000 appliance.

Users must be authenticated prior to gaining access to the administrative functionality of the ACS TOE component. Administrators are authenticated locally to the ACS. 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.

1.6.4.2 Administrative Auditing

The Nexus 7000 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 7000 and ACS TOE components.

1.6.4.3 Administrative Authorization

The Nexus 7000 switch TOE component provides a granular administration authorization framework for defining the exact Nexus 7000 administrative capabilities available to the user based on assigned role(s). Users may be assigned multiple roles. The Nexus 7000 switch supports four predefined roles, as follows: network-admin, network-operator, vdc-admin, and vdc-operator. All roles with the exception of the pre-defined network-admin and network-operator are specific to a particular Virtual Device Context (VDC). Authorized administrators of the Nexus 7000 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: NetworkDeviceAdmin, PolicyAdmin, ReadOnlyAdmin, ReportAdmin, SecurityAdmin, SystemAdmin, UserAdmin, ChangeAdminPassword, ChangeUserPassword, and SuperAdmin. The ACS TOE component also supports two CLI administrative roles, Admin and Operator.

1.6.4.4 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 7: Secure Management Communication

TOE Component	Secure Management Protocol
Nexus 7000 Switch TOE component	Secure Shell (SSH)
ACS TOE component	Secure Shell (SSH) Transport Layer Security (TLS) 1.0

1.6.5 Virtualization and Availability

The TOE provides several measures to help assure that Nexus 7000 switch is able to constantly provide the desired switching services. The TOE protects the Virtual Device Contexts resident within the Nexus 7000 switch from interfering with other Virtual Device Contexts. The TOE also provides a several traffic control policies specifically to ensure that the TOE services are available to legitimate traffic.

1.6.5.1 Virtual Device Context (VDC) Security

VDCs are instrumental in the consolidation of separate networks onto a common infrastructure. The TOE ensures that the operation of each VDC operates independently of the other VDCs located on the Nexus 7000 switch. A failure within one VDC will not adversely affect the other VDCs resident on the Nexus 7000 switch.

1.6.5.2 Port Security

Port security allows the administrative users to configure Layer 2 interfaces that allow inbound traffic from only a restricted set of MAC addresses. The MAC addresses in the restricted set are called secure MAC addresses. In addition, the device does not allow traffic from these MAC addresses on another interface within the same VLAN. The number of MAC addresses that the device can secure is configurable per interface.

1.6.5.3 IP Source Guard

IP Source Guard is a per-interface traffic filter that permits IP traffic only when the IP address and MAC address of each packet matches one of two sources of IP and MAC address bindings:

- ◆ Entries in the DHCP snooping binding table.
- ◆ Administratively configured static IP source entries.

1.6.5.4 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.

1.6.5.5 Control Plane Policing

The supervisor module component of the Nexus 7000 switch handles both management plane and control plane traffic and is critical to the operation of the network. Any disruption to the supervisor module would result in serious network outages. Excessive

traffic to the supervisor module could overload it and slow down the performance of the entire TOE.

To protect the control plane, the TOE segregates different packets destined to the control plane into different classes. Once these classes are identified, the Nexus 7000 switch polices or marks down packets, which ensures that the supervisor module is not overwhelmed.

1.6.5.6 Rate Limiting

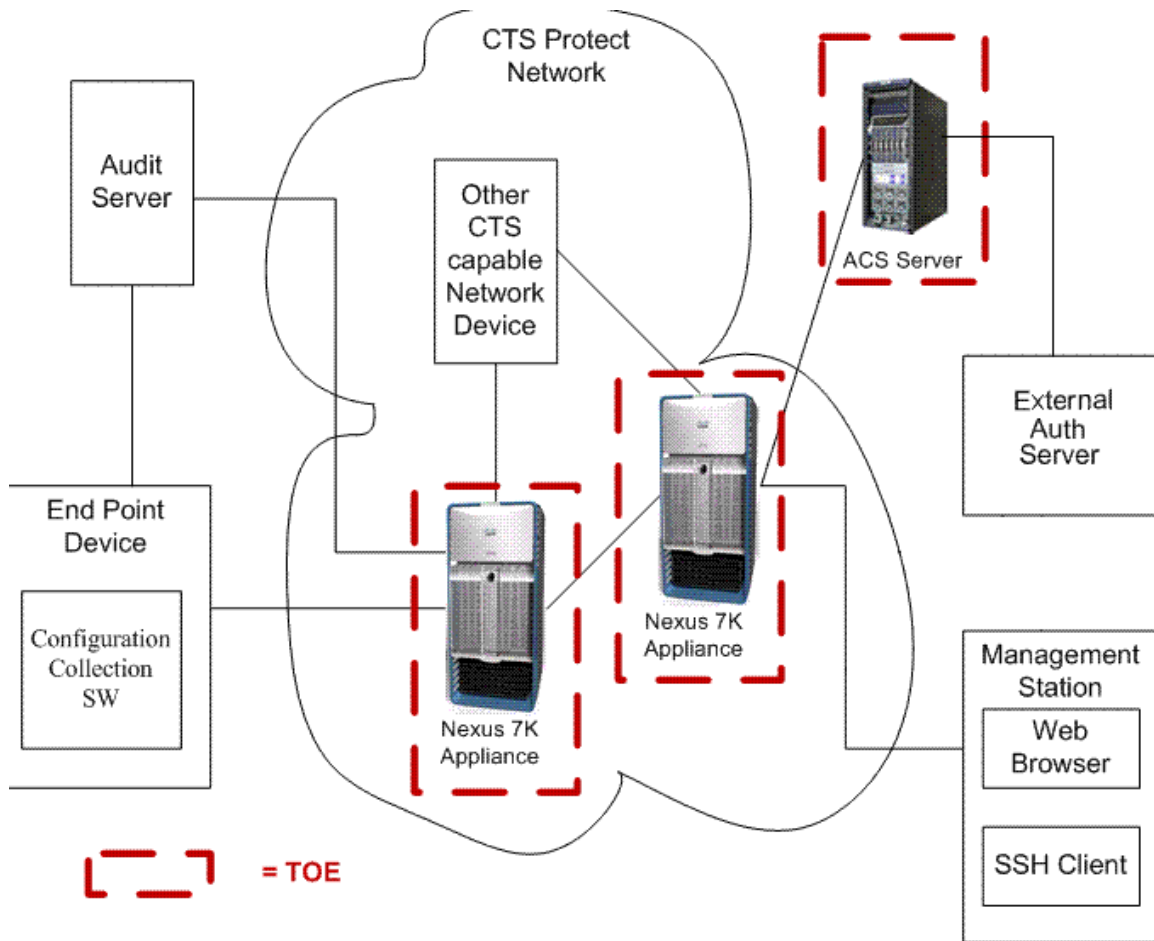
Rate limits on outgoing traffic can prevent redirected packets for egress exceptions from overwhelming the supervisor module on the Nexus 7000 switch. You can configure rate limits in packets per second for the following types of redirected packets: Access list logging packets, Data and control packets copied to the supervisor module, Layer 2 storm control packets, Layer 2 port security packets, Layer 3 glean packets, Layer 3 maximum transmission unit (MTU) check failure packets, Layer 3 multicast directly connected packets, Layer 3 Time-to-Live (TTL) check failure packets, and Receive packets.

1.6.5.7 DHCP Snooping – Dynamic ARP Inspection

DHCP snooping acts like a firewall between untrusted hosts and trusted DHCP servers. DHCP snooping performs the following activities: Validates DHCP messages received from untrusted sources and filters out invalid messages. Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses. Using information extracted from intercepted DHCP messages, DHCP snooping dynamically builds and maintains a database. Dynamic ARP Inspection ensures that only valid ARP requests and responses are relayed. When DAI is enabled the Nexus 7000 switch performs these activities: Intercepts all ARP requests and responses on untrusted ports. Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination. Drops invalid ARP packets.

1.7 TOE Evaluated Configuration

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



The previous figure includes the following:

- ◆ One or more Nexus 7000 switch TOE components (the figure includes two Nexus 7000 switches)
- ◆ ACS TOE component
- ◆ Other CTS capable network devices (IT environment)
- ◆ End point device (IT environment)
- ◆ Audit Server (IT environment)
- ◆ Configuration Collection Software (IT environment)
- ◆ Management Station (IT environment)
- ◆ Web Browser (IT environment)
- ◆ SSH Client (IT environment)
- ◆ External Authentication Server (IT Environment)

1.7.1 Excluded Functionality

The following functionality has been excluded from the evaluation and must not be used with the TOE:

- Telnet Management – excluded because credentials are sent via clear text.

- SNMP Management – excluded because weak crypto is used and the roles do not provide access to the required security functionality.

DRAFT

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 3, dated: July 2009.

The TOE and ST are EAL4 Augmented with ALC_FLR.2 Part 3 conformant.

The TOE and ST are CC Part 2 conformant

2.2 Protection Profile Conformance

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

DRAFT

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 8 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 accessed by authorized users.

3.2 Threats

Table 9 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 unsophisticated.

Table 9 Threats

Threat Name	Threat Definition
T.AVAIL	An attacker may prevent the availability of Nexus 7000 switch services by attacking the switch using network based attacks.
T.NETTRAFFIC	An unauthorized user may send network traffic to unauthorized destinations through the Nexus 7000 switch without detection.

Threat Name	Threat Definition
T.UNAUTHDEVICE	An unauthorized end point or network device may obtain access to the CTS network.
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.NETWORK-C&I	An attacker may view or modify network traffic sent within the CTS network without detection.
T.ADMINAUDIT	An authorized or unauthorized administrative user may make configuration changes to the Nexus 7000 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.VDCCOMP	An attacker may be able to affect the proper functioning of a VDC on the Nexus 7000 switch by attacking a different VDC on the Nexus 7000 switch.
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 7000 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 10 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

Table 11: Security Objectives for the TOE identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Table 11 Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.Nexus7KAvail	The TOE shall ensure the availability of its services on one vdc even when subjected to network traffic based attacks on another vdc.
O.DataFlowControl	The TOE shall ensure that only authorized traffic is permitted to flow through the TOE to its destination.
O.Endpt/NetwkDeviceAuth	The TOE shall be able to identify and authenticate Endpoints and Network Devices prior to allowing access to TOE functions and data.
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.CTS-PC&I	The TOE shall ensure that packets within the CTS network are protected from unauthorized disclosure or modification.
O.Audit	The TOE shall record audit records for RACLs, 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.VDCSec	The TOE shall ensure that each VDC within the Nexus 7000 switch does not interfere with other VDCs within the same Nexus 7000 switch.

TOE Security Obj.	TOE Security Objective Definition
O.VRFSec	The TOE shall provide VRFs and ensure that traffic received by the Nexus 7000 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 12: Security Objectives for the Environment identifies the security objectives for the environment.

Table 12 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 (both the Nexus 7000 switch 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.
OE.CTSCOMPATIBLE	The environment may include devices that support CTS-enabled communications.
OE.EXTERNALAUTH	The environment shall optionally provide authentication credential verification 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 13: How Security Objectives Map to Threats, Assumptions, and OSPs

	O.Nexus7KAvail	O.DataFlowControl	O.Endpt/NetwkDeviceAuth	O.Admin	O.AdminAuth	O.AdminAccess	O.CTS-PC&I	O.Audit	O.AuditIntegrity	O.SecureMgtComm	OE.PERSON	OE.INSTALL	OE.PHYCAL	OE.TIME	OE.CTSCOMPATIBLE	O.VDCSec	O.VDCSec	OE.EXTENLAUTH
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.UNAUTHDEVICE			X															X
T.IMPCONF				X		X												
T.ADMINAUTHOR					X	X												
T.NETWORK-C&I							X								X			
T.ADMINAUDIT								X										
T.AUDITCOMP									X									
T.ADMINTRAF-C&I										X								
T.VDCCOMP																X		
T.VRFCOMP																	X	
P.ACCOUNTABLE			X					X						X				

Table 14: 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

Threat/Assumption	Objective	Rationale
		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.Nexus7KAvail	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 7000 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 7000. 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.UNAUTHDEVICE	O.Endpt/NetwkDeviceAuth	This objective counters this threat by providing the ability to authenticate all devices attempting to access the TOE protected network. This object also provides that access can be denied until the device is authenticated.
	OE.EXTERNALAUTH	This objective counters this threat by providing the ability to authenticate all devices attempting to access the TOE protected network via ACS communications with an external authentication server.
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 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.

Threat/Assumption	Objective	Rationale
	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.NETWORK-C&I	O.CTS-PC&I	This objective helps to counter this threat by providing the TOE capability to encrypt and decrypt message sent on the TOE protected network. This protects traffic from unauthorized disclosure. This objective also provides that the TOE is able verify the integrity of the network traffic. This prevents traffic from being modified without knowledge.
	OE.CTSCOMPATIBLE	This objective provides the environment with CTS compatible devices. CTS compatible devices allow the device to pass and receive network traffic from the TOE in an encrypted and integrity checked manner.
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.VDCCOMP	O.VDCSec	This objective counters this threat by ensuring that Virtual Device Context operate in a self-contained environment and do not share common resources. This prevents failure or compromise of one Virtual Device Context to affect the operation of another Virtual Device Context.
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.Endpt/NetwkDeviceAuth	This objective upholds this policy by requiring that all devices that connect to the network be identified. The TOE can use the identity of the device to track any actions performed by the device.
	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

Threat/Assumption	Objective	Rationale
		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 option 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.

DRAFT

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 3* 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 15 are described in more detail in the following subsections.

Table 15 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
FAU_SAR.1(2)	Audit review
FAU_STG.1	Protected audit trail storage
FCS_CKM.1(1)	Cryptographic key generation
FCS_CKM.1(2)	Cryptographic key generation
FCS_CKM.1(4)	Cryptographic key generation
FCS_CKM.1(5)	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1(1)	Cryptographic operation
FCS_COP.1(2)	Cryptographic operation
FCS_COP.1(3)	Cryptographic operation
FCS_COP.1(5)	Cryptographic operation
FCS_COP.1(6)	Cryptographic operation
FCS_COP.1(7)	Cryptographic operation
FCS_COP.1(8)	Cryptographic operation
FDP_ACC.1 (1)	Subset access control
FDP_ACC.1 (2)	Subset access control
FDP_ACF.1 (1)	Security attribute based access control
FDP_ACF.1 (2)	Security attribute based access control
FDP_IFC.1(1)	Subset information flow control

Functional Component	
FDP_IFC.1(2)	Subset information flow control
FDP_IFF.1(1)	Simple security attributes
FDP_IFF.1(2)	Simple security attributes
FIA_UAU.1(1)	Timing of authentication
FIA_UAU.1(2)	Timing of authentication
FIA_UAU.1(3)	Timing of authentication
FIA_UAU.1(4)	Timing of authentication
FIA_UAU.5(1)	Multiple authentication mechanisms
FIA_UAU.5(2)	Multiple authentication mechanisms
FIA_UAU.5(3)	Multiple authentication mechanisms
FIA_UID.1(1)	Timing of identification
FIA_UID.1(2)	Timing of identification
FIA_UID.1(3)	Timing of identification
FIA_UID.1(4)	Timing of identification
FMT_MSA.1(1)	Management of security attributes
FMT_MSA.1(2)	Management of security attributes
FMT_MSA.1(3)	Management of security attributes
FMT_MSA.1(4)	Management of security attributes
FMT_MSA.3(1)	Static attribute initialisation
FMT_MSA.3(2)	Static attribute initialisation
FMT_MSA.3(3)	Static attribute initialisation
FMT_MSA.3(4)	Static attribute initialisation
FMT_MTD.1(1)	Management of TSF data
FMT_MTD.1(2)	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_FLS.1	Failure with preservation of secure state
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) [
 - *When a packet matches a configured RACL, PACL IP ACLs rule;*
 - *When a packet matches a configured VACL IP ACLs rule;*
 - *When a packet matches a configured PACL MAC ACLs rule;*
 - *When a packet matches a configured VACL MAC ACLs rule;*
 - *Configuration Changes on the Nexus 7000 switch;*
 - *Administrative Authentication on the Nexus 7000 switch;*
 - *Administrative Log-off on the Nexus 7000 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 16: ACL Audit Information

Audited Action	Recorded Information
When a packet matches a configured RACL, PACL IP ACLs rule	Protocol Whether the packet is a TCP, UDP, ICMP, or “other” (Other refers to any type of packet other than TCP, UDP, or ICMP. The TOE records “other” in the audit log for packets other than TCP, UDP, or ICMP packets.) type Source address Destination address Source Port (if applicable) Destination Port (if applicable)
When a packet matches a configured VACL IP ACLs rule	Protocol Whether the packet is a TCP, UDP, ICMP, or “other” (Other refers to any type of packet other than TCP, UDP, or ICMP. The TOE records “other” in the audit log for packets other than TCP, UDP, or ICMP packets.) type Source address Destination address Source Port (if applicable) Destination Port (if applicable)
When a packet matches a configured PACL MAC ACLs rule	Protocol Whether the packet is a TCP, UDP, ICMP, or “other” (Other refers to any type of packet other than TCP, UDP, or ICMP. The TOE records “other” in the audit log for packets other than TCP, UDP, or ICMP packets.) type Source address Destination address Source Port (if applicable) Destination Port (if applicable)
When a packet matches a configured VACL MAC ACLs rule	Protocol Whether the packet is a TCP, UDP, ICMP, or “other” (Other refers to any type of packet other than TCP, UDP, or ICMP. The TOE records “other” in the audit log for packets other than TCP, UDP, or ICMP packets.) type Source address Destination address Source Port (if applicable) Destination Port (if applicable)
Configuration Changes on the Nexus 7000 switch	Day of Week, Date, Action, User, status of the configuration change, terminal information (when applicable)

Audited Action	Recorded Information
Administrative Authentication on the Nexus 7000 switch	Day of Week, Date, Action, User, terminal information (when applicable)
Administrative Log-off on the Nexus 7000 switch	Day of Week, Date, Action, User, terminal information (when applicable)
Configuration Changes	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)
Administrative Authentication	User ID, Interface on which the action took place (CLI or GUI), Time and Date, the action that took place,
Administrative Log-off	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 7000 Related Logging

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

- ◆ *network-admin/network-operator can read all information within the audit records stored within the Nexus 7000 regardless of VDC.*
- ◆ *vdc-admin/vdc-operator can read all information within the audit records associated with the administrator's VDC stored within the Nexus 7000.*
- ◆ *Administrator defined role(s) can read all information within the audit records (consistent with the role definition) associated with the administrator's VDC stored within the Nexus 7000]*

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 [*ReportAdmin (ACS Predefined GUI role), SuperAdmin (ACS Predefined GUI role), Admin (ACS Predefined CLI role), and Operator (ACS Predefined CLI role)*] 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] and specified cryptographic key sizes [512, 1024, 2048, or 4096-bits] that meet the following: [FIPS 140-2].

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 17: Cryptographic Key Generation Provided by the TOE (RSA)

Usage	Purpose
TLS/GUI Key Generation	The key that is used to protect a TLS/GUI session.
EAP-FAST Key Generation	The key that is used to protect an EAP-FAST authentication session.
SSH Key Generation	The generated key is used for SSH hosts.

5.2.1.1.6 FCS_CKM.1(2) Cryptographic key generation - Diffie-Hellman

FCS_CKM.1.1(2) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [Diffie-Hellman (Group 1, Group 14)] and specified cryptographic key sizes [64, 128, 192, and 256 bits] that meet the following: [FIPS 140-2].

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 or FCS_COP.1], FCS_CKM.4

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

Usage	Purpose
SSH Key Generation	The generated key is used to protect an SSH session.
TLS Key Generation	The generated key is used to protect a TLS session.
EAP-FAST Key Generation	The generated key is used to protect an EAP-FAST session.

5.2.1.1.7 FCS_CKM.1(4) ¹Cryptographic key generation – PAC Key Generation

¹ Although iteration 3 has been removed, the iteration numbering is being preserved for consistency with other documents.

FCS_CKM.1.1(4) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*EAP-FAST*] and specified cryptographic key sizes [*256 bits*] that meet the following: [*FIPS 140-2*].

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 or FCS_COP.1], FCS_CKM.4

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

Table 18: PAC Key Creation Provided by the TOE

Usage	Purpose
EAP-FAST	Creates the PAC Key that is used to establish an EAP-FAST communication session
PAC Secured-RADIUS	Creates the PAC Key that is used to establish PAC Secured-RADIUS

5.2.1.1.8 FCS_CKM.1(5) Cryptographic key generation – HMAC-SHA-1 Based Key Generation

FCS_CKM.1.1(5) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*HMAC-SHA1*] and specified cryptographic key sizes [*128 bits*] that meet the following: [*FIPS 140-2*].

Table 19: HMAC-SHA1 Based Key Generation

Usage	Purpose
Initial SAP session establishment	Cryptographic algorithm used to generate the key in the initial SAP session establishment
SAP session rekey	Cryptographic algorithm used to generate the key in the SAP session rekey
RADIUS KeyWrap authentication	Cryptographic algorithm used to authenticate the RADIUS message.
PAC authentication	Cryptographic algorithm used to authenticate the PAC.

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 or FCS_COP.1], FCS_CKM.4

5.2.1.1.9 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2 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 20: Cryptographic Key Destruction Provided by the TOE

Usage	Purpose
EAP-FAST Tunnel Teardown	After an EAP-FAST based authentication (endpoint or network

Usage	Purpose
	device), the tunnel is torn down and the session key is overwritten.
CTS Tunnel Teardown	The TOE tears down a CTS tunnel after a CTS session between two network devices are finished.
SSH/SFTP Tunnel Teardown	After TOE administration via SSH/SFTP is completed, the tunnel is torn down and the session key is overwritten.
TLS Tunnel Teardown	After TOE administration via TLS is completed, the tunnel is torn down and the session key is overwritten.

5.2.1.1.10 *FCS_COP.1(1) Cryptographic operation – RSA signature verification*

FCS_COP.1.1(1) The TSF shall perform [*Encryption/Decryption*] in accordance with a specified cryptographic algorithm [*RSA*] and cryptographic key sizes [*512-bits to 4096-bits*] that meet the following: [*FIPS 140-2*].

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 21: RSA Encryption/Decryption Provided by the TOE

Usage	Purpose
EAP-FAST	This provides the asymmetric encryption used as part of the session setup process for EAP-FAST communications.
TLS	This provides the asymmetric encryption used as part of the session setup process for TLS communications.

5.2.1.1.11 *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)*] and cryptographic key sizes [*128-bits*] that meet the following: [*FIPS 140-2*].

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

Table 22: AES Encryption/Decryption Provided by the TOE

Usage	Purpose
EAP-FAST	Provides data protection using symmetric encryption and decryption for EAP-FAST communications.
CTS	This provides packet confidentiality during protected network device to network device communication.
SSH/SFTP	This provides the protection for SSH/SFTP based administrative communication.
TLS	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

5.2.1.1.12 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*] and cryptographic key sizes [*168-bits*] that meet the following: [*FIPS 140-2*].

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 Triple-DES encryption and decryption for the following purposes:

Table 23: Triple-DES Encryption/Decryption Provided by the TOE

Usage	Purpose
SSH/SFTP	Provides data protection using symmetric encryption and decryption for SSH/SFTP communications.
TLS	Provides data protection using symmetric encryption and decryption for TLS communications.

5.2.1.1.13 FCS_COP.1(5)² Cryptographic operation - SHS Hashing

FCS_COP.1.1(5) 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 140-2*].

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 24: SHS Hashing Provided by the TOE

Usage	Purpose
EAP-FAST	Provides the hashing required as part of the EAP-FAST session establishment protocol.
TLS	Provides the hashing required as part of the TLS session establishment protocol.
RADIUS-KeyWrap	Provides the hashing required as part of the RADIUS-KeyWrap session establishment protocol.

5.2.1.1.14 FCS_COP.1(6) Cryptographic operation – MD5 Hashing

FCS_COP.1.1(6) 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: [*FIPS 140-2*].

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 MD5 Hashing for the following purposes:

² Although iteration 4 has been removed, the iteration numbering is being preserved for consistency with other documents.

Table 25: MD5 Hashing Provided by the TOE

Usage	Purpose
TACACS+	Provides the hashing protection required by the TACACS+ protocol

5.2.1.1.15 FCS_COP.1(7) Cryptographic operation – GMAC Message Authentication

FCS_COP.1.1(7) The TSF shall perform [*Message Authentication*] in accordance with a specified cryptographic algorithm [*Advanced Encryption Standard Galois Message Authentication Code (AES-GMAC)*] and cryptographic key sizes [*128-bit*] that meet the following: [*FIPS 140-2*].

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 GMAC message authentication for the following purposes:

Table 26: GMAC Message Authentication Provided by the TOE

Usage	Purpose
CTS	Provides packet integrity for packets sent on the CTS network.

5.2.1.1.16 FCS_COP.1(8) Cryptographic operation – DSA E/D

FCS_COP.1.1(8) The TSF shall perform [*Encryption/Decryption*] in accordance with a specified cryptographic algorithm [*DSA*] and cryptographic key sizes [*768-bits to 2048-bits*] that meet the following: [*FIPS 140-2*].

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 encryption and decryption for the following purposes:

Table 27: DSA Encryption/Decryption Provided by the TOE

Usage	Purpose
SSH/SFTP	Provides data protection using symmetric encryption and decryption for SSH/SFTP communications.

5.2.1.1.17 FDP_ACC.1(1) Subset access control – Administrative RBAC

FDP_ACC.1.1(1) The TSF shall enforce the [*RBAC*] on [

Subject:

- ◆ *Authenticated user/Processes acting on behalf of authenticated user;*

Objects:

- ◆ *Commands - Individual commands available through the Nexus 7000 CLI administrative interface;*

- ◆ *Features* – These are collections of commands available through the Nexus 7000 CLI administrative interface;
- ◆ *Feature Groups* – These are collections of features available through the Nexus 7000 CLI administrative interface.

Operations:

- ◆ *Permit Read Access;*
- ◆ *Permit Write Access;*
- ◆ *Deny Access*].

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

5.2.1.1.18 FDP_ACC.1(2) Subset access control – Key Chains

FDP_ACC.1.1(2) The TSF shall enforce the [*Key Chains*] on [

Subject:

- ◆ *Network Device (Nexus 7000 switch TOE component)*

Objects:

- ◆ *TOE Cryptographic Keys*

Operations:

- ◆ *Use*
- ◆ *Not use*].

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

5.2.1.1.19 FDP_ACF.1(1) Security attribute based access control – Administrative RBAC Nexus 7000 Switch

FDP_ACF.1.1(1) The TSF shall enforce the [*RBAC*] to objects based on the following:

[*Subject security attributes:*

- ◆ *Authenticated user/Processes acting on behalf of authenticated user:*
 - *User Identity;*
 - *Role Assignment(s)*

Objects security attributes:

- ◆ *Commands*
 - *Role Privilege*
- ◆ *Features*
 - *Role Privilege*
- ◆ *Feature Groups*
 - *Role Privilege*].

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- ◆ *Authenticated users are permitted read access to Commands, Features, or Feature Groups if the role definition(s) of the authenticated users' role assignment(s) grant access to the Commands, Features, or Feature Groups; and;*

- ◆ *Authenticated users are permitted write access to Commands, Features, or Feature Groups if the role definition(s) of the authenticated users' role assignment(s) grant access to the Commands, Features, or Feature Groups; and;*
- ◆ *Authenticated users are denied any access to Commands, Features, or Feature Groups if the role definition(s) of the authenticated users' role assignment(s) denies access to the Commands, Features, or Feature Groups; and;*
- ◆ *If an authenticated user has multiple role assignments and the role definitions for individual role assignments conflict with regards to access to a particular Command, Feature, or Feature Group, access being allowed to the Command, Feature, or Feature Group takes priority over being denied access to the Command, Feature, or Feature Group].*

FDP_ACF.1.3(1) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*Authenticated users with the role assignment "network-admin" are permitted read access and write access to all Commands, Features, and Feature Groups*].

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the [*none*].

Hierarchical to: No other components.

Dependencies: FDP_ACC.1, FMT_MSA.3

5.2.1.1.20 FDP_ACF.1(2) Security attribute based access control – Key Chains

FDP_ACF.1.1(2) The TSF shall enforce the [*Key Chains*] to objects based on the following: [

Network Device (Subject) security attributes:

- ◆ *Device Identity*
- ◆ *Associated TOE Cryptographic Keys*

TOE Cryptographic Keys (Objects) security attributes:

- ◆ *Accept start-time*
- ◆ *Accept Duration (One of the following: duration value in seconds, infinite, end-time)*
- ◆ *Send start-time*
- ◆ *Send Duration (One of the following: duration value in seconds, infinite, end-time)].*

FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- ◆ *The TOE will accept a communication from a network device on the CTS network using a specified cryptographic key (as part of the authentication process) if the following holds true:*

- *The communication starts after the configured “Accept start-time” associated with the cryptographic key*
- *The communication occurs during the “Accept Duration” (“Accept Duration” is specified as one of the following, infinite, before a configured end time and date, or in seconds after the “Accept start-time”) associated with the cryptographic key*
- ◆ *The TOE will send communications to a network device on the CTS network using a specified cryptographic key (as part of the authentication process) if the following holds true:*
 - *The communication starts after the configured “Send start-time” associated with the cryptographic key*
 - *The communication occurs during the “Send Duration” (“Send Duration” is specified as one of the following, infinite, before a configured end time and date, or in seconds after the “Send start-time”) associated with the cryptographic key].*

FDP_ACF.1.3(2) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

FDP_ACF.1.4(2) The TSF shall explicitly deny access of subjects to objects based on the [*none*].

Hierarchical to: No other components.

Dependencies: FDP_ACC.1, FMT_MSA.3

5.2.1.1.21 FDP_IFC.1(1) Subset information flow control

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

- ◆ *Nexus 7000 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*
 - *Tunnels*
 - *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:

- ◆ *Permit traffic flow*
- ◆ *Deny traffic flow*].

Hierarchical to: No other components.

Dependencies: FDP_IFF.1

5.2.1.1.22 FDP_IFC.1(2) Subset information flow control – Control Plane Policing/Rate Limiting

FDP_IFC.1.1(2) The TSF shall enforce the [*Control Plane Policing/Rate Limiting*] on [Subjects:

- ◆ *Nexus 7000 Supervisor interfaces*

Information:

- ◆ *Ingress Control Plane Traffic (routing protocol control traffic);*
- ◆ *Egress Network Traffic from the Supervisor card*

Operations:

- ◆ *Transmit Control Plane Traffic Flow;*
- ◆ *Drop Control Plane Traffic Flow;*
- ◆ *Mark Down (downgrade the QoS) the Control Plane Traffic Flow;*
- ◆ *Permit Egress Network Traffic Flow;*
- ◆ *Deny Egress Network Traffic Flow*].

Hierarchical to: No other components.

Dependencies: FDP_IFF.1

5.2.1.1.23 FDP_IFF.1(1) Simple security attributes

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

[Subject security attributes:

- ◆ *Nexus 7000 interfaces*
 - *Port Security policy, IP Source Guard Policy, Traffic Storm threshold, DHCP Snooping Policy, Dynamic ARP Inspection policy, PACL/VACL/RACL/SGACL policies configured for the Nexus 7000 interfaces*
- ◆ *Source Network Device*
 - *Security Group Tag (SGT)*
- ◆ *Destination Network Device*
 - *Destination Group Tag (DGT)*

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*
- *Packet length*
- *Precedence*
- *DSCP Value*
- *Destination interface (specific to DHCP/ARP IP traffic)*
- *MAC address of the presumed host (specific to DHCP/ARP IP traffic)*
- *leased IP address of the presumed host (specific to DHCP/ARP IP traffic)*
- *VLAN number of the presumed host (specific to DHCP/ARP IP traffic)*
- *Source Network Device associated with the traffic*
- *Destination Network Device associated with the traffic*
- ◆ *Non-IP Packets*
 - *Source MAC address*
 - *Destination MAC address*
 - *Protocol*
 - *Class of Service (COS)*
 - *VLAN ID*
 - *Traffic Type: Broadcast Traffic, Unicast Traffic, Multicast Traffic*
 - *Source Network Device associated with the traffic*
 - *Destination Network Device associated with the 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. *Port Security/IP Source Guard/Traffic Storm/DHCP Snooping/Dynamic ARP Inspection (all applied at the same time)*
2. *PACL MAC ACLs*
3. *VRFs*
4. *VACL IP/MAC ACLs*
5. *RACL IP/MAC ACLs*
6. *SGACL*

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

- ◆ *Port Security*
 - *Network traffic flow is permitted if the source MAC address is administratively configured as secure for the Nexus 7000 interface, or,*
 - *The source MAC address is dynamically identified as secure by the TOE. A source MAC address is dynamically identified as secure if the following criteria are met,*
 - *The Nexus 7000 has not reached any connection maximums;*

- *The source MAC address has not already been secured for another port within the same VLAN*
- *And, the network traffic flow is not denied by any IP Source Guard/Traffic Storm/DHCP Snooping/Dynamic ARP Inspection policies*
- *If a Nexus 7000 interface receives network traffic from a source MAC address that is not identified as secure, one of the following actions takes place, the ingress port is disabled or the network traffic flow is denied based on the administratively configured policy*
- ◆ *IP Source Guard*
 - *Network traffic flow is permitted if the Source IP address and MAC address combination are administratively configured as a valid combination, or,*
 - *The Source IP address and MAC address combination were previously identified as a valid combination by the TOE through DHCP Snooping*
 - *And, the network traffic flow is not denied by any Port Security/Traffic Storm/DHCP Snooping/Dynamic ARP Inspection policies*
- ◆ *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*
 - *And, the network traffic flow is not denied by any IP Source Guard/Port Security/DHCP Snooping/Dynamic ARP Inspection policies*
 - *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*
- ◆ *DHCP Snooping*
 - *The Nexus 7000 switch permits DHCP traffic to flow unless any of the following conditions (listed in the four indented bullets directly below) occur (in which case the traffic flow is denied):*
 - *The Nexus 7000 switch receives a DHCP response packet (such as DHCPACK, DHCPNAK, or DHCPOFFER packet) on an untrusted interface*
 - *The Nexus 7000 receives a packet on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match. This check is performed only if the DHCP snooping MAC address verification option is turned on*
 - *The Nexus 7000 receives a DHCPRELEASE or DHCPDECLINE message from an untrusted host with an entry in the DHCP snooping binding table,*

and the interface information in the binding table does not match the interface on which the message was received

- *And, the network traffic flow is not denied by any IP Source Guard/Traffic Storm/Port Security/Dynamic ARP Inspection policies*

◆ *Dynamic ARP Inspection*

- *The TOE permits ARP traffic flows received on an untrusted Nexus 7000 switch interface to the appropriate destination if a valid IP-to-MAC address binding exists within the DHCP binding table*
- *And, the network traffic flow is not denied by any IP Source Guard/Traffic Storm/DHCP Snooping/Port Security policies*
- *The TOE denies ARP traffic flows received on an untrusted Nexus 7000 switch interface if a valid IP-to-MAC address binding does not exist within the DHCP binding table*

◆ *PACL MAC ACLs*

- *Ingress Non-IP traffic with security attributes that match an administratively configured PACL permit policy for non-IP traffic rule is allowed to flow, or,*
- *Ingress Non-IP traffic with security attributes that match an administratively configured deny policy rule is not permitted.*

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

◆ *VRFs*

- *IP traffic with security attributes that map to a configured VRF will be forwarded through the Nexus 7000 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, or,*
- *IP traffic with security attributes that match an administratively configured deny policy rule is not permitted to flow. IP traffic with security attributes that match an administratively configured redirect policy rule is redirected to the specified interface, or,*
- *IP traffic with security attributes that match an administratively configured deny-and-log policy rule is not permitted to flow and a copy of the traffic is logged by the TOE, or,*

The permit/deny/redirect/deny-and-log policies for IP traffic are comprised of a combination of subject security attributes and information attributes and a

permit/deny/redirect/deny-and-log operation. The subject attributes that are available for the creation of permit/deny/redirect/deny-and-log policies include: vlan-ID. The information attributes that are available for the creation of permit/deny/redirect/deny-and-log policies include: Source IP address, Destination IP address, Source port number, Destination port number, Protocol, ICMP message type, ICMP message code, IGMP message type, Packet length, Precedence, DSCP Value

- *Non-IP traffic with security attributes that match an administratively configured permit policy rule is allowed to flow, or,*
- *Non-IP traffic with security attributes that match an administratively configured deny policy rule is not permitted to flow. Non-IP traffic with security attributes that match an administratively configured redirect policy rule is redirected to the specified interface, or,*
- *Non-IP traffic with security attributes that match an administratively configured deny-and-log policy rule is not permitted to flow.*

The permit/deny/redirect/deny-and-log policies 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/redirect/deny-and-log policies include: vlan-ID. The information attributes that are available for the creation of these permit/deny/redirect/deny-and-log policies include: Source MAC address, Destination MAC address, Protocol, Class of Service (COS), or VLAN ID

◆ *RACL IP/MAC ACLs*

- *Ingress or egress IP traffic with security attributes that match an administratively configured RACL permit policy rule is allowed to flow, or,*
- *Ingress or egress IP traffic with security attributes that match an administratively configured RACL deny policy for IP traffic rule is not permitted.*

The RACL permit/deny policies for IP traffic are comprised of a combination of information attributes and a permit/deny operation. The information attributes that are available for the creation of RACL permit/deny policies include: Source IP address, Destination IP address, Source port number, Destination port number, Protocol, ICMP message type, ICMP message code, IGMP message type, Packet length, Precedence, DSCP Value

◆ *SGACL*

- *Network traffic is permitted to flow to its destination if an administratively configured SGACL policy rule with the SGT/DGT pair associated with the network traffic's Source SGT and Destination (DGT) explicitly allows it, or,*
- *Network traffic is not permitted to flow to its destination if an administratively configured SGACL policy rule with the SGT/DGT pair associated with the network traffic's Source SGT and Destination (DGT) explicitly disallows it*

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

- *none*].

FDP_IFF.1.4(1) The TSF shall explicitly authorise an information flow based on the following rules: [

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

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

For IP Network Traffic Flows:

- ◆ *The TOE denies IP traffic flow when the IP address and MAC address of the traffic are not identified as a valid combination either through DHCP Snooping or administrative configuration, or,*
- ◆ *For IP traffic, if the security attributes do not match an administratively configured RACL or VACL, the traffic flow is denied, or,*
- ◆ *If the IP traffic security attributes do not map to a configured VRF, the traffic flow is denied*

For Non-IP Network Traffic Flows:

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

Hierarchical to: No other components.

Dependencies: FDP_IFC.1, FMT_MSA.3

5.2.1.1.24 FDP_IFF.1(2) Simple security attributes – Control Plane Policing/Rate Limiting

FDP_IFF.1.1(2) The TSF shall enforce the [*Control Plane Policing/Rate Limiting*] based on the following types of subject and information security attributes:

[*Nexus 7000 Supervisor interfaces (subject) security attributes:*

- ◆ *Committed information rate (CIR) (Desired bandwidth);*
- ◆ *Peak information rate (PIR) (Rate above which data traffic is negatively affected);*
- ◆ *Committed burst (BC) (Size of a traffic burst that can exceed the CIR within a given unit of time and not impact scheduling);*
- ◆ *Extended burst (BE) (Size that a traffic burst can reach before all traffic exceeds the PIR);*
- ◆ *Configured Rate Limit per traffic type*

Ingress Control Plane Traffic (information) security attributes:

- ◆ *Source IP address*

- ◆ *Destination IP address*
- ◆ *Source MAC address*
- ◆ *Destination MAC address*
- ◆ *VLAN*
- ◆ *Source port*
- ◆ *Destination port*

Egress Network Traffic (information) security attributes:

- ◆ *Access list logging packets*
- ◆ *Data and control packets copied to the supervisor module*
- ◆ *Layer 2 storm control packets*
- ◆ *Layer 2 port security packets*
- ◆ *Layer 3 glean packets*
- ◆ *Layer 3 maximum transmission unit (MTU) check failure packets*
- ◆ *Layer 3 multicast directly connected packets*
- ◆ *Layer 3 Time-to-Live (TTL) check failure packets*
- ◆ *Receive packets*].

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 ingress Control Plane Traffic with security attributes that match the administratively configured Control Plane Traffic policy (Source IP address, Destination IP address, Source MAC address, Destination MAC address, VLAN, Source port, Destination port) does not exceed the configured rate limits for CIR, PIR, BC, or BE, the traffic is permitted to flow, and,*
- ◆ *If the Egress Network Traffic does not exceed the configured Rate Limit for its traffic type (Access list logging packets, Data and control packets copied to the supervisor module, Layer 2 storm control packets, Layer 2 port security packets, Layer 3 glean packets, Layer 3 maximum transmission unit (MTU) check failure packets, Layer 3 multicast directly connected packets, Layer 3 Time-to-Live (TTL) check failure packets, Receive packets), the traffic is permitted to flow*
- ◆ *If ingress Control Plane Traffic with security attributes that match the administratively configured Control Plane Traffic policy (Source IP address, Destination IP address, Source MAC address, Destination MAC address, VLAN, Source port, Destination port) exceeds the administratively configured threshold for CIR, PIR, BC, or BE, the traffic will be dropped or Marked Down based on the administratively configured policy, or,*
- ◆ *If the Egress Network Traffic exceeds the configured Rate Limit for its traffic type (Access list logging packets, Data and control packets copied to the supervisor module, Layer 2 storm control packets, Layer 2 port security packets, Layer 3 glean packets, Layer 3 maximum transmission unit (MTU) check failure packets, Layer 3 multicast directly connected packets, Layer 3 Time-to-Live (TTL) check failure packets, Receive packets), the traffic is not permitted to flow].*

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

Application Note: Glean packets are packets that indicate unresolved adjacencies of neighboring routers.

5.2.1.1.25 FIA_UAU.1(1) Timing of authentication – Network Device Authentication

FIA_UAU.1.1(1) The TSF shall allow [*EAP-FAST Tunnel Establishment with the Nexus 7000, Administratively configured access for unauthenticated devices*] on behalf of the ~~user~~ **Network Device** to be performed before the ~~user~~ **Network Device** is authenticated.

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

Hierarchical to: No other components.

Dependencies: FIA_UID.1

5.2.1.1.26 FIA_UAU.1(2) Timing of authentication – Endpoint Authentication

FIA_UAU.1.1(2) The TSF shall allow [*Secure Tunnel Establishment, Administratively configured access for unauthenticated Endpoints*] on behalf of the ~~user~~ **Endpoint** to be performed before the ~~user~~ **Endpoint** 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~~ **Endpoint**.

Hierarchical to: No other components.

Dependencies: FIA_UID.1

5.2.1.1.27 FIA_UAU.1(3) Timing of authentication – Nexus 7000 Switch Administrator Authentication

FIA_UAU.1.1(3) The TSF shall allow [*establishment of a secure remote session between the administrative user and the Nexus 7000 Switch TOE component*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2(3) 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

5.2.1.1.28 FIA_UAU.1(4) Timing of authentication – ACS Administrator Authentication

FIA_UAU.1.1(4) 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(4) 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

5.2.1.1.29 FIA_UAU.5(1) Multiple authentication mechanisms – Network Device³

FIA_UAU.5.1(1) The TSF shall provide [*the following authentication mechanism:*

- a) *Password-based Authentication;*
- b) *none]*

to support ~~user~~ **Network Device** authentication.

FIA_UAU.5.2(1) The TSF shall authenticate any ~~user's~~ **Network Device's** claimed identity according to the **following:** [

- a) *For Device ID/Password-based Authentication, the TSF will authenticate the device based on the administratively configured Identification and Authentication scheme*
- b) *none].*

Hierarchical to: No other components.

Dependencies: No dependencies.

5.2.1.1.30 FIA_UAU.5(2) Multiple authentication mechanisms - Endpoint

FIA_UAU.5.1(2) The TSF shall provide [*the following authentication mechanisms:*

- a) *EAP-FAST Authentication;*
- b) *MAC Auth Bypass Authentication]*

to support ~~user~~ **Endpoint** authentication.

³ Although changes to this requirement during evaluation resulted in a single mechanism for the Network Device authentication, the FIA_UAU.5 SFR is still being used to preserve the same requirement iteration format for: network device, endpoint, and N7K administrators.

FIA_UAU.5.2(2) The TSF shall authenticate any ~~user's~~ **Endpoint's** claimed identity according to the **following**: [

- a) *The TSF will authenticate the endpoint based on the administratively configured Identification and Authentication scheme*].

Hierarchical to: No other components.

Dependencies: No dependencies.

5.2.1.1.31 FIA_UAU.5(3) Multiple authentication mechanisms – Nexus 7000 Switch Administrator

FIA_UAU.5.1(3) 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 7000 switch]*
to support user authentication.

FIA_UAU.5.2(3) 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 7000 switch, the TSF will authenticate the administrator based on the administratively configured Identification and Authentication scheme*].

Hierarchical to: No other components.

Dependencies: No dependencies.

5.2.1.1.32 FIA_UID.1(1) Timing of identification – Network Device Identification

FIA_UID.1.1(1) The TSF shall allow [*EAP-FAST Tunnel Establishment, Administratively configured access for unauthenticated devices*] on behalf of the ~~user~~ **Network Device** to be performed before the ~~user~~ **Network Device** is identified.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

5.2.1.1.33 FIA_UID.1(2) Timing of identification – Endpoint Identification

FIA_UID.1.1(2) The TSF shall allow [*Secure Tunnel Establishment, Administratively configured access for unauthenticated Endpoints*] on behalf of the ~~user~~ **Endpoint** to be performed before the ~~user~~ **Endpoint** is identified.

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

Hierarchical to: No other components.

Dependencies: No dependencies.

5.2.1.1.34 FIA_UID.1(3) Timing of identification – Nexus 7000 Switch Administrator Identification

FIA_UID.1.1(3) The TSF shall allow [*establishment of a secure remote session between the administrative user and the Nexus 7000 Switch TOE component*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2(3) 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.

5.2.1.1.35 FIA_UID.1(4) Timing of identification – ACS Administrator Identification

FIA_UID.1.1(4) 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(4) 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.

5.2.1.1.36 FMT_MSA.1(1) Management of security attributes – ACLs SFP

FMT_MSA.1.1(1) The TSF shall enforce the [*ACLs SFP*] 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 28: Role/Operations Associated with ACLs

Role	Operations
network-admin (Resident on the Nexus 7000 Switch)	read, write operations for all security attributes defined within administratively configured ACLs policy rules regardless of VDC. read, write operations for all security attributes defined within administratively configured ACLs policy rules regardless of VDC.
network-operator (Resident on the Nexus 7000 Switch)	Read operations for all security attributes defined within administratively configured ACLs policy rules regardless of VDC.

	read operations for all security attributes defined within administratively configured ACLs policy rules regardless of VDC.
vdc-admin (Resident on the Nexus 7000 Switch)	read, write operations for all security attributes defined within administratively configured ACLs policy rules defined within the administrator's VDC. read, write operations for all security attributes defined within administratively configured ACLs policy rules defined within the administrator's VDC.
vdc-operator (Resident on the Nexus 7000 Switch)	Read operations for all security attributes defined within administratively configured ACLs policy rules defined within the administrator's VDC. Read operations for all security attributes defined within administratively configured ACLs policy rules defined within the administrator's VDC.
Administrator defined role(s) (Resident on the Nexus 7000 Switch)	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

5.2.1.1.37 *FMT_MSA.1(2) Management of security attributes – Control Plane Policing/Rate Limiting SFP*

FMT_MSA.1.1(2) The TSF shall enforce the [*Control Plane Policing/Rate Limiting*] to restrict the ability to [*read, write*] the security attributes [*the security attributes found in administratively configured Control Plane Policing/Rate Limiting rules*] to [*the roles/operations defined in the following table*].

Table 29: Role/Operations Associated with Control Plane Policing

Role (Resident on the Nexus 7000 Switch)	Operations
network-admin	read, write operations for all security attributes defined within administratively configured Control Plane Policing policy rules regardless of VDC. read, write operations for rate limits per traffic type.
network-operator	read operations for all security attributes defined within administratively configured Control Plane Policing policy rules regardless of VDC. read operations for rate limits per traffic type.
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

5.2.1.1.38 *FMT_MSA.1(3) Management of security attributes – RBAC SFP*

FMT_MSA.1.1(3) The TSF shall enforce the [*RBAC*] to restrict the ability to [*read, write*] the security attributes [*defined within administratively configured RBAC*] to [*the roles/operations defined in the following table*].

Table 30: Role/Operations Associated with RBAC

Role (Resident on the Nexus 7000 Switch)	Operations
network-admin	read, write operations for all role privileges associated with commands, features, and groups regardless of VDC.
network-operator	read operations for all role privileges associated with commands, features, and groups regardless of VDC.
vdc-admin	read, write operations for all role privileges associated with commands, features, and groups defined within the administrator's VDC.
vdc-operator	read operations for all role privileges associated with commands, features, and groups defined within the administrator's VDC.
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

5.2.1.1.39 *FMT_MSA.1(4) Management of security attributes – Key Chains SFP*

FMT_MSA.1.1(4) The TSF shall enforce the [Key Chains] to restrict the ability to [read, write] the security attributes [all security attributes associated with Key Chains] to [the roles/operations defined in the following table].

Table 31: Role/Operations Associated with VRFs

Role (Resident on the Nexus 7000 Switch)	Operations
network-admin	read, write operations for the accept duration, accept start-time, send duration, and send start-time associated with TOE cryptographic Keys defined within administratively configured Key Chains.
network-operator	read operations for the accept duration, accept start-time, send duration, and send start-time associated with TOE cryptographic Keys defined within administratively configured Key Chains.
vdc-admin	read, write operations for the accept duration, accept start-time, send duration, and send start-time associated with TOE cryptographic Keys defined within administratively configured Key Chains.
vdc-operator	read operations for the accept duration, accept start-time, send duration, and send start-time associated with TOE cryptographic Keys defined within administratively configured Key Chains.
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

5.2.1.1.40 *FMT_MSA.3(1) Static attribute initialisation – ACLs SFP*

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

FMT_MSA.3.2(1) The TSF shall allow the [no role] 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

5.2.1.1.41 FMT_MSA.3(2) Static attribute initialisation – Control Plane Policing/Rate Limiting SFP

FMT_MSA.3.1(2) The TSF shall enforce the [*Control Plane Policing/Rate Limiting SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow the [*no role*] to specify alternative initial values to override the default values when an object or information is created.

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

5.2.1.1.42 FMT_MSA.3(3) Static attribute initialisation –RBAC SFP

FMT_MSA.3.1(3) The TSF shall enforce the [*RBAC SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(3) The TSF shall allow the [*no role*] 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

5.2.1.1.43 FMT_MSA.3(4) Static attribute initialisation - Key Chains SFP

FMT_MSA.3.1(4) The TSF shall enforce the [*Key Chains SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(4) The TSF shall allow the [*no role*] 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

5.2.1.1.44 FMT_MTD.1(1) Management of TSF data – Nexus 7000 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 32: Role/Operations/TSF Data

Role	Operation	TSF Data
network-admin	Read, write	All Nexus 7000 configuration data regardless of the VDC it is associated with. This includes cryptographic related Nexus 7000 configuration data.
network-operator	read	All Nexus 7000 configuration data regardless

Role	Operation	TSF Data
		of the VDC it is associated with. This includes cryptographic related Nexus 7000 configuration data.
vdc-admin	Read, write	All Nexus 7000 configuration data associated with the VDC the administrator is associated with. This includes cryptographic related Nexus 7000 configuration data.
vdc-operator	read	All Nexus 7000 configuration data associated with the VDC the administrator is associated with. This includes cryptographic related Nexus 7000 configuration data.
Administratively configured Nexus 7000 roles with “read” privileges	Read	Nexus 7000 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 7000 configuration data.
Administratively configured Nexus 7000 roles with “write” privileges	Write	Nexus 7000 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 7000 configuration data.

Hierarchical to: No other components.

Dependencies: FMT_SMR.1, FMT_SMF.1

5.2.1.1.45 *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 33: Role/Operations/TSF Data

Role	Operation	TSF Data
Network Device Admin (GUI role)	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 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	All reports on the ACS TOE component
SecurityAdmin (GUI role)	Query, Modify, Delete	ACS administrative user configuration related Configuration Data on the ACS TOE component.

Role	Operation	TSF Data
System Admin (GUI role)	Query, Modify, Delete	ACS system administration related Configuration Data on the ACS TOE component NOTE: ACS system administration refers to 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.
ChangeAdminPassword	Query	Administrator data
	Modify	Administrator passwords
ChangeUserPassword	Query	User data
	Modify	User passwords
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

5.2.1.1.46 FMT_SMF.1 Specification of Management Functions

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

- ◆ *Nexus 7000 Switch TOE component related management functions:*
 - *Configuration of RACL, PACL IP ACLs within the ACLs SFP;*
 - *Configuration of VACL IP ACLs within the ACLs SFP;*
 - *Configuration of PACL MAC ACLs within the ACLs SFP;*
 - *Configuration of VACL MAC ACLs within the ACLs SFP;*
 - *Configuration of SGACLs within the ACLs SFP;*
 - *Configuration of RBACs within the ACLs SFP;*
 - *Configuration of Port Security within the ACLs SFP;*
 - *Configuration of IP Source Guard within the ACLs SFP;*
 - *Configuration of Traffic Storm within the ACLs SFP;*
 - *Configuration of Control Plane Policing within the Control Plane Policing/Rate Limiting SFP;*
 - *Configuration of Rate Limiting within the Control Plane Policing/Rate Limiting SFP;*
 - *Review audit records;*
 - *Configuration of Nexus 7000 cryptographic services;*
 - *Management of Users;*
 - *Review Nexus 7000 configuration.*

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

Hierarchical to: No other components.

Dependencies: No dependencies.

5.2.1.1.47 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [

- ◆ *Nexus 7000 Switch TOE component related roles:*
 - *network-admin (CLI role)*
 - *network-operator(CLI role)*
 - *vdc-admin(CLI role)*
 - *vdc-operator(CLI role)*
 - *Administrator defined role(s) (CLI role)*

- ◆ *ACS TOE component related roles:*
 - *Network Device Admin (GUI role)*
 - *Policy Admin (GUI role)*
 - *ReadOnlyAdmin (GUI role)*
 - *ReportAdmin (GUI role)*
 - *SecurityAdmin (GUI role)*
 - *SystemAdmin (GUI role)*

- *UserAdmin (GUI role)*
- *ChangeAdminPassword (GUI role)*
- *ChangeUserPassword (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

5.2.1.1.48 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a the secure state and availability of other VDCs when the following types of failures occur: [*a VDC failure occurs on the Nexus 7000 switch*].

Hierarchical to: No other components.

Dependencies: No dependencies.

5.2.1.1.49 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.

Table 34: 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

SFR	Dependencies	Rationale
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) Met by FCS_COP.1(2) Met by FCS_COP.1(3) Met by FCS_COP.1(5) Met by FCS_COP.1(8)
	FCS_CKM.4	Met by FCS_CKM.4
FCS_CKM.1(2)	[FCS_CKM.2 or FCS_COP.1]	Met by FCS_COP.1(1) Met by FCS_COP.1(2) Met by FCS_COP.1(3) Met by FCS_COP.1(5) Met by FCS_COP.1(8)
	FCS_CKM.4	Met by FCS_CKM.4
FCS_CKM.1(4)	[FCS_CKM.2 or FCS_COP.1]	Met by FCS_COP.1(2) Met by FCS_COP.1(7)
	FCS_CKM.4	Met by FCS_CKM.4
FCS_CKM.1(5)	[FCS_CKM.2 or FCS_COP.1]	Met by FCS_COP.1(2) Met by FCS_COP.1(7)
	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) Met by FCS_CKM.1(4) Met by FCS_CKM.1(5)
FCS_COP.1(1)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Met by FCS_CKM.1(1) Met by FCS_CKM.1(2)
	FCS_CKM.4	Met by FCS_CKM.4
FCS_COP.1(2)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Met by FCS_CKM.1(1) Met by FCS_CKM.1(2) Met by FCS_CKM.1(4) Met by FCS_CKM.1(5)
	FCS_CKM.4	Met by FCS_CKM.4
	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) Met by FCS_CKM.1(2)
	FCS_CKM.4	Met by FCS_CKM.4
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]	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(7)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Met by FCS_CKM.1(4) Met by FCS_CKM.1(5)
	FCS_CKM.4	Met by FCS_CKM.4
FCS_COP.1(8)	[FDP_ITC.1 or FCS_CKM.1]	Met by FCS_CKM.1(1)

SFR	Dependencies	Rationale
	FDP_ITC.2 or FCS_CKM.1]	Met by FCS_CKM.1(2)
	FCS_CKM.4	Met by _FCS_CKM.4
FDP_ACC.1 (1)	FDP_ACF.1	Met by FDP_ACF.1 (1)
FDP_ACC.1 (2)	FDP_ACF.1	Met by FDP_ACF.1 (2)
FDP_ACF.1 (1)	FDP_ACC.1	Met by FDP_ACC.1(1)
	FMT_MSA.3	Met by FMT_MSA.3(3)
FDP_ACF.1 (2)	FDP_ACC.1	Met by FDP_ACC.1(2)
	FMT_MSA.3	Met by FMT_MSA.3(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(4)
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.1(3)	FIA_UID.1	Met by FIA_UID.1(3)
FIA_UAU.1(4)	FIA_UID.1	Met by FIA_UID.1(4)
FIA_UAU.5(1)	No Dependencies	Not applicable.
FIA_UAU.5(2)	No Dependencies	Not applicable.
FIA_UAU.5(3)	No Dependencies	Not applicable.
FIA_UID.1(1)	No Dependencies	Not applicable.
FIA_UID.1(2)	No Dependencies	Not applicable.
FIA_UID.1(3)	No Dependencies	Not applicable.
FIA_UID.1(4)	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_MSA.1(3)	[FDP_ACC.1 or FDP_IFC.1]	Met by FDP_ACC.1(1)
	FMT_SMR.1	Met by FMT_SMR.1
	FMT_SMF.1	Met by FMT_SMF.1
FMT_MSA.1(4)	[FDP_ACC.1 or FDP_IFC.1]	Met by FDP_ACC.1(2)
	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
FMT_MSA.3(2)	FMT_MSA.1	Met by FMT_MSA.1(2)
	FMT_SMR.1	Met by FMT_SMR.1
FMT_MSA.3(3)	FMT_MSA.1	Met by FMT_MSA.1(3)
	FMT_SMR.1	Met by FMT_SMR.1
FMT_MSA.3(4)	FMT_MSA.1	Met by FMT_MSA.1(4)
	FMT_SMR.1	Met by FMT_SMR.1
FMT_MTD.1(1)	FMT_SMF.1	Met by FMT_SMF.1

Objective	SFRs	Rationale
		<p>attacker trying to send traffic to unused ports on the Nexus 7000 switch by preventing traffic on unauthorized ports, or from a spoofed destination 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 7000 interface with traffic by limiting the rate of traffic on a particular interface.</p> <p>This SFR applies DHCP Snooping – Dynamic ARP Inspection to traffic received by the Nexus 7000 switch. This allows the Nexus 7000 switch to continue to provide its services even when attacked by an attacker attempting ARP spoofing attacks, ARP cache poisoning, and attempts to circumvent the TOE functionality through a spoofed DHCP attack.</p>
	FDP_IFC.1(2)	<p>This SFR applies Control Plane Policing/ Rate Limiting to control plane traffic received by the Nexus 7000. This allows the Nexus 7000 switch to continue to provide its services even when attacked by an attacker with attempting to overload the Nexus 7000 switch control plane interface with traffic by limiting the control plane traffic received and processed by the TOE or attempting to overload the Nexus 7000 by enticing the Nexus 7000 to excessively output control plane and exception traffic by limiting the control plane traffic processed and sent by the TOE.</p>
O.DataFlowControl	FDP_IFF.1(1)	<p>This SFR helps to ensure that only authorized traffic flows through the TOE to its destination by applying RACL, 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.</p> <p>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.</p> <p>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.</p> <p>This SFR helps to ensure that only authorized traffic flows through the TOE to its destination by applying SGACLs based on the traffic source and destination pair to data plane traffic processed by the TOE. Traffic that meets a configured SGACL 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.</p> <p>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 7000 TOE component is associated with a configured VRF. Traffic that is associated with a configured VRF is processed according to the VRF's 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.</p> <p>This SFR helps to ensure that only authorized traffic flows through the TOE to its destination by applying SGACLs to data plane traffic processed by the TOE. Traffic that meets a configured ACL is</p>

Objective	SFRs	Rationale
		<p>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.</p>
	FDP_IFF.1(2)	<p>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.</p>
	FDP_IFC.1(1)	<p>This SFR helps to ensure that only authorized traffic flows through the TOE to its destination by applying RACL, 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.</p> <p>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.</p> <p>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.</p> <p>This SFR helps to ensure that only authorized traffic flows through the TOE to its destination by applying SGACLs based on the traffic source and destination pair to data plane traffic processed by the TOE. Traffic that meets a configured SGACL 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.</p> <p>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 7000 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.</p> <p>This SFR helps to ensure that only authorized traffic flows through the TOE to its destination by applying SGACLs 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.</p>
	FDP_IFC.1(2)	<p>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.</p>

Objective	SFRs	Rationale
		intended destination.
O.Endpt/NetwkDeviceAuth	FCS_CKM.1(1)	This SFR helps to ensure that endpoints are authenticated by creating the keys used in the EAP-FAST portion of the authentication process (if configured to use EAP-FAST in endpoint authentication).
	FCS_CKM.1(2)	This SFR helps to ensure that endpoints and network devices are authenticated by creating the keys used in the EAP-FAST portion of the authentication process.
	FCS_CKM.1(4)	This SFR helps to ensure that network devices are authenticated by creating the keys used in the EAP-FAST portion of the authentication process
	FCS_CKM.4	This SFR helps to ensure that endpoints are authenticated by tearing down the tunnels used in the EAP-FAST portion of the authentication process. EAP-FAST is always used for network device authentication.
	FCS_COP.1(1)	This SFR helps to ensure that network devices are authenticated by providing the RSA encryption and decryption used in the EAP-FAST portion of the authentication process . EAP-FAST is always used for network device authentication.
	FCS_COP.1(2)	This SFR helps to ensure that network devices are authenticated by providing the AES encryption and decryption used in the EAP-FAST portion of the authentication process . EAP-FAST is always used for network device authentication.
	FCS_COP.1(5)	This SFR helps to ensure that network devices are authenticated by providing the hashing used in the EAP-FAST and RADIUS-KeyWrap, portion of the authentication process. EAP-FAST is always used for network device authentication.
	FCS_COP.1(6)	This SFR helps to ensure that endpoint are authenticated by providing the hashing used in the TACACS+ portion of the authentication process
	FCS_COP.1(8)	This SFR helps to ensure that network devices are authenticated by providing the DSA encryption and decryption used in the EAP-FAST portion of the authentication process. EAP-FAST is always used for network device authentication.
	FDP_ACC.1(2)	This SFR helps to ensure that network devices are authenticated by providing a method to securely use the cryptographic key used in the authentication process.
	FDP_ACF.1(2)	This SFR helps to ensure that network devices are authenticated by providing a method to securely use the cryptographic key used in the authentication process.
	FIA_UAU.1(1)	This SFR helps to ensure that network devices are authenticated by requiring the device is authenticated prior to the TOE allowing any actions, with the exception of the TOE allowing any actions administratively configured as allowed for an unauthenticated device and establishment of an EAP-FAST tunnel to secure pass the authentication credentials.
	FIA_UAU.1(2)	This SFR helps to ensure that endpoint devices are authenticated by requiring the device is authenticated prior to the TOE allowing any actions, with the exception of the TOE allowing any actions administratively configured as allowed for an unauthenticated device and establishment of a secure tunnel to secure pass the authentication credentials.
	FIA_UAU.5(1)	The TOE helps to ensure that network devices are authenticated by providing multiple authentication mechanisms for the device to authenticate against.
FIA_UAU.5(2)	The TOE helps to ensure that endpoint devices are authenticated by providing multiple authentication mechanisms for the device to authenticate against.	
FIA_UID.1(1)	This SFR helps to ensure that network devices are identified by requiring that the device is identified prior to the TOE allowing any actions, with the exception of the TOE allowing any actions administratively configured as allowed for an unauthenticated (or	

Objective	SFRs	Rationale
		identified) device and establishment of an EAP-FAST tunnel to secure pass the authentication and identification credentials.
	FIA_UID.1(2)	This SFR helps to ensure that endpoint devices are identified by requiring the device is identified prior to the TOE allowing any actions, with the exception of the TOE allowing any actions administratively configured as allowed for an unauthenticated (or identified) device and establishment of a secure tunnel to secure pass the authentication and identification credentials.
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 RACL, 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 SFP.
	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 Control Plane Policing/Rate Limiting policies.
	FMT_MSA.1(3)	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 RBACs SFP.
	FMT_MSA.1(4)	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 Key Chains SFP.
	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 SFP.
	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 Control Plane Policing/Rate Limiting policies.
	FMT_MSA.3(3)	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 RBACs SFP.
	FMT_MSA.3(4)	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 Key Chains SFP.
	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(3)	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 7000 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.

Objective	SFRs	Rationale
	FIA_UAU.1(4)	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 authenticated is establishment of a secure channel to pass the authentication credentials to the TOE in a protected fashion.
	FIA_UAU.5(3)	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 7000 switch.
	FIA_UID.1(3)	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 7000 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(4)	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.
	FDP_ACC.1(1)	This SFR helps to ensure that authorized administrators only have access to the appropriate administrative functions by requiring the Nexus 7000 switch to support a granular role authorization scheme. This authorization scheme only allows administrators to access the administrative functionality of the Nexus 7000 switch associated with the administrators' assigned roles.
	FDP_ACF.1(1)	This SFR helps to ensure that authorized administrators only have access to the appropriate administrative functions by requiring the Nexus 7000 switch to support a granular role authorization scheme. This authorization scheme only allows administrators to access the administrative functionality of the Nexus 7000 switch associated with the administrators' assigned roles.
	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 SFP to only administrators with a role which allows ACLs SFP 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 Control Plane Policing/Rate Limiting functionality to only administrators with a role which allows Control Plane Policing/Rate Limiting administration.
	FMT_MSA.1(3)	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 RBACs SFP to only administrators with a role which allows RBAC administration.
	FMT_MSA.1(4)	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 Key Chains SFP to only administrators with a role which allows Key Chains SFP

Objective	SFRs	Rationale
		administration.
	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 7000 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.CTS-PC&I	FCS_CKM.4	This SFR helps to ensure that network packets on the TOE protected (CTS) network are protected from unauthorized disclosure and modification tearing down the secure session used in the data encryption scheme used to encrypt data flowing between network devices in the TOE Protected (CTS) network after the communication is finished.
	FCS_CKM.1(4)	This SFR helps to ensure that network packets on the TOE protected (CTS) network are protected from unauthorized disclosure and modification by requiring the TOE to generate the PAC Secured-RADIUS keys used in the data encryption scheme used to encrypt data flowing between network devices in the CTS network.
	FCS_CKM.1(5)	This SFR helps to ensure that network packets on the TOE protected (CTS) network are protected from unauthorized disclosure and modification by requiring the TOE to generate the keys used for data plane encryption network devices in the CTS network during the rekeying process.
	FCS_COP.1(2)	This SFR helps to ensure that network packets on the TOE protected (CTS) network are protected from unauthorized disclosure and modification by requiring the TOE to perform encryption and decryption in the data encryption scheme used to encrypt data flowing between network devices in the TOE Protected (CTS) network.
	FCS_COP.1(7)	This SFR helps to ensure that network packets on the TOE protected (CTS) network are protected from unauthorized disclosure and modification by requiring the TOE to perform message authentication in the data encryption scheme used to encrypt data flowing between network devices in the TOE Protected (CTS) network. This message authentication ensure the integrity of the network traffic on the TOE protected network.
O.Audit	FAU_GEN.1	This SFR helps to ensure that the TOE provides audit records for RACLs, 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 RACL, PACL, or VACL.
	FPT_STM.1	This SFR helps to ensure that the TOE provides audit records for RACLs, PACLs, VACLs, and administrative actions by requiring that the TOE provides timestamps to be used with each audit record.
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(2)	This SFR helps to ensure that management communications to the TOE are protected by providing the key creation used in SSH communications. SSH is used for administrative CLI communications with the Nexus 7000 switch and the ACS TOE component. Additionally, SSH is also used for administration via XML for the Nexus 7000 Switch. This SFR also helps to ensure that management communications to the TOE are protected by providing the key creation used in TLS communications. TLS is used for administrative GUI communications with the ACS TOE component.
	FCS_CKM.1(1)	This SFR helps to ensure that management communications to the TOE are protected by providing the key creation used in TLS communications. TLS is used for administrative GUI communications with the ACS TOE component.
	FCS_CKM.4	This SFR helps to ensure that management communications to the

Objective	SFRs	Rationale
		TOE are protected by providing the tunnel tear down used in SSH, SFTP, and TLS communications. SSH, SFTP, and TLS are used for administrative communications with the Nexus 7000 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, SFTP, and TLS communications. SSH, SFTP, and TLS are used for administrative communications with the Nexus 7000 switch TOE component.
	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, SFTP, and TLS communications. SSH, SFTP, and TLS are used for administrative communications with the TOE.
	FCS_COP.1(5)	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(8)	This SFR helps to ensure that management communications to the TOE are protected by providing DSA encryption and decryption used in TLS communications. TLS is used for administrative communications with the ACS TOE component.
O.VDCSec	FPT_FLS.1	This SFR helps to ensure that each Virtual Device Context does not interfere with the operation of other Virtual Device Contexts on the Nexus switch by requiring the a failure in one Virtual Device Context is isolated from the other Virtual Device Contexts on the nexus 7000 switch.
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 3. This section identifies the Configuration Management, Delivery and Operation, Development, Flaw Remediation, Guidance Documents, Testing, and Vulnerability Assessment assurance requirements.

Table 37: 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

6.1 TOE Security Functional Requirement Measures

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

Table 38: How TOE SFRs are Met

TOE SFRs	How the SFR is Met
FAU_GEN.1	<p>The administrative configuration of RACLs, PACLs, and VACLs contain an option to enable auditing. If auditing is enabled, each time traffic that matches a configured RACL, PACL, or VACL enters or leaves the Nexus 7000 switch an audit record is generated. The type of information recorded depends on what type of ACL is met and the action applied to the traffic. A full list of the contents of the generated audit information can be found in the table associated with FAU_GEN.1.</p> <p>Each time an administrative user logs into or off of the Nexus 7000 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 7000 switch. Whenever an administrative user make a configuration change to the Nexus 7000 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.</p> <p>For both the ACS and Nexus platforms, auditing is enabled when the platform is on and cannot be disabled.</p> <p>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).</p>
FAU_SAR.1(1)	<p>Access to audit records stored on the Nexus 7000 switch is controlled by an Access Control Policy. There are several default roles which can access audit records, including, network-admin, network-operator, vdc-admin, and vdc-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.</p>
FAU_SAR.1(2)	<p>Access to audit records stored on the ACS TOE component is controlled per the privileges 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 (GUI role), Admin (CLI role), and Operator (CLI role). Additionally, the ACS TOE component allows administratively created roles that may be created with audit review permissions. 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 unauthorized users to access audit records.</p>
FAU_STG.1	<p>Access to the audit records stored on the TOE is only 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.</p> <p>For Nexus 7K logs are stored in local system files and NVRAM. By default, system messages are logged to the file log:messages. Also by default, the TOE logs the most recent 100 messages of severity 0, 1, or 2 (emergency, alert, or critical) to the</p>

TOE SFRs	How the SFR is Met
	<p>NVRAM log. You cannot configure logging to the NVRAM. AAA logs are stored separately in the AAA accounting log. All log locations are protected from modification and unauthorized deletion.</p> <p>For ACS there is no interface provided to modify or delete the audit records for any role. The ACS logs are sent to one log file, located at /opt/CSCOacs/logs/localStore/, regardless of which logging category they belong to. Administrative and operational audit log messages are always sent to the local store.</p>
FCS_CKM.1(1)	<p>The TOE establishes several types of cryptographic sessions including EAP-FAST, and TLS sessions (if configured to authenticate using EAP-FAST). A portion of the creating the session establishment includes key generation. This requirement has been verified by FIPS 140-2 validation. Please see certificates #1533 and #1534, Nexus 7000 10 Slot and 18 Slot, for details.</p>
FCS_CKM.1(2)	<p>The TOE uses Diffie-Hellman (Group1 and Group 14) to create keys for multiple purposes. The uses for the keys include SSH sessions, TLS sessions, and EAP-FAST sessions. This requirement has been verified by FIPS 140-2 validation. Please see certificates #1533 and #1534, Nexus 7000 10 Slot and 18 Slot, for details</p>
FCS_CKM.1(4)	<p>The ACS TOE component creates a Key (known as the PAC key). This key is unique to each device within the CTS network. The key is used in the EAP-FAST and PAC Secured-RADIUS session creation process. This operation can occur with either another instance of the TOE or a CTS capable device in the IT environment. This requirement has been verified by FIPS 140-2 validation. Please see certificates #1533 and #1534, Nexus 7000 10 Slot and 18 Slot, for details.</p>
FCS_CKM.1(5)	<p>The Nexus 7000 TOE component establishes sessions with other CTS capable devices. These sessions are protected by encryption. The key used to protect the communication is generated using HMAC-SHA1. The Nexus 7000 TOE component also rekeys the session. HMAC-SHA1 is used to ask the key generation algorithm to create the new key.</p>
FCS_CKM.4	<p>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. This requirement has been verified by FIPS 140-2 validation. Please see certificates #1533 and #1534, Nexus 7000 10 Slot and 18 Slot, for details.</p>
FCS_COP.1(1)	<p>As part of the EAP-FAST and TLS communications, the TOE performs RSA encryption and decryption. This requirement has been verified by FIPS 140-2 validation. Please see certificates #1533 and #1534, Nexus 7000 10 Slot and 18 Slot, for details.</p>
FCS_COP.1(2)	<p>As part of the EAP-FAST, CTS, SSH, and TLS communications, the TOE performs AES encryption and decryption. This requirement has been verified by FIPS 140-2 validation. Please see certificates #1533 and #1534, Nexus 7000 10 Slot and 18 Slot, for details.</p>
FCS_COP.1(3)	<p>As part of the SSH, and TLS communications, the TOE performs Triple-DES encryption and decryption. This requirement has been verified by FIPS 140-2 validation. Please see certificates #1533 and #1534, Nexus 7000 10 Slot and 18 Slot, for details.</p>
FCS_COP.1(5)	<p>Provides the hashing required as part of the EAP-FAST, RADIUS-KeyWrap, and TLS session establishment protocols. This requirement has been verified by FIPS 140-2 validation. Please see certificates #1533 and #1534, Nexus 7000 10 Slot and 18 Slot, for details.</p>
FCS_COP.1(6)	<p>The TOE performs the necessary hashing as part of TACACS+ communications. This requirement has been verified by FIPS 140-2 validation. Please see certificates #1533 and #1534, Nexus 7000 10 Slot and 18 Slot, for details.</p>
FCS_COP.1(7)	<p>If configured to provide confidentiality and integrity for communications between CTS enable device, the Nexus 7000 appliance will establish a SAP session with the communicating device. After the SAP session has been generated, the Nexus 7000</p>

TOE SFRs	How the SFR is Met
	<p>appliance will check the integrity of network traffic using AES-GMAC. This requirement has been verified by FIPS 140-2 validation. Please see certificates #1533 and #1534, Nexus 7000 10 Slot and 18 Slot, for details.</p>
FCS_COP.1(8)	<p>As part of the EAP-FAST and TLS communications, the TOE performs DSA encryption and decryption. This requirement has been verified by FIPS 140-2 validation. Please see certificates #1533 and #1534, Nexus 7000 10 Slot and 18 Slot, for details.</p>
FDP_ACC.1 (1)	<p>The TOE enforces role-based access restrictions on administrative access and authorization to the Nexus 7000 switch. Access to the administrative functionality of the Nexus 7000 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.</p>
FDP_ACC.1 (2)	<p>The TOE provides the ability to administratively configure how the cryptographic keys used in the Network Device authentication process are used. Specifically, the TOE allows the administrator to establish a lifecycle for a particular key. This lifecycle includes a valid start time and an end time. When the criteria match the criteria specified for a specific cryptographic key, the TOE uses that cryptographic key in the authentication process.</p>
FDP_ACF.1 (1)	<p>The TOE enforces role-based access restrictions on administrative access and authorization to the Nexus 7000 switch. Access to the administrative functionality of the Nexus 7000 switch is permitted based on the role assigned to the user attempting to access the functionality. The decision to allow a user access to specific administrative functionality is based on the administratively configured permission assigned to the role(s) for which the user is associated.</p>
FDP_ACF.1(2)	<p>The TOE provides the ability to administratively configure how the cryptographic keys used in the Network Device authentication process are used. Specifically, the TOE allows the administrator to establish a lifecycle for a particular key. This lifecycle includes a valid start time and an end time. When the criteria match the criteria specified for a specific cryptographic key, the TOE uses that cryptographic key in the authentication process.</p>
FDP_IFC.1(1)	<p>The TOE enforces information flow policies on network traffic (both IPv4 and v6 and non-IP) received by the Nexus 7000 interfaces including any Nexus Layer 3 interface, VLAN interfaces, Physical Layer 3 interfaces, Layer 3 Ethernet subinterfaces, Layer 3 Ethernet port-channel interfaces, Layer 3 Ethernet port-channel subinterfaces, Tunnels, Management interfaces, Layer 2 interfaces, or Layer 2 Ethernet port-channel interfaces. The TOE makes an information flow decision to Permit traffic flow, Deny traffic flow, Redirect the traffic to an interface, Deny traffic flow and log a copy of the traffic, Disable the ingress interface, or Create DHCP binding table</p> <p>Whenever an endpoint device attempts to send network traffic to the TOE protected network, the TOE verifies that the posture, or state, of the endpoint devices complies with the administratively configured security policies before the endpoint device can send network traffic to TOE protected resources. For endpoint devices that comply with the administratively configured policies, the TOE permits the network traffic to flow to the TOE protected resource in the network. For endpoint devices that do not comply with administratively configured security policies, the TOE either denies the traffic flow or quarantines the Traffic flow to access to the TOE protected network that is sufficient only for remediation. After remediation the TOE checks the posture of the device again.</p> <p>The TOE can control the traffic flow within the TOE protected network based on assigned security groups using security group access lists (SGACLs). The TOE assigns a unique 16-bit tag, called the security group tag (SGT), to a security group.</p>

TOE SFRs	How the SFR is Met
	<p>The SGT is a single label that indicates the privileges of the source within the TOE protected network. The TOE applies tags to any network traffic that originates from a device with the SGT that represents the security group to which the device is assigned. The packet carries this SGT throughout the TOE protected network within the traffic header. Because this tag represents the group of the source, the tag is referred to as the source SGT. At the outer edge of the TOE protected network, the TOE determines the group that is assigned to the traffic destination device and permits or denies the traffic flow based on the administratively configured information flow policy.</p>
<p>FDP_IFC.1(2)</p>	<p>The Nexus 7000 switch provides the ability for an administrative user to configure information flow policies for incoming control plane traffic. For traffic that is received by the Nexus 7000 Supervisor Module interfaces, the Nexus 7000 switch applies the configured policies. The Nexus 7000 may choose to permit the information flow, deny the information flow, or downgrade the QoS associated with the traffic. The traffic flow decision is based on the administratively configured policy.</p> <p>The Nexus 7000 switch provides the ability for an administrative user to configure information flow policies for exception traffic traveling from the line card installed within a Nexus 7000 to the supervisor card installed within the Nexus 7000. For exception traffic that is sent from the Nexus 7000, the Nexus 7000 switch applies the administratively configured rate limiting policy. The Nexus 7000 switch may choose to permit or deny the traffic based on the configured rate limiting policy.</p> <p>NOTE: Rate limit policies apply to the following traffic: Access list logging packets, Data and control packets copied to the supervisor module, Layer 2 storm control packets, Layer 2 port security packets, Layer 3 glean packets (Glean packets are packets that indicate unresolved adjacencies of neighboring routers), Layer 3 maximum transmission unit (MTU) check failure packets, Layer 3 multicast directly connected packets, Layer 3 Time-to-Live (TTL) check failure packets, or Receive packets.</p>
<p>FDP_IFF.1(1)</p>	<p>Whenever network traffic (both IP and non-IP traffic) is received by one of the Nexus 7000 interfaces, the TOE applies administratively configured information flow policies to the traffic in the following order,</p> <ol style="list-style-type: none"> 1. Port Security/IP Storm/DHCP Inspection (all applied at the same time) 2. Source Guard/Traffic Snooping/Dynamic ARP 3. PAACL MAC ACLs 4. VRFs 5. VACL IP/MAC ACLs 6. RACL IP/MAC ACLs 7. SGACL <p>The specific rules associated with each policy are, as follows:</p> <p>Port Security</p> <p>An administrator can configure the Nexus 7000 switch to allow inbound traffic from only a restricted set of MAC addresses. This policy can be applied to Layer 2 Access Ports, Layer 2 Trunk Ports, or Layer 2 SPAN Source Ports. The Nexus 7000 switch makes an information flow decision to permit, deny, or disable the port whenever traffic is received on the port. The TOE makes the information decision based on the following,</p> <ul style="list-style-type: none"> ▪ The source MAC address is administratively configured as secure for the

TOE SFRs	How the SFR is Met
	<p>Nexus 7000 interface, or,</p> <ul style="list-style-type: none"> ▪ The source MAC address is dynamically identified as secure by the TOE. A source MAC address is considered secure if the following criteria is met, <ul style="list-style-type: none"> ▪ The Nexus 7000 has not reached any connection maximums; ▪ The source MAC address has not already been secured for another port within the same VLAN ▪ And, the network traffic flow is not denied by any IP Source Guard/Traffic Storm/DHCP Snooping/Dynamic ARP Inspection policies ▪ If a Nexus 7000 interface receives network traffic from a source MAC address that is not identified as secure, one of the following actions takes place, the ingress port is shutdown or the network traffic is denied <p>IP Source Guard IP Source Guard is a per-interface traffic filter that permits IP traffic only when the IP address and MAC address of each packet matches. The IP Source Guard information flow policy is applied to the layer 2 interfaces of the Nexus 7000 switch. If the TOE determines that the IP address and MAC address of the traffic does not come from the same source the TOE will deny the network traffic flow. The following rules are enforced by the TOE for this information flow policy,</p> <ul style="list-style-type: none"> ▪ Network traffic flow is permitted if the Source IP address and MAC address combination are administratively configured as a valid combination, or, ▪ The Source IP address and MAC address combination were previously identified as a valid combination by the TOE through DHCP Snooping ▪ And, the network traffic flow is not denied by any Port Security/Traffic Storm/DHCP Snooping/Dynamic ARP Inspection policies <p>Traffic Storm Traffic storm control allows an administrator to monitor the levels of the incoming traffic to a Nexus 7000 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,</p> <ul style="list-style-type: none"> ▪ 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 ▪ And, the network traffic flow is not denied by any IP Source Guard/Port Security/DHCP Snooping/Dynamic ARP Inspection policies ▪ 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 <p>DHCP Snooping The Nexus 7000 switch provides the ability to validate DHCP messages received from untrusted sources and prevent invalid DHCP messages from passing. The Nexus 7000 switch builds a database from information collected by valid DHCP</p>

TOE SFRs	How the SFR is Met
	<p>requests. The Nexus 7000 switch then uses the information obtained from the valid DHCP requests to verify the validity of ARP requests received by untrusted sources by checking the collected IP-to-MAC address mapping. Traffic that is identified as valid ARP requests are allowed to pass. Packets identified as invalid ARP traffic are dropped. These services can be administratively turned on and off. The following rules are enforced by the TOE.</p> <ul style="list-style-type: none"> ▪ The Nexus 7000 switch permits DHCP traffic to flow unless any of the following conditions occur (in which case the traffic flow is denied): The Nexus 7000 switch receives a DHCP response packet (such as DHCPACK, DHCPNAK, or DHCPOFFER packet) on an untrusted interface. The Nexus 7000 receives a packet on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match. This check is performed only if the DHCP snooping MAC address verification option is turned on. The Nexus 7000 receives a DHCPRELEASE or DHCPDECLINE message from an untrusted host with an entry in the DHCP snooping binding table, and the interface information in the binding table does not match the interface on which the message was received. ▪ And, the network traffic flow is not denied by any IP Source Guard/Traffic Storm/Port Security/Dynamic ARP Inspection policies <p>Dynamic ARP Inspection Dynamic ARP Inspection ensures that only valid ARP requests and responses are relayed. When DAI is enabled the Nexus 7000 switch performs these information flows:</p> <ul style="list-style-type: none"> ▪ The TOE permits ARP traffic flows received on an untrusted Nexus 7000 switch interface to the appropriate destination if a valid IP-to-MAC address binding exists within the DHCP binding table ▪ And, the network traffic flow is not denied by any IP Source Guard/Traffic Storm/DHCP Snooping/Port Security policies ▪ The TOE denies ARP traffic flows received on an untrusted Nexus 7000 switch interface if a valid IP-to-MAC address binding does not exist within the DHCP binding table <p>▪</p> <p>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 7000 switch makes an information flow decision to either permit or deny the traffic. Traffic is permitted or denied, as follows,</p> <ul style="list-style-type: none"> ▪ 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 information attributes and a permit/deny operation. The information attributes that are available for the creation of PACL permit/deny policies for non-IP traffic include: Source MAC address, Destination MAC address, Protocol, Class of Service (COS), VLAN ID <p>VRFs</p>

TOE SFRs	How the SFR is Met
	<p>The Nexus 7000 switch provides the ability for an administrative user to configure VRFs for incoming IP traffic. For IP traffic that is received by the Nexus 7000 interfaces, the Nexus 7000 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.</p> <ul style="list-style-type: none"> ▪ IP traffic with security attributes that map to a configured VRF will be forwarded through the Nexus 7000 switch TOE component per the VRF routing table <p>VACL IP/MAC ACLs</p> <p>When network traffic that meets an administratively configured VACL IP ACL is received on VLAN interfaces, the Nexus 7000 switch makes an information flow decision to forward the traffic, redirect the traffic, drop the traffic, or drop the packet and create a log of the traffic. Traffic is forwarded, redirected, dropped, or dropped and logged, as follows,</p> <ul style="list-style-type: none"> ▪ IP traffic with security attributes that match an administratively configured permit policy rule is allowed to flow, or, ▪ IP traffic with security attributes that match an administratively configured deny policy rule is not permitted to flow. IP traffic with security attributes that match an administratively configured redirect policy rule is redirected to the specified interface, or, ▪ IP traffic with security attributes that match an administratively configured deny-and-log policy rule is not permitted to flow and a copy of the traffic is logged by the TOE. <p>The permit/deny/redirect/deny-and-log policies (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/redirect/deny-and-log operation. The subject attributes that are available for the creation of permit/deny/redirect/deny-and-log policies include: vlan-ID. The information attributes that are available for the creation of permit/deny/redirect/deny-and-log policies include: Source IP address, Destination IP address, Source port number, Destination port number, Protocol, ICMP message type, ICMP message code, IGMP message type, Packet length, Precedence, DSCP Value</p> <ul style="list-style-type: none"> ▪ Non-IP traffic with security attributes that match an administratively configured permit policy rule is allowed to flow, or, ▪ Non-IP traffic with security attributes that match an administratively configured deny policy rule is not permitted to flow. Non-IP traffic with security attributes that match an administratively configured redirect policy rule is redirected to the specified interface, or, ▪ Non-IP traffic with security attributes that match an administratively configured deny-and-log policy rule is not permitted to flow. <p>The permit/deny/redirect/deny-and-log policies (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/redirect/deny-and-log policies include: vlan-ID. The information attributes that are available for the creation of these permit/deny/redirect/deny-and-log policies include: Source MAC address,</p>

TOE SFRs	How the SFR is Met
	<p data-bbox="578 233 1370 260">Destination MAC address, Protocol, Class of Service (COS), or VLAN ID</p> <p data-bbox="482 279 721 306">RACL IP/MAC ACLs</p> <p data-bbox="482 310 1382 520">When network traffic that meets an administratively configured RACL or PACL IP ACL is received on VLAN interfaces, Physical Layer 3 interfaces, Layer 3 Ethernet subinterfaces, Layer 3 Ethernet, port-channel interfaces, Layer 3 Ethernet port-channel subinterfaces, Tunnels, Management interfaces, Layer 2 interfaces, or Layer 2 Ethernet port-channel interfaces, the Nexus 7000 switch makes an information flow decision to either permit or deny the traffic. Traffic is permitted or denied, as follows,</p> <ul data-bbox="531 541 1382 919" style="list-style-type: none"> <li data-bbox="531 541 1349 632">▪ Ingress or egress IP traffic with security attributes that match an administratively configured RACL permit policy rule is allowed to flow, or, <li data-bbox="531 646 1382 919">▪ Ingress or egress IP traffic with security attributes that match an administratively configured RACL deny policy for IP traffic rule is not permitted. The RACL permit/deny policies for IP traffic are comprised of a combination of information attributes and a permit/deny operation. The information attributes that are available for the creation of RACL permit/deny policies include: Source IP address, Destination IP address, Source port number, Destination port number, Protocol, ICMP message type, ICMP message code, IGMP message type, Packet length, Precedence, DSCP Value <p data-bbox="482 940 1349 995">Note: RACLs are applied to both ingress and egress traffic. PACLs are applied to only ingress traffic.</p> <p data-bbox="482 1016 570 1043">SGACL</p> <p data-bbox="482 1047 1382 1409">The TOE can control the traffic flow within the TOE protected network based on assigned security groups using security group access lists (SGACLs). The TOE assigns a unique 16-bit tag, called the security group tag (SGT), to a security group. The SGT is a single label that indicates the privileges of the source within the TOE protected network. The TOE applies tags to any packets that originate from a device with the SGT that represents the security group to which the device is assigned. The packet carries this SGT throughout the TOE protected network within the traffic header. Because this tag represents the group of the source, the tag is referred to as the source SGT. At the outer edge of the TOE protected network, the TOE determines the group that is assigned to the traffic destination device and permits or denies the traffic flow based on the administratively configured information flow policy. The following information flow policies are enforced by the TOE.</p> <ul data-bbox="531 1430 1382 1682" style="list-style-type: none"> <li data-bbox="531 1430 1382 1549">▪ Network traffic is permitted to flow to its destination if an administratively configured SGACL policy rule with the SGT/DGT pair associated with the network traffic's Source SGT and Destination (DGT) explicitly allows it, or, <li data-bbox="531 1564 1349 1682">▪ Network traffic is not permitted to flow to its destination if an administratively configured SGACL policy rule with the SGT/DGT pair associated with the network traffic's Source SGT and Destination (DGT) explicitly disallows it <p data-bbox="482 1703 1349 1787">In addition to the TOE, IT environment devices that are CTS capable have the ability to recognize the SGT/DGT. The TOE treats any CTS enable device as part of the CTS network.</p> <p data-bbox="482 1808 1312 1866">Additionally, the following explicit authorize rules are enforce on information flows.</p>

TOE SFRs	How the SFR is Met
	<ul style="list-style-type: none"> ▪ DHCP traffic received on interfaces configured as trusted is always allowed to pass, or, ▪ ARP traffic received on interfaces configured as trusted is always allowed to pass. <p>The following explicit deny rules are enforced on information flows.</p> <p>For IP Network Traffic Flows:</p> <ul style="list-style-type: none"> ▪ The TOE denies IP traffic flow when the IP address and MAC address of the traffic are not identified as a valid combination either through DHCP Snooping or administrative configuration, or, ▪ For IP traffic, if the security attributes do not match an administratively configured RACL or VACL, the traffic flow is denied, or, ▪ If the IP traffic security attributes do not map to a configured VRF, the traffic flow is denied <p>For Non-IP Network Traffic Flows:</p> <ul style="list-style-type: none"> ▪ For Non-IP traffic, if security attributes do not match an administratively configured RACL, PACL, or VACL, the traffic flow is denied
FDP_IFF.1(2)	<p>The Nexus 7000 switch provides the ability for an administrative user to configure information flow policies for incoming and outgoing control plane traffic. For traffic that is received by the Nexus 7000 Supervisor Module interfaces, the Nexus 7000 switch applies the configured policies. The Nexus 7000 may choose to permit the information flow, deny the information flow, or downgrade the QoS (Mark Down) associated with the traffic. The traffic flow decision is based on the administratively configured policy. The following decisions are enforced by the TOE.</p> <ul style="list-style-type: none"> ▪ If the ingress Control Plane Traffic conforms to the configured rate limits for CIR, PIR, BC, or BE, the traffic is permitted to flow ▪ If ingress Control Plane Traffic with security attributes that match the administratively configured Control Plane Traffic policy exceeds the administratively configured threshold for CIR, PIR, BC, or BE, the traffic will be dropped or Marked Down based on the administratively configured policy <p>For exception traffic that is sent from the Nexus 7000, the Nexus 7000 switch applies the administratively configured rate limiting policy. The Nexus 7000 switch may choose to permit or deny the traffic based on the configured rate limiting policy. The following decisions are enforced by the TOE,</p> <ul style="list-style-type: none"> ▪ If the Egress Network Traffic does not exceed the configured Rate Limit for its traffic type, the traffic is permitted to flow ▪ If the Egress Network Traffic exceeds the configured Rate Limit for its traffic type, the traffic is not permitted to flow <p>NOTE: Rate limit policies apply to the following traffic: Access list logging packets, Data and control packets copied to the supervisor module, Layer 2 storm control packets, Layer 2 port security packets, Layer 3 glean packets, Layer 3 maximum transmission unit (MTU) check failure packets, Layer 3 multicast directly connected packets, Layer 3 Time-to-Live (TTL) check failure packets, or Receive packets.</p>
FIA_UAU.1(1)	Whenever a network device attempts to gain access to the TOE protected network as part of the CTS protected cloud, the TOE challenges the network device to be authenticated. Prior to being authenticated the network device attempting to access

TOE SFRs	How the SFR is Met
	<p>the TOE protected network may only perform the following functions,</p> <ul style="list-style-type: none"> ▪ Establish an EAP-FAST Tunnel with the Nexus 7000 TOE component– A CTS capable network device can initiate communications and establish an EAP-FAST tunnel with the TOE. At this point, authentication data is sent from the CTS capable device to the Nexus 7000 TOE component over the established EAP-FAST Tunnel. This authentication data is passed to the ACS TOE component where the actual authentication occurs. ▪ Any administratively configured unauthenticated access – An administrator can configure network access for network devices that have not yet been authenticated by the TOE.
FIA_UAU.1(2)	<p>Whenever an endpoint device attempts to gain access to the TOE protected network, the TOE challenges the endpoint device to be authenticated. Prior to being authenticated, the endpoint device attempting to access the TOE protected network may only perform the following functions,</p> <ul style="list-style-type: none"> ▪ Establish a secure tunnel – This encrypted tunnel will be used to send authentication credentials over the network in a protected format (Tunnel formats, include, EAP-FAST). ▪ Any administratively configured unauthenticated access – An administrator can configure network access for endpoint devices that have not yet been authenticated by the TOE.
FIA_UAU.1(3)	<p>Prior to being granted any administrative access to the Nexus 7000 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 7000 switch (SSH) so that administrative credentials (e.g., username/password) can be sent in a protected form. Authentication may be provided via either</p> <ul style="list-style-type: none"> ▪ Remote authentication (facilitated by RADIUS or TACACS+ (provided by the ACS TOE component)); ▪ Authentication against a database local to the Nexus 7000 switch. <p>Authentication of Nexus 7000 administrators is required regardless of whether access is attempted from the local console connection or remotely via SSH. Authentication is done with a username and password.</p>
FIA_UAU.1(4)	<p>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.</p> <p>NOTE: ACS administrative users are always authenticated locally to the ACS TOE component.</p> <p>Authentication of ACS administrators is required regardless of whether access is attempted from the TLS protected GUI or the SSH-protected CLI. Authentication is done with a username and password.</p>
FIA_UAU.5(1)	<p>The TOE supports two authentication techniques for network devices attempting to gain access to the TOE protected network (to become a member of the CTS cloud network). The authentication technique includes the following,</p> <ul style="list-style-type: none"> ▪ Device ID/Password-based Authentication; <p>The TOE will authenticate network devices attempting to access the TOE protected network based on the administratively configured authentication scheme.</p> <p>The administratively configured authentication scheme specifies the authentication</p>

TOE SFRs	How the SFR is Met
	<p>method order in which the TOE will attempt to authenticate an entity. 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.</p>
FIA_UAU.5(2)	<p>The TOE supports several authentication techniques for endpoint devices attempting to gain access to the TOE protected network. The authentication techniques supported by the TOE for endpoint authentication include the following,</p> <ul style="list-style-type: none"> ▪ EAP-FAST Authentication; ▪ MAC Bypass Authentication <p>The TOE will authenticate network devices attempting to access the TOE protected network based on the administratively configured authentication scheme. All authentication schemes are facilitated by either RADIUS or TACACS+ communications between the Nexus 7000 switch and the ACS server.</p> <p>The administratively configured authentication scheme specifies the authentication method order in which the TOE will attempt to authenticate an entity.</p> <p>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.</p>
FIA_UAU.5(3)	<p>The TOE supports several authentication techniques for administrative users attempting to access the Nexus 7000 switch administrative functions. The authentication techniques supported by the TOE for Nexus 7000 switch administrative users include the following,</p> <ul style="list-style-type: none"> ▪ Remote authentication (facilitated by RADIUS or TACACS+ (provided by the ACS TOE component)); ▪ Authentication against a database local to the Nexus 7000 switch <p>The TOE will perform authentication based on the following rules:</p> <ul style="list-style-type: none"> ▪ 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 7000 switch, the TSF will authenticate the administrator based on the administratively configured Identification and Authentication scheme <p>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 7000. Note that the local credentials will not be used unless the ACS server cannot be reached.</p> <p>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.</p>
FIA_UID.1(1)	<p>Whenever a network device attempts to gain access to the TOE protected network as part of the CTS protected cloud, the TOE challenges the network device to be identified. Prior to being identified the network device attempting to access the TOE protected network may only perform the following functions,</p> <ul style="list-style-type: none"> ▪ Establish an EAP-FAST Tunnel – This encrypted tunnel will be used to send authentication credentials over the network in a protected format. ▪ Any administratively configured unauthenticated access – An administrator

TOE SFRs	How the SFR is Met
	can configure network access for network devices that have not yet been authenticated by the TOE.
FIA_UID.1(2)	<p>Whenever an endpoint device attempts to gain access to the TOE protected network, the TOE challenges the endpoint device to be identified. Prior to being identified, the endpoint device attempting to access the TOE protected network may only perform the following functions,</p> <ul style="list-style-type: none"> ▪ Establish a secure tunnel – This encrypted tunnel will be used to send authentication credentials over the network in a protected format (Tunnel formats, include, EAP-FAST). ▪ Any administratively configured unauthenticated access – An administrator can configure network access for endpoint devices that have not yet been authenticated or identified by the TOE.
FIA_UID.1(3)	<p>Prior to being granted any administrative access to the Nexus 7000 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 7000 switch (SSH) so that administrative and identification credentials (e.g., username/password) can be sent in a protected form.</p>
FIA_UID.1(4)	<p>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.</p>
FMT_MSA.1(1)	<p>The TOE allows authenticated and authorized administrative users of the Nexus 7000 switch TOE component to Read, write 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. 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.</p>
FMT_MSA.1(2)	<p>The TOE allows authenticated and authorized administrative users of the Nexus 7000 switch TOE component to Read, write Control Plane and Rate Limiting Policing 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.</p>
FMT_MSA.1(3)	<p>The TOE allows authenticated and authorized administrative users of the Nexus 7000 switch TOE component to read, write RBAC 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.</p>
FMT_MSA.1(4)	<p>The TOE allows authenticated and authorized administrative users of the Nexus 7000 switch TOE component to read, write Key Chains. The TOE allows access to the Key Chains configuration based on the permissions defined for the user’s administratively assigned roles. Only users assigned a role with access privileges to</p>

TOE SFRs	How the SFR is Met
	the Key Chains have any access.
FMT_MSA.3(1)	There are no default ACLs for the information flow control on the Nexus 7000 switch TOE component. Without default ACLs, packet flows are not allowed. This is a restrictive policy and only supports very limited access. The TOE provides no facility to have a default policy applied by the TOE. The TOE does allow other policies to be created. However, when the policies are removed, the default TOE information flow control policy is still restrictive.
FMT_MSA.3(2)	The default Control Plane Policing and Rate Limiting policies for the information flow control on the Nexus 7000 switch TOE component are restrictive and only support very limited access. The TOE provides no facility to change the policies applied by default by the TOE. The TOE does allow other policies to be created. However, when the policies are removed, the default TOE information flow control policy is still restrictive.
FMT_MSA.3(3)	The default Administrative RBAC policies for administrative control of the Nexus 7000 switch are restrictive and only support very limited access. The TOE provides four predefined administrative accounts with defined access rules. The permissions associated with the predefined roles are non-modifiable. The TOE does allow other policies to be created. However, when the policies are removed, the default TOE information flow control policy is still restrictive. By default, no access is allowed to the TOE administrative functionality beyond what is allowed for the predefined roles.
FMT_MSA.3(4)	The default policies for Key Chains are restrictive and only support limited access. The TOE provides no facility to change the Key Chains applied by default by the TOE. The TOE does allow other Key Chains to be created. However, when the policies are removed, the default TOE Key Chains are still restrictive.
FMT_MTD.1(1)	The TOE provides the ability for administrators of the Nexus 7000 to access TOE configuration and audit data. Each of the predefined and administratively configured roles has either read or write access to the configuration and audit data. See the SFR definition in section 5 for details regarding the specific access available to each user role.
FMT_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 SFR definition in section 5 for details regarding the specific access available to each user role.
FMT_SMF.1	<p>Through the administrative interface of the Nexus 7000 switch (CLI), the TOE facilitates the following administrative functions,</p> <ul style="list-style-type: none"> ▪ Configuration of RACL, PACL IP ACLs within the ACLs SFP – This functionality allows the configuration of RACL and PACL IP ACLs by an administrative user. ▪ Configuration of VACL IP ACLs within the ACLs SFP – This functionality allows the configuration of VACL IP ACLs by an administrative user. ▪ Configuration of PACL MAC ACLs within the ACLs SFP – This functionality allows the configuration of PACL MAC ACLs by an administrative user. ▪ Configuration of VACL MAC ACLs within the ACLs SFP - This functionality allows the configuration of VACL MAC ACLs by an administrative user. ▪ Configuration of SGACLs within the ACLs SFP - This functionality allows the configuration of SGACLs by an administrative user.

TOE SFRs	How the SFR is Met
	<ul style="list-style-type: none"> ▪ Configuration of RBACs - This functionality allows the configuration of RBACs by an administrative user. ▪ Configuration of Port Security within the ACLs SFP - This functionality allows the configuration of Port Security by an administrative user. ▪ Configuration of IP Source Guard within the ACLs SFP - This functionality allows the configuration of IP Source Guard by an administrative user. ▪ Configuration of Traffic Storm within the ACLs SFP - This functionality allows the configuration of Traffic Storm by an administrative user. ▪ Configuration of Control Plane Policing within the Control Plane Policing/Rate Limiting SFP - This functionality allows the configuration of Control Plan Policing by an administrative user. ▪ Configuration of Rate Limiting within the Control Plane Policing/Rate Limiting SFP - This functionality allows the configuration of Rate limiting by an administrative user. ▪ Reviewing audit records – This functionality allows Nexus 7000 audit records to be viewed by an administrative user. ▪ Configuration of Nexus 7000 cryptographic services - This functionality allows the configuration of Nexus 7000 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 7000 configuration - This functionality allows the administrative user to review the Nexus 7000 configuration. <p>Through the administrative interface of the ACS TOE component (CLI and GUI), the TOE facilitates the following administrative functions,</p> <ul style="list-style-type: none"> ▪ 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. ▪ Management of Network Users – The functionality allows the creation and configuration of network users. ▪ Review audit records – This functionality allows ACS TOE component audit records to be viewed by an administrative user.
FMT_SMR.1	<p>The Nexus 7000 switch supports the following predefined roles,</p> <ul style="list-style-type: none"> ▪ network-admin – This role is a super administrative role. This role has read and write privileges for any configuration item on the Nexus 7000 switch regardless of the assigned VDC. ▪ network-operator - This role has read access to the entire Cisco NX-OS device (only available in the default VDC).

TOE SFRs	How the SFR is Met
	<ul style="list-style-type: none"> ▪ vdc-admin - This role has read and write privileges for any configuration item on the Nexus 7000 switch for a specific VDC. ▪ vdc-operator - This role has read privileges for any configuration item on the Nexus 7000 switch for a specific VDC <p>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 7000 switch. The custom administrative roles are created on a per VDC basis. Access for the custom roles can be defined per command, feature (a group of command, or feature group (a collection of features)).</p> <p>The ACS TOE component supports several predefined roles, as follows:</p> <ul style="list-style-type: none"> ▪ 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 ▪ System Admin (GUI role) – This role has privileges to ACS system administration and ACS instances related Configuration Data ▪ User Admin (GUI role) – This role has privileges to Network user and host related Configuration Data ▪ 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. ▪ 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 CLI 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 <p>The permissions associated with the predefined administrative roles cannot be modified.</p>
FPT_FLS.1	<p>The Nexus 7000 switch may contain up to four separate Virtual Device Contexts (default and three additional VDCs). Each Virtual Device Context act as standalone Nexus 7000 switch. This feature allows each Nexus 7000 switch to support multiple networks. The Virtual Device Contexts do not share any of the same processing or</p>

TOE SFRs	How the SFR is Met
	storage resource. This prevents a failure in one Virtual Device Context from interfering with the other Virtual Device Contexts resident on the same Nexus 7000 switch.
FPT_STM.1	Both the Nexus 7000 switch and the ACS TOE component can provide hardware based timestamp that are used to provide that timestamp in audit records. The TOE provides the option to either use the internally generated time stamps or at the discretion of the administrator use an external time server to provide the time stamp.

6.2 TOE Bypass and interference/logical tampering Protection Measures

Both the Nexus 7000 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 or GUI interfaces. There are no undocumented interfaces for managing the product.

All cards included in the TOE rely on the main Nexus 7000 switch for power, memory management, and access control. In order to access any portion of the Nexus 7000 switch, the Identification & Authentication mechanisms of the Nexus 7000 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 7000 switch provides the ability to segment Operating System and hardware resources into virtual contexts that act as independent virtual switches. These virtual device contexts are known as VDCs. Each VDC has its own software processes, dedicated hardware resources, and independent management environment.

The Nexus 7000 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 7000 switch TOE component are not able to affect.

The Nexus 7000 switch provides a secure domain for each VRF to operate within. Each VRF has its own resources that other VRFs within the same Nexus 7000 switch TOE component are not able to affect.

Finally, the Nexus 7000 switch enforce ACLs and apply other network traffic security 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. Traffic flow

characterized as malicious (through administratively configured policies) are discarded and not permitted to circumvent the TOE. The TOE includes protections against various attacks, including, traffic burst, address spoofing, attempts to over load the TOE control plane, and others. The information flow defenses built into the TOE to counter these attacks, such as, Rate Limiting Policies, Control Plane Policing, Traffic Storm Policies, IP Source Guards, and Port Security, help prevent logical tampering of the TOE.

The TOE also includes separate operating domains for each of the Virtual Device Contexts resident on the Nexus 7000 switch. The TOE prevents any sharing of internal resources for each of the Virtual Device Contexts. Each internal process is mapped to each memory allocation call. In turn, each process that is running on the box is associated with a specific VDC. The TOE prevents processes from interfering with other process resources. This helps to prevent circumvention of any of the security policies associated with a specific Virtual Device Context by attacking a separate Virtual Device Context on the same Nexus 7000 switch. Each port on the Nexus 7000 is administratively configured to be associated with a specific VDC. Any traffic received on a particular port is only associated with the VDC for which it is administratively configured.

There are no unmediated traffic flows into or out of either component of the TOE (Nexus 7000 switch or ACS). The information flow policies identified in the SFRs are applied to all traffic received and sent by the Nexus 7000 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.

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 July 2009, version 3.1, Revision 3, CCMB-2009-07-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated July 2009, version 3.1, Revision 3, CCMB--2009-07-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated July 2009, version 3.1, Revision 3, CCMB-2009-07-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated July 2009, version 3.1, Revision 3, CCMB-2009-07-004