National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

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

Cisco Nexus 5000 Series Switch

Report Number: CCEVS-VR-10384-2011
Dated: 8 September 2011
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Olin Sibert
Orion Security
McLean, VA

Michelle Brinkmeyer
National Security Agency
Ft. Meade, MD

Common Criteria Testing Laboratory

Tammy Compton
Julie Cowan
Eve Pierre
Quang Trinh
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Nexus 5000 Series Switch with 2000 Series Fabric Extenders and Cisco Secure Access Control Server (ACS) solution provided by Cisco Systems, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in August 2011. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.2.

The Nexus 5000 Series TOE offers a unified fabric with high-capacity 10GbE, Fibre-Channel over Ethernet (FCoE) with low-latency, together with Data Center Ethernet (DCE). In addition to the Nexus 5000 Series Switch itself, the solution provided by the TOE includes the CISCO Nexus 2000 Series Fabric Extender, the NX-OS software and the Cisco Secure Access Control Server (ACS), which provides a scalable IGbE and 10GbE Data Center access solution in addition to providing classical Ethernet. The ACS TOE component is an Administration, Authorization, and Accounting (AAA) server that provided authentication services and supports the implementation of information flow policies by the Nexus 5000 switch TOE component. The AAA services provided by the ACS server include RADIUS and TACACS+ for authentication.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 3) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 3). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4 augmented with ALC_FLR.2) have been met.

The technical information included in this report was obtained from the Nexus 5000 Series Switch Security Target and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Nexus 5000 Series Switch with 2000 Series Fabric Extenders running software version NX-OS version 5.0(3)N1(1c) and Cisco Secure Access Control Server (ACS) running software version 5.2 patch 3.
Protection Profile	None
ST:	Nexus 5000 Series Switch Security Target, Version .15, July 2011
Evaluation Technical Report	Evaluation Technical Report For the Nexus 5000 Series Switch (Proprietary), Version 2.0, July 29, 2011
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 3
Conformance Result	CC Part 2 extended, CC Part 3 conformant

Item	Identifier
Sponsor	Cisco Systems, Inc
Developer	Cisco Systems, Inc
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validators	Michelle Brinkmeyer, National Security Agency, Ft. Meade, MD Olin Sibert, Orion Security, McLean, VA

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1 TOE Introduction

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

Table 3-1: TOE Component Descriptions

TOE Component	TOE-Subcomponent	Description
Nexus 5000 Series Switch	Cisco Nexus 5548P	Supporting 32 fixed 1 and 10 Gigabit Ethernet ports(Ports 1 to 16 Can Run at 1 Gigabit Ethernet), FCoE, and 1 Expansion Module Slot
	Cisco Nexus 5596UP	A 2RU switch supporting 48 1/10 Gigabit Ethernet fixed enhanced Small Form-Factor Pluggable (SFP+) Ethernet/FCoE or 1/2/4/8-Gbps native FC unified ports and three expansion slots.
	Cisco Nexus 5020	Supporting 40 Fixed Ports of 10 Gigabit Ethernet (Ports 1 to 16 Can Run at 1 Gigabit Ethernet), FCoE, and 2 Expansion Module Slots
	Cisco Nexus 5010	Supporting 20 Fixed Ports of 10 Gigabit Ethernet (Ports 1 to 16 Can Run at 1 Gigabit Ethernet), FCoE, and 1 Expansion Module Slot
Cisco Nexus 2000 Series Fabric Extenders	Cisco Nexus 2148T, 2224TP, 2248TP, and 2232PP Fabric Extenders.	The Cisco Nexus 2000 Series sits on top of a server rack and essentially acts as a remote line card for an upstream switch and becomes an extension of the switch, so software, configuration, and policy are all inherited from the upstream switch; even advanced features such as FCoE and Cisco VN-Link support are inherited. Designed specifically to give customers a means of granularly transitioning from Gigabit Ethernet to 10 Gigabit Ethernet and Unified Fabric; and supporting up to 48 Gigabit Ethernet downlinks and 4 10 Gigabit Ethernet uplinks.
NX-OS	Software image running on N5k and N2k components.	NX-OS 5.0(3)N1(1c)
Cisco Secure Access	Cisco Secure ACS Solution	Cisco Secure ACS is an access control server that

TOE Component	TOE-Subcomponent	Description
Control Server (ACS) v5.2	Engine appliance models 1120, or 1121, or virtual machine.	operates as a centralized authentication server.

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

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

3.2 Physical Scope of the TOE

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

Table 3-2: Physical Scope of the TOE

TOE Component	Hardware (within the TOE)	Software (within the TOE)
Nexus 5000 Series Switch	Cisco Nexus 5020 Supporting 40 Fixed Ports of 10 Gigabit Ethernet (Ports 1 to 16 Can Run at 1 Gigabit Ethernet), FCoE, and 2 Expansion Module Slots	NX-OS 5.0(3)N1(1c) This includes a hardened version of Linux Kernel 2.6.
	Cisco Nexus 5010 Supporting 20 Fixed Ports of 10 Gigabit Ethernet (Ports 1 to 16 Can Run at 1 Gigabit Ethernet), FCoE, and 1 Expansion Module Slot	
	Cisco Nexus 5596UP supporting 48 1/10 Gigabit Ethernet fixed enhanced Small Form-Factor Pluggable (SFP+) Ethernet/FCoE or 1/2/4/8-Gbps native FC unified ports and three expansion slots.	
	Cisco Nexus 5548P Supporting 32 fixed 1 and 10 Gigabit Ethernet ports(Ports 1 to 16 Can Run at 1 Gigabit Ethernet), FCoE, and 1 Expansion Module Slot	

TOE Component	Hardware (within the TOE)	Software (within the TOE)
	Cisco Nexus 5000 Series Expansion Modules	
Cisco Nexus 2000 Series Fabric Extenders	Cisco Nexus 2148T, 2224TP, 2248TP, and 2232PP Fabric Extenders	NX-OS 5.0(3)N1(1c) This includes a hardened version of Linux Kernel 2.6.
Cisco Secure Access Control Server (ACS)	Cisco Secure ACS hardware appliance or virtual machine	ACS Software version 5.2

Product Architecture

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

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

Cisco Nexus 5548P 32-Port Switch

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

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

Cisco Nexus 5596UP

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

- Forty-eight 1/10 Gigabit Ethernet fixed enhanced Small Form-Factor Pluggable (SFP+) Ethernet/FCoE or 1/2/4/8-Gbps native FC unified ports and three expansion slots. These slots have a combination of Ethernet/FCoE and native FC ports.

- Unified ports support traditional Ethernet, Fibre Channel (FC),and Fibre Channel over Ethernet (FCoE)
- Connectivity options include 1 Gigabit Ethernet, 10 Gigabit Ethernet, 10 Gigabit Ethernet with FCoE, and 1/2/4/8G Native Fibre Channel
- Switch supports all Cisco Nexus 2000 Series Fabric Extenders

Cisco Nexus 5020 56-Port Switch

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

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

Cisco Nexus 5010 28-Port Switch

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

- Twenty fixed 10-Gigabit Ethernet, Cisco Data Center Ethernet, and FCoE Small Form Factor Pluggable Plus (SFP+) ports. Eight of the Twenty fixed ports support both Gigabit Ethernet and 10-Gigabit Ethernet.
- One expansion module slots that can be configured to support up to 6 additional 10-Gigabit Ethernet, Cisco Data Center Ethernet, and FCoE SFP+ ports, up to 8 Fibre Channel switch ports, or a combination of both.
- Serial console port and an out-of-band 10/100/1000-Mbps Ethernet management port.
- 1+1 redundant, hot-pluggable power supplies.
- 1+1 redundant, hot-pluggable fan modules to provide reliable front-to-back cooling.

Cisco Nexus 5000 Series Expansion Modules

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

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

Physical Specifications

SFP+ Optics

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

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

SFP Optics

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

Fabric Extenders

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

- Operation as a remote I/O module, extending the internal fabric of the Cisco Nexus 5010 and 5020 Switches for low-cost port-count expansion
- Zero-touch provisioning, including configuration and upgrade
- 48 Gigabit Ethernet server access ports with RJ-45 connectors

- Four 10 Gigabit Ethernet uplink ports using SFP+ short-reach (SR) and long-reach (LR) optical or CX1 directattach copper interconnects
- Compact 1RU form factor
- Front-to-back cooling compatible with data center hot-aisle and cold-aisle designs, with all switch ports at the rear of the unit in close proximity to server ports
- 1+1 redundant, hot-pluggable, dual-sensing power supplies
- Hot-swappable fan trays
- All user-serviceable components accessible from the front panel

Cisco Secure ACS

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

4 Security Policy

This section summaries the security functionality of the TOE:

1. Data Plane Information Flow Control
    a. PACLs
    b. VACLs
    c. VRFs
2. Secure Management
    a. Administrator Identification and Authentication
    b. Administrative Auditing
    c. Administrative Authorization
    d. Secure Management Communication
    e. Authentication, Authorization, and Accounting (AAA)
3. Virtualization and Availability
    a. IP Source Guard
    b. Traffic Storm Control
    c. Control Plane Policing
    d. Rate Limiting
    e. DHCP Snooping – Dynamic ARP Inspection
    f. Cisco Fabric Services (CFS) provisioning

4.1 Data Plane Information Flow Control

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

- Layer 2 Traffic – PACLs
- VLAN Traffic – VACLs

- VRFs

A PACL is an administratively configured access control list that is applied to Layer 2 traffic that is routed into Nexus 5000 switch. A VACL is an administratively configured access control list that is applied to packets that are routed into or out of a VLAN or are bridged within a VLAN. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces.

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

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

The TOE supports Virtual Routing and Forwarding (VRF). VRFs allow multiple instances of routing tables to exist within the Nexus 5000 switch TOE component simultaneously. The TOE implements two VRFs (management and default). This increases functionality by allowing network paths to be segmented without using multiple devices. Each VRF instance uses a single routing table. These tables prevent traffic from being forwarded outside a specific VRF path and also keep out traffic that should remain outside the VRF path.

4.2 Management Security

The TOE provides the ability to be securely administered.

4.2.1 Administrator Identification and Authentication

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

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

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

4.2.2 Authentication, Authorization, and Accounting (AAA)

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

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

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

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

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

4.2.3 Administrative Auditing

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

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

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

4.2.4 Administrative Authorization

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

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

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

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

4.2.5 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 4-1: Secure Management Communication

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

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

4.3 Virtualization and Availability

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

4.3.1 Traffic Storm Control

Traffic Storm Control allows an administrative user to monitor the levels of the incoming traffic over a 1-second interval. During this interval, the traffic level, which is a percentage of the total available bandwidth of the port, is compared with the administratively configured traffic storm control. When the ingress traffic reaches the Traffic Storm Control level that is configured on the port, Traffic Storm Control drops the traffic until the interval ends.

4.3.2 Control Plane Protection

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

4.3.3 Private VLANs (PVLANs)

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

5 Assumptions

The following assumptions were made during the evaluation of Nexus 5000 Series Switch:

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

6 Documentation

The following documentation was used as evidence for the evaluation of the Nexus 5000 Series Switch:

6.1 Design Documentation

1. Cisco 5000 Series Switch Security Architecture, Revision 0.3, January 4, 2011
2. Cisco 5000 Series Switch Functional Specification, Revision 0.3, March 4, 2011
3. Cisco 5000 Series Switch TOE Design Specification, Revision 0.5, July 1, 2011
4. Cisco Secure Access Control Server (ACS) TOE Design Specification, Revision 0.4, November 11, 2010
5. Annex A: Command Interface Commands, March 4, 2011
6. Annex B: RFC Security Parameter Relevancy, March 4, 2011
7. Annex C: ACS Programming Interface, November 11, 2010

6.2 Guidance Documentation

1. Nexus 5000 Series Switch Nexus 2000 Series Fabric Extender Cisco Secure ACS Preparative Procedures and Operational User Guidance Wrapper, July 2011
2. Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes, Release 5.0(2)N1(1) and Release 5.0(2)N2(1)
3. Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 5.0(2)N2(1)
4. Cisco Nexus 5000 Series NX-OS Security Configuration Guide, Release 5.0(2)N2(1)
5. Cisco Nexus 5000 Series NX-OS Command Reference
6. Cisco NX-OS Releases 4.x, 5.x Text Part Number: OL-22746-04
7. Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide, Release 5.0(2)N1(1)
8. Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide, Release 5.0(2)N2(1)
9. Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS, Release 5.0(2)N1(1)
10. Cisco Nexus 5000 Series NX-OS Quality of Service Configuration Guide, Release 5.0(2)N1(1)
11. Cisco NX-OS System Messages Reference, November 8, 2010
12. Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide, Release 5.0(2)N2(1)
13. Installation and Upgrade Guide for the Cisco Secure Access Control System 5.2, Text Part Number: OL-21574-01
14. User Guide for Cisco Secure Access Control System 5.2, Text Part Number: OL-21572-01
15. CLI Reference Guide for Cisco Secure Access Control System 5.2, Text Part Number: OL-21575-01

6.3 Life Cycle

1. Configuration Management, Lifecycle and Delivery Procedures for Cisco Nexus 5000/2000 Series, February 2010, Version: 1.1
2. Development Security for Nexus 5000/2000 Series, January 2010, Version: 1.0

6.4 Testing

1. Cisco N5K Common Criteria Detailed Test Plan, EDCS-993725, Rev. 6, 06/06/11
2. N5K_CC_ATE_FUN_ATE_COV_ATE_DPT_20110603.xls

3. Cisco N5K Common Criteria Test Results, EDCS-1023108, Rev. 1, 05/11/2011

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the Cisco Nexus 5000 Series Switch, Version 1.0, July 21, 2011.

7.1 Developer Testing

At EAL4, testing must demonstrate correspondence between the tests and the functional specification. The vendor testing addressed each of the security functions identified in the ST and interfaces in the design. These security functions include:

1. Data Plane Information Flow Control
    a. PACLs
    b. VACLs
    c. VRFs
2. Secure Management
    a. Administrator Identification and Authentication
    b. Administrative Auditing
    c. Administrative Authorization
    d. Secure Management Communication
    e. Authentication, Authorization, and Accounting (AAA)
3. Virtualization and Availability
    a. IP Source Guard
    b. Traffic Storm Control
    c. Control Plane Policing
    d. Rate Limiting
    e. DHCP Snooping – Dynamic ARP Inspection
    f. Cisco Fabric Services (CFS) provisioning

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according the Common Criteria Guide, ran a sample of the developer tests and verified the results, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

The evaluation team testing focused on testing boundary conditions not tested by Cisco. The evaluation team tested combinations of the information flow policies that Cisco did not test. For vulnerability testing the evaluation team performed port and vulnerability scanning as well as other team developed tests.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is the Cisco Nexus 5000 Switch Solution including:

- Nexus 5000 Series Switch with 2000 Series Fabric Extenders running software version NX-OS version 5.0(3)N1(1c)
- Cisco Secure Access Control Server (ACS) running software version 5.2 patch 3

To use the product in the evaluated configuration, the product must be configured as specified in the **Nexus 5000 Series Switch Nexus 2000 Series Fabric Extender Cisco Secure ACS Preparative Procedures and Operational User Guidance Wrapper, July 2011** document.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL4 augmented with ALC_FLR.2 work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 3 and CEM version 3.1 rev 3. The evaluation determined the Cisco Nexus 5000 Switch Solution TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.2 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Nexus 5000 Series product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a detailed design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was

conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The ALC evaluation also ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation.

In addition to the EAL 4 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team re-ran the entire vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each EAL 4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the entire vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

- The evaluation team observed that the vendor's security tests are predominantly manual and apparently not closely integrated with the extensive automated testing performed as a routine part of product development. While these evaluated tests are sufficient to satisfy Common Criteria requirements, the validation team recommends a closer integration in future efforts, in order to improve test integration and provide greater test coverage.
- Although the vendor apparently maintains a significant internal organization responsible for vulnerability analysis and flaw remediation, the evaluation team was not provided access to any of that organization's personnel nor to the vulnerability reports and analysis performed therein. Again, while the materials provided are sufficient to satisfy the conformance requirements for vulnerability analysis and flaw remediation, the validation team considers the lack of access a lost opportunity to assess and describe the details of analysis and remediation work performed by the vendor.
- The ACS appliance portion of the TOE was not tested as part of this effort but the virtual ACS component was. It was tested as part of the recently completed Nexus 7000 evaluation (physical appliance only). The same version was used in this evaluation as

was tested in the Nexus 7000 evaluation (version 5.2.0.26.3). The same roles and security functions were supported so the evaluator concludes the functional testing from the Nexus 7000 evaluation was adequate for this evaluation. The evaluator repeated the vulnerability scans in case an update to a tool or the virtual environment discovered something new.

- The public search for vulnerabilities found one ACS related vulnerability in ACS version 5.2. The web-based management interface in Cisco Secure Access Control System (ACS) 5.1 before 5.1.0.44.6 and 5.2 before 5.2.0.26.3 allows remote attackers to change arbitrary user passwords via unspecified vectors, aka Bug ID CSCtl77440. The evaluated configuration uses the patched ACS Software Release 5.2.0.26.3 to address/patch this vulnerability.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Nexus 5000 Series Switch Security Target Security Target, Version 1.0, July 2011*.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Science Applications International Corporation. *Evaluation Technical Report for the Nexus 5000 Series Switch Part 2 (Proprietary)*, Version 2.0, July 29, 2011.

[7] Science Applications International Corporation. *Evaluation Team Test Report for the Cisco* Nexus 5000 Series Switch, *ETR Part 2 Supplement (SAIC and Cisco Proprietary)*, Version 1.0, July 21, 2011.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] Nexus 5000 Series Switch Security Target Security Target, Version 1.0, July 29, 2011.