National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

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

Cisco Nexus 7000 Series Switch

Report Number:	**CCEVS-VR-10349-2011**
Dated:	**27 April 2011**
Version:	**0.1**

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

Jandria Alexander
Aerospace Corporation
Columbia, MD

Olin Sibert
Orion Security Solutions, Inc.
McLean, VA

Common Criteria Testing Laboratory

Tammy Compton
Gary Grainger
Eve Pierre
Katie Sykes
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 7000 Series Switch 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 March 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 7000 Target of Evaluation (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.

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, observed evaluation testing activities, 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 7000 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 7000 Series Switch running software version NX-OS version 5.1(1a) and Cisco Secure Access Control Server (ACS) running software version 5.2 patch 3.
Protection Profile	None
ST:	Nexus 7000 Series Switch Security Target, Version 0.22, April 2011
Evaluation Technical Report	Evaluation Technical Report For the Nexus 7000 Series Switch (Proprietary), Version 2.0, February 11, 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	Jandria Alexander, Aerospace Corporation, McLean, VA Olin Sibert, Orion Security Solutions, Inc., 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 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 1: TOE Component Descriptions

TOE Component	TOE-Subcomponent	Description
Nexus 7000 Series Switch	Cisco Nexus 7000 Series 10-Slot Chassis (Also referred to as the 7010 Switch)	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.
	Cisco Nexus 7000 Series 18-Slot Chassis (Also referred to as the 7018 Switch)	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.
	Cisco Nexus 7000 Series Supervisor Module (plugs into either the 10-Slot or 18-Slot chassis)	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.
	Cisco Nexus 7000 10-Slot Chassis 46Gbps/Slot Fabric Module (plugs into the 10-Slot chassis)	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.
	Cisco Nexus 7000 18-Slot Chassis 46Gbps/Slot Fabric Module (plugs into the 18-Slot chassis)	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.
	Cisco Nexus 7000 Series 32-Port 10Gb Ethernet	The Cisco Nexus 7000 Series 32-Port 10Gb Ethernet Module with 80 Gb of bandwidth to the fabric is a

TOE Component	TOE-Subcomponent	Description
	Module with 80Gbps Fabric (plugs into either the 10-Slot or 18-Slot chassis)	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.
	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)	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.
	Cisco Nexus 7000 Series 48-Port Gigabit Ethernet SFP Module with 46 Gbps Fabric (plugs into either the 10-Slot or 18-Slot chassis)	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.
	Cisco Nexus 7000 Series 8-Port 10Gigabit Ethernet X2 XL Module with 80 Gbps Fabric (plugs into either the 10-Slot or 18-Slot chassis)	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 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.

3.2 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 2: Physical Scope of the TOE

TOE Component	Hardware (within the TOE)	Software (within 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 5.1(1a) 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	
	Cisco Nexus 7000 Series 48-Port Gigabit Ethernet SFP Module with 46Gbps Fabric	
Cisco Secure Access Control Server (ACS)	Cisco CAM25 appliance – 1120 or 1121	ACS Software version 5.2 This includes a hardened version of Linux Kernel 2.4.

.

3.3 Required non-TOE Hardware/ Software/ Firmware

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

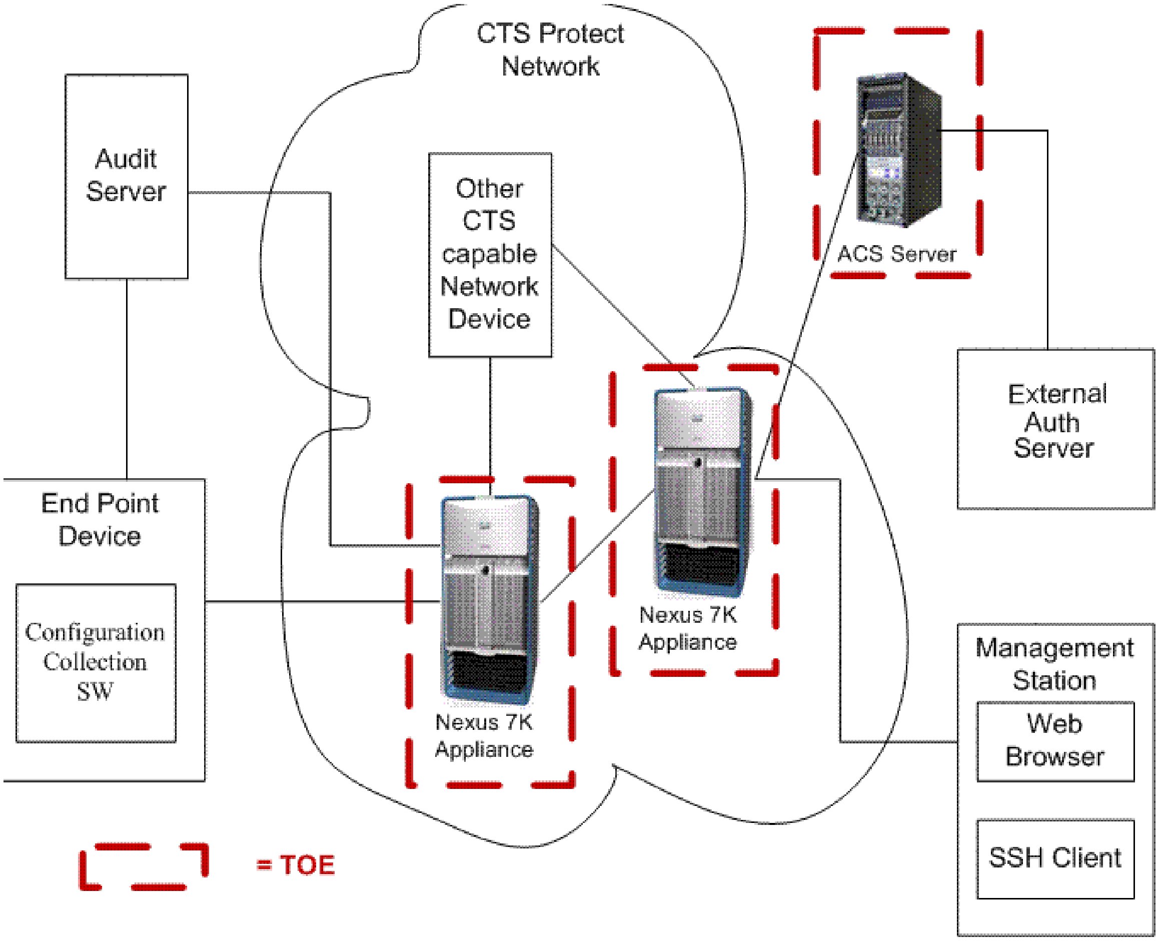
Table 3: IT Environment Components

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	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

IT Environment Component	Required	Usage/Purpose Description for TOE performance
devices		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.

3.3.1 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).

4 Security Policy

This section summaries the security functionality of the TOE:

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
6. DHCP Snooping – Dynamic ARP Inspection.

4.1 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 Nexus 7000 switch. A PACL is an administratively configured access control list that is applied to Layer 2 traffic that is routed into 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.

4.2 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.

4.3 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 is final destination. Cisco TrustSec uses ingress tagging and egress filtering to enforce access control policy in as a conversation.

4.4 Management Security

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.

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.

4.5 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.

5 Assumptions

The following assumptions were made during the evaluation of Nexus 7000 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 7000 Series Switch:

6.1 Design Documentation

1. Cisco 7000 Series Switch Security Architecture, Revision 0.4, January 3, 2011
2. Cisco 7000 Series Switch Functional Specification, Revision 0.4, November 11, 2010
3. Cisco 7000 Series Switch TOE Design Specification, Revision 0.5, November 11, 2010
4. Cisco Secure Access Control Server (ACS) TOE Design Specification, Revision 0.4, November 11, 2010
5. Annex A: Command Interface Commands, November 15, 2010
6. Annex B: RFC Security Parameter Relevancy, November 15, 2010
7. Annex C: ACS Programming Interface, November 11, 2010

6.2 Guidance Documentation

1. Cisco Nexus 7000 Series Switch Preparative Procedures Wrapper, Version 0.5, February 2011

2. Nexus 7000 Series Switch Operational User Guidance (Common Criteria Specific), Version 0.4, February 2011

3. Cisco Nexus 7000 Series Connectivity Management Processor Configuration Guide May 2010

4. Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 5.x 2009March 15, 2010
5. User Guide for the Cisco Secure Access Control System 5.2 (Text Part Number: OL-21572-01)
6. CLI Reference Guide for the Cisco Secure Access Control System 5.2 (Text Part Number: OL-21575-01)
7. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x July 2010
8. Cisco Nexus 7000 Series NX-OS System Management Command Reference, Release 5.x April 2010 (Text Part Number: OL-16006-01)
9. Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference, Release 5.x April 2010(Text Part Number: OL-19603-01)
10. Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x June 29, 2010 (Text Part Number: OL-19821-01)
11. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x June 20, 2010 (Text Part Number: OL-19824-01)
12. Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference, Release 5.x April 2010 (Text Part Number: OL-19826-01)
13. Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x August 2, 2010 (Text Part Number: OL-20001-01)
14. Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference, Release 5.x September 21, 2010 (Text Part Number: OL-20084-01)
15. Cisco Nexus 7000 Series NX-OS Security Command Reference, Release 5.x July 2010 (Text Part Number: OL-19597-01)
16. Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference, Release 5.x July 2010 (Text Part Number: OL-19600-01)
17. Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x July 2010 (Text Part Number: OL-19599-01)
18. Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 5.x, March 31, 2010 (Text Part Number: OL-19602-01)
19. Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 5.x September 1, 2010 (Text Part Number: OL-19797-01)
20. Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide, Release 5.x March 5, 2010 (Text Part Number: OL-19823-01)
21. Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide, Release 5.x April 2010 (Text Part Number: OL-19825-01)
22. Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x August 16, 2010 (Text Part Number: OL-21548-01)

23. Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 5.x September 17, 2010 (Text Part Number: OL-21641-01)
24. Cisco Nexus 7000 Series NX-OS Licensing Guide, Release 4.2 August 10, 2009 (Text Part Number: OL-18669-01)
25. Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x April 2010 (Text Part Number: OL-19336-01)
26. Cisco NX-OS System Messages Reference September 22, 2010 (Text Part Number: OL-23717-01)

6.3 Life Cycle

1. Configuration Management, Lifecycle and Delivery Procedures for Cisco Nexus 7000 Series Switch and Cisco Secure Access Control Server (ACS), Reference: N7K-ACS-CMP-v1-0, February 2011, Version: 1.2

6.4 Testing

1. Common Criteria – Detailed Test Plan, Cisco Systems, Inc., EDCS-861205 version 7, 3 January 2011
2. Nexus 7000 + ACS 5.2 Common Criteria Test Documentation, Cisco Systems, Inc. version 1.4, 3 January 2011
3. ACS Common Criteria Test: Detailed Report, Cisco Systems, Inc., 22 December 2010.
4. Common Criteria – Nexus7K and ACS Detailed Test Plan, Cisco Systems, Inc., revision 4, 22 December 2010.
5. Nexus 7000 Common Criteria Test Actual Results, Cisco Systems, Inc., 20 December 2010.
6. ACS Common Criteria Test Actual Results, Cisco Systems, Inc., 10 February, 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 7000 Series Switch, Version 2.0, February 11, 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. 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
6. DHCP Snooping – Dynamic ARP Inspection

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 7000 Switch Solution including:

- Nexus 7000 Series Switch running software version NX-OS version 5.1(1a)
- 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 **Cisco Nexus 7000 Series Switch Preparative Procedures Wrapper, Version 0.5, February 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 7000 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 7000 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 validation team considers the evaluated subset of product functions to be consistent with the product’s intended purpose and mode of operation. The rationale for excluded features is plausible and introduces no unreasonable constraints.

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.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Nexus 7000 Series Switch Security Target Security Target, Version 0.22, April 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 7000 Series Switch Part 2 (Proprietary)*, Version 3.0, February 11, 2011.

[7] Science Applications International Corporation. *Evaluation Team Test Report for the Cisco* Nexus 7000 Series Switch, *ETR Part 2 Supplement (SAIC and Cisco Proprietary)*, Version 2.0, February 11, 2011.

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

[10] Nexus 7000 Series Switch Security Target Security Target, Version 0.22, April 2011.