Cisco Nexus 5600 Series Switch with 2000 Series Fabric Extenders

Common Criteria Configuration Guide

Version 1.0

January 22, 2016

Table of Contents

List of Tables

List of Acronyms

The following acronyms and abbreviations are used in this document:

Table 1: Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
AES	Advanced Encryption Standard
CI	Configuration Item
FIPS	Federal Information Processing Standards
EAL	Evaluation Assurance Level
HTTPS	Hyper-Text Transport Protocol Secure
IP	Internet Protocol
NTP	Network Time Protocol
RADIUS	Remote Authentication Dial In User Service
SFP	Security Function Policy
SSHv2	Secure Shell (version 2)
TACACS+	Terminal Access Controller Access-Control System Plus
TCP	Transport Control Protocol
TOE	Target of Evaluation

DOCUMENT INTRODUCTION

Prepared By:

Cisco Systems, Inc.

170 West Tasman Dr.

San Jose, CA 95134

DOCUMENT INTRODUCTION

This document provides supporting evidence for an evaluation of a specific Target of Evaluation (TOE), the Nexus 5600 Series Switch with 2000 Series Fabric Extenders (Nexus 5k). This Operational User Guidance with Preparative Procedures addresses the administration of the TOE software and hardware and describes how to install, configure, and maintain the TOE in the Common Criteria evaluated configuration. Administrators of the TOE will be referred to as administrators, authorized administrators, TOE administrators, semi-privileged administrators, and privileged administrators in this document. All administrative actions that are relevant to the Common Criteria (CC) Evaluation and claimed Protection Profile(s) are described within this document. This document will include pointers to the official Cisco documentation in order to aid the administrator in easily identifying the CC relevant administrative commands, including subcommands, scripts (if relevant), and configuration files, that are related to the configuration (including enabling or disabling) of the mechanisms implemented in Nexus 5k that are necessary to enforce the requirements claimed.

1 Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Nexus 5600 Series Switch with 2000 Series Fabric Extenders (Nexus 5k), the TOE, as it was certified under Common Criteria. The Nexus 5600 Series Switch with 2000 Series Fabric Extenders (Nexus 5k) may be referenced below by the model number series related acronym ex. Nexus 5k, TOE, Nexus 5000 Series, Nexus 5600 Series, or simply switch.

1.1 Audience

This document is written for administrators configuring the TOE. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, and understand your network topology and the protocols that the devices in your network can use, that you are a trusted individual, and that you are trained to use the operating systems on which you are running on your network.

1.2 Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining Nexus 5k operations. All security relevant commands to manage the TSF data are provided within this documentation within each functional section.

1.3 Document References

This section lists the Cisco Systems documentation that is also the Common Criteria Configuration Item (CI) List. The documents used are shown below in Table 2. Throughout this document, the guides will be referred to by the "#", such as **[4]**.

Table 2 Cisco Documentation

Note: The 5500 and 5600 documents can be used interchangeably with the 5600 switch.

#	Title	Link
[1]	Cisco Nexus 5600 Series Switch with 2000 Series Fabric Extenders Security Target, (Current Version)	https://www.niap-ccevs.org/CCEVS_Products/vpl.cfm
[2]	Cisco Nexus 5600 Series NX-OS System Management Configuration Guide, Release 7.x	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5600/sw/system_management/7x/b_5600_System_Mgmt_Config_7x.pdf
[3]	Cisco Nexus 5600 Series NX-OS Security Configuration Guide, Release 7.x	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5600/sw/security/7x/b_5600_Security_Config_7x.pdf
[4]	Cisco Nexus 5600 Series NX-OS Fundamentals Configuration Guide, Release 7.x	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5600/sw/fundamentals/7x/b_5600_Fund_Config_7x.pdf

#	Title	Link
[5]	Cisco Nexus 5600 Series NX-OS Fundamentals Command Reference, Release 7.x	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5600/sw/command/reference/fund/7x/n5600-fund-cr.pdf
[6]	Cisco Nexus 5500 Series NX-OS Security Command Reference, Release 7.x	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5500/sw/command/reference/security/7x/n5500-sec-cr.html
[7]	Cisco Nexus 5600 Series NX-OS System Management Command Reference, Release 7.x	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5600/sw/system_management/7x/b_5600_System_Mgmt_Config_7x/b_6k_System_Mgmt_Config_7x_preface_00.html
[8]	Cisco Nexus 5500 Series NX-OS Virtual Port Channel Command Reference	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5500/sw/command/reference/vpc/7x/n5500-vpc-cmd.pdf
[9]	Cisco Nexus 5600 Series Hardware Installation Guide, Cisco Nexus 2000 Series Hardware Installation Guide	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5600/hw/installation/guide/n56k_hig.pdf http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus2000/hw/installation/guide/nexus_2000_hig/install.html
[10]	Nexus 5600 Series NX-OS System Message Reference	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5600/sw/system_messages/reference/sl_nxos_book.pdf
[11]	Cisco Nexus 5000 Series Command Reference	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/command/reference/rel_4_1/NX5000CommdReference.pdf
[12]	Cisco Nexus 5600 Series NX-OS Layer 2 Switching Configuration Guide	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5600/sw/layer2/7x/b_5600_Layer2_Config_7x.pdf
[13]	Cisco Nexus 5600 Series NX-OS Interfaces Configuration Guide	http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5600/sw/interfaces/7x/b_5600_Interfaces_Config_Guide_Release_7x.pdf

1.4 Supported Hardware and Software

Only the hardware and software listed in section 1.5 of the Security Target (ST) is compliant with the Common Criteria evaluation. Using hardware not specified in the ST invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed in the ST will invalidate the secure configuration. The TOE is a hardware and software solution that makes up the switch models as follows: 2000, 5600. The network, on which they reside, is considered part of the environment. The software is comprised of the Universal Cisco NX-OS software image Release 7.2(1).

1.5 Operational Environment

1.5.1 Supported non-TOE Hardware/ Software/ Firmware

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

Table 3: Operational Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Syslog Server	No	This includes any syslog server to which the TOE would transmit syslog messages.
RADIUS or TACACS+ AAA Server	No	This includes any IT environment RADIUS or TACACS+ AAA server that provides single-use authentication mechanisms. The TOE correctly leverages the services provided by this RADIUS or TACACS+ AAA server to provide single-use authentication to administrators.

1.6 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 4 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.
Telnet	Telnet will be disabled in the evaluated configuration.
SNMP	SNMP will be disabled in the evaluated configuration.
NTP	NTP will be disabled in the evaluated configuration.
Web Management GUI	The Web Management GUI was not included in the evaluated configuration.
VMtracker	VMtracker is disabled by default and will not be enabled in the evaluated configuration.
NX-API	NX-API will not be configured for use.

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the claimed security functions. FIPS configuration is described in section 3.2.4 . Telnet is disabled by default. SNMP is enabled by default. To disable SNMP, please run the following command:

n5600(config)# **no snmp-server protocol enable**

The AUX ports are not to be used in the evaluated configuration. The exclusion of this functionality does not affect compliance to the claimed security functions.

2 Secure Acceptance of the TOE

In order to ensure the correct TOE is received, the TOE should be examined to ensure that that is has not been tampered with during delivery.

Verify that the TOE software and hardware were not tampered with during delivery by performing the following actions:

Step 1 Before unpacking the TOE, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 2 Verify that the packaging has not obviously been opened and resealed by examining the tape that seals the package. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 3 Verify that the box has a white tamper-resistant, tamper-evident Cisco Systems bar coded label applied to the external cardboard box. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This label will include the Cisco product number, serial number, and other information regarding the contents of the box.

Step 4 Note the serial number of the TOE on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5 Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

Step 6 Once the TOE is unpacked, inspect the unit. Verify that the serial number displayed on the unit itself matches the serial number on the shipping documentation and the invoice. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner). To further ensure proper and secure delivery of the Nexus 5k TOE, the recipient must check the models received against the list of TOE component hardware models listed in Table 5 below.

Table 5 TOE External Identification

Cisco 5600 Series
Cisco Nexus 5624Q
Cisco Nexus 5648Q
Cisco Nexus 5672UP
Cisco Nexus 56128P

2000 Series Fabric Connectors
Cisco Nexus 2224TP
Cisco Nexus 2248TP
Cisco Nexus 2248TP-E
Cisco Nexus 2232PP
Cisco Nexus 2248PQ
Cisco Nexus 2232TM
Cisco Nexus 2232TM-E

Step 7 Approved methods for obtaining a Common Criteria evaluated software images:

- Download the Common Criteria evaluated software image file from Cisco.com onto a trusted computer system. Software images are available from Cisco.com at the following: http://www.cisco.com/cisco/software/navigator.html.

Step 8 Once the file is downloaded, the authorized administrator verifies that it was not tampered with by either using a hash utility to verify the hash by comparing the MD5 or SHA512 hash that is listed on the Cisco web site and in Table **6** below or by using the **show file** command on the Nexus 5k. The "**show file** *filename* **md5sum**" command on the Nexus 5k can be used to verify the md5 hash. In addition, the **install all** command will verify the integrity of the NX-OS image. Refer to section "Displaying File Contents" in **[4]**. If the hashes do not match, contact Cisco Technical Assistance Center (TAC) http://tools.cisco.com/ServiceRequestTool/create/launch.do.

Step 9 Install the downloaded and verified software image onto your Nexus 5k as described in section "Setting Up Your Cisco NX-OS Device" of Chapter 3 "Using the Cisco NX-OS Setup Utility" in the *Fundamentals Configuration Guide* **[4]**.

Start your Nexus 5k as described in **[4]**. Confirm that your Nexus 5k loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console.

Table 6 Evaluated Software Images

Model	Software Version	Image Name	MD5 hash	SHA512
Cisco Nexus 5624Q	7.2(1)	n6000-uk9.7.2.1.N1.1.bin	242aa060bda4819bc3b0b75d35fff141	6bf7c213566aab4993836c4cdd57a73772fa8c27029369c9124d4d030de2499c5f7b6e05e5a5be49e39878d1ad696a4fdc62e56c0df4be893a5c029fec83d106
		n6000-uk9-kickstart.7.2.1.N1.1.bin	589dfe8dc01a2f164da91513497d6371	033f03df4bc102960ea25e96da054d5196d21ba8554ccd988727f6eb02617fe6925a081351049cab3d6345f3a579fcbc4b5c6b7e3c5095dfc119aff9f9752ae5
Cisco Nexus 5648Q	7.2(1)	n6000-uk9.7.2.1.N1.1.bin	242aa060bda4819bc3b0b75d35fff141	6bf7c213566aab4993836c4cdd57a73772fa8c27029369c9124d4d030de2499c5f7b6e05e5a5be49e39878d1ad696a4fdc62e56c0df4be893a5c029fec83d106

Model	Software Version	Image Name	MD5 hash	SHA512
		n6000-uk9-kickstart.7.2.1.N1.1.bin	589dfe8dc01a2f164da91513497d6371	033f03df4bc102960ea25e96da054d5196d21ba8554ccd988727f6eb02617fe6925a081351049cab3d6345f3a579fcbc4b5c6b7e3c5095dfc119aff9f9752ae5
Cisco Nexus 5672UP	7.2(1)	n6000-uk9.7.2.1.N1.1.bin	242aa060bda4819bc3b0b75d35fff141	6bf7c213566aab4993836c4cdd57a73772fa8c27029369c9124d4d030de2499c5f7b6e05e5a5be49e39878d1ad696a4fdc62e56c0df4be893a5c029fec83d106
		n6000-uk9-kickstart.7.2.1.N1.1.bin	589dfe8dc01a2f164da91513497d6371	033f03df4bc102960ea25e96da054d5196d21ba8554ccd988727f6eb02617fe6925a081351049cab3d6345f3a579fcbc4b5c6b7e3c5095dfc119aff9f9752ae5
Cisco Nexus 5696Q	7.2(1)	n6000-uk9.7.2.1.N1.1.bin	242aa060bda4819bc3b0b75d35fff141	6bf7c213566aab4993836c4cdd57a73772fa8c27029369c9124d4d030de2499c5f7b6e05e5a5be49e39878d1ad696a4fdc62e56c0df4be893a5c029fec83d106
		n6000-uk9-kickstart.7.2.1.N1.1.bin	589dfe8dc01a2f164da91513497d6371	033f03df4bc102960ea25e96da054d5196d21ba8554ccd988727f6eb02617fe6925a081351049cab3d6345f3a579fcbc4b5c6b7e3c5095dfc119aff9f9752ae5
Cisco Nexus 56128P	7.2(1)	n6000-uk9.7.2.1.N1.1.bin	242aa060bda4819bc3b0b75d35fff141	bf7c213566aab4993836c4cdd57a73772fa8c27029369c9124d4d030de2499c5f7b6e05e5a5be49e39878d1ad696a4fdc62e56c0df4be893a5c029fec83d106
		n6000-uk9-kickstart.7.2.1.N1.1.bin	589dfe8dc01a2f164da91513497d6371	033f03df4bc102960ea25e96da054d5196d21ba8554ccd988727f6eb02617fe6925a081351049cab3d6345f3a579fcbc4b5c6b7e3c5095dfc119aff9f9752ae5
Cisco Nexus 2224TP	N/A	Not Applicable		
Cisco Nexus 2248TP	N/A	Not Applicable		
Cisco Nexus 2248TP-E	N/A	Not Applicable		

Model	Software Version	Image Name	MD5 hash	SHA512
Cisco Nexus 2232PP	N/A	Not Applicable		
Cisco Nexus 2248PQ	N/A	Not Applicable		
Cisco Nexus 2232TM	N/A	Not Applicable		
Cisco Nexus 2232TM-E	N/A	Not Applicable		
Cisco Nexus B22HP	N/A	Not Applicable		
Cisco Nexus B22F	N/A	Not Applicable		
Cisco Nexus B22DELL	N/A	Not Applicable		

3 Secure Installation and Configuration

3.1 Physical Installation

Follow the Cisco Nexus 5600 and 2000 Series Hardware Installation and Reference Guides **[9]** for hardware installation instructions. Follow these directions for connecting all N5k and N2k models.

3.2 Initial Setup via Direct Console Connection

The Nexus 5k must be given basic configuration via console connection prior to being connected to any network.

3.2.1 Options to be chosen during the initial setup of the Nexus 5k

For an un-configured N5K the setup utility will automatically run at initial startup of the switch from the CLI console. To run the setup utility once a switch has already been configured simply execute the "setup" command at the CLI. When setup is initiated, it presents the System Configuration Dialog. This dialog guides the administrator through the initial configuration with prompts for basic information about the TOE and network and then creates an initial configuration file. After the file is created, an authorized administrator can use the CLI to perform additional configuration. For initial setup, follow the directions in Chapter 3 Using the Cisco NX-OS Setup Utility *Cisco Nexus 5600 Series NX-OS Fundamentals Configuration Guide* **[4]**. The following items must be noted during setup:

For Step 1 Enable password-strength checking by using the command "**password strength-check**. This will ensure the password complexity rules are automatically enforced when an administrator user creates their password.

For Step 2 Choose a strong password according to the guidelines below.

Characteristics of Strong Passwords

A strong password has the following characteristics:

- At least eight characters long
- Does not contain many consecutive characters (such as "abcd")
- Does not contain many repeating characters (such as "aaabbb")
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers
- Contain special characters

For Step 3 Do **NOT** configure the SNMP community string. SNMP management is not allowed in the TOE.

For Step 4 Configure advanced IP options such as the static routes, default network, DNS, and domain name is optional

Example:

Configure Advanced IP options (yes/no)? [n]: **no**

Note: No is the default here. However, if you choose not to configure the advanced IP options you will skip steps 12-15.

For Step 5 Telnet service. Ensure that the telnet service is **NOT** enabled by changing the selection to **no**.

Example:

Enable the telnet service? (yes/no) [y]: **no**

For Step 6 Enable the SSH service by entering yes. You can then enter the key type and number of key bits. For more information, see "Generating SSH Server Keys" from **[3]**. RSA keys of 1024 bits or greater must be used.

Example:

Enable the ssh service? (yes/no) [y]: **yes**

Type of ssh key you would like to generate (dsa/rsa) : *rsa*

Number of key bits <768-2048>: *1024 (or higher)*

3.2.2 FEX Configuration

After the FEX has been cabled and installed and the 5600 switch has been powered up and operational, the 5600 switch has to be configured to see the attached FEX. See the **[11]** *Cisco Nexus 5000 Series Command Reference,* section "Fabric Extender Commands" for more information.

Configure a virtual port-channel and add physical interfaces. One FEX uplink will be connected to one 5k. One topology option is to dual-home the physical Fabric Extender. Dual-homing a FEX provides path redundancy, but cuts in half the total number of Fabric Extenders that can be deployed. A Nexus 5k supports 24 total connected FEX devices, meaning that two 5ks could support 48 total single-homed physical FEX. When dual-homing, only 24 total FEX are supported between the two 5ks. Then, all four of the FEX uplinks will be combined into a single virtual port channel. Each FEX is assigned a number from 100-199.

The physical interface requires two specific commands to tell the hosting 5K that the interface is servicing a FEX. The command "**switchport mode fex-fabric**" lets the Nexus switch know that the device on the other end of the link is a fabric extender.

The command "**fex associate**" tells the Nexus switch which specific FEX is being uplinked to that port. The number selected must match for all uplink ports. The following are example commands to configure the 5k to see the attached FEX. Sample configuration is below:

switch# **configure terminal**
switch(config)# **interface ethernet 1/1**
switch(config-if)# **switchport mode fex-fabric**
switch(config-if)# **fex associate 101**

Example Running Config:

```
interface Po101
description UPLINK FEX-01
vpc 101
switchport mode fex-fabric
fex associate 101
no shut

interface Ethernet1/1
description UPLINK FEX-01
switchport mode fex-fabric
fex associate 101
channel-group 101
no shut

interface Ethernet1/9
description UPLINK FEX-01
switchport mode fex-fabric
fex associate 101
channel-group 101
no shut
```

To verify that the FEX connection is up and operational, use the following show commands:

This command shows the physical 5500 ports uplinked to a physical FEX port.
switch# **show interface fex-fabric**

This command displays all of the FEX access ports:
switch# **show interface status fex 101**

3.2.3 Saving Configuration

NX-OS uses both a running configuration and a startup configuration. Configuration changes affect the running configuration, in order to save that configuration the running configuration (held in memory) must be copied to the startup configuration. This may be achieved by using the following command **[4]**, see section "Copying Configuration Files" and "Backing Up Configuration Files":

TOE-common-criteria# **copy nvram:snapshot-config nvram:startup-config**
Warning: this command is going to overwrite your current startup-config:
Do you wish to continue? {y/n} [y] y

(Note: A short hand version of the command is **copy run start**). These commands should be used frequently when making changes to the configuration of the switch. If the switch reboots and resumes operation when uncommitted changes have been made, these changes will be lost and the switch will revert to the last configuration saved.

3.2.4 Enabling FIPS Mode

In the evaluated configuration the TOE is run in the FIPS mode of operation. By default, FIPS mode is disabled. The "fips mode enable" command needs to be run in order to turn on FIPS mode. A reload is required for the system to operate in FIPS mode.

To enable FIPS mode, follow the below steps:

TOE-common-criteria# **configure terminal**

TOE-common-criteria (config)# **fips mode enable**

TOE-common-criteria (config)# **exit**

TOE-common-criteria# **show fips status**

FIPS mode is enabled

TOE-common-criteria# **copy running-config startup-config**

TOE-common-criteria# **reload**

When the system is booted up in FIPS mode, the FIPS power-up self-tests run on the supervisor and line card modules. If any of these FIPS self-tests fail, the whole system is moved to the FIPS error state. In this state, as per the FIPS requirement, all cryptographic keys are deleted, and all line cards are shut down. This mode is exclusively meant for debugging purposes.

Once the switch is in the FIPS error state, any reload of a line card moves it to the failure state. To move the switch back to FIPS mode, it has to be rebooted. However, once the switch is in FIPS mode, any power-up self-test failure on a subsequent line card reload or insertion affects only that line card, and only the corresponding line card is moved to the failure state.

If any of the self-tests fail, the TOE transitions into an error state. In the error state, all secure data transmission is halted and the TOE outputs status information indicating the failure.

Note: If an error occurs during the self-test, a SELF_TEST_FAILED system log is generated.

Example Error Message Error Message SECURITYD-2-FIPS_SELF_TEST_FAILED: FIPS self-test failure : [chars]

Explanation FIPS self-test failed [chars] for service [chars]

Cisco provides an online error message decoder that can be used for looking up any error messages that may be received: https://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi

Also an exhaustive list of NX-OS error messages are located in the *Nexus 5600 Series NX-OS System Messages Reference* **[10]**.

3.2.5 Administrator Configuration and Credentials

The Nexus 5k must be configured to use a username and password for each administrator and one password for the enable command. There are three possible passwords: enable password, enable secret, and virtual terminal (vty) password. Enable password provides the local console password for accessing the User mode.

Warning: If an unprivileged administrator user has this password and has access to the local console, they will be able to issues all commands.

Enable secret sets the password for Enable mode. The vty password sets the password for remotely accessing the CLI via SSH. All three must adhere to the password complexity rules.

Ensure all passwords are not stored in plaintext, but a SHA256 hash of the password is stored by using the following listed commands. See **[11]** *Cisco Nexus 5000 Series Command Reference,* command "username":

TOE-common-criteria (config)#**username** *name* {**password** *password* | **password** *5*}

TOE-common-criteria# **username network-admin password 5**

TOE-common-criteria# **key config-key ascii**

Configures local AAA authentication:

TOE-common-criteria(config)# **aaa authentication login default local**

All NX-OS administrators will have a role assigned to them

TOE-common-criteria# configure terminal

3.2.5.1 Assigning User Roles

User accounts have the following attributes:

- Username
- Password
- Expiry date
- User roles

An authorized administrator can enter the password in clear text format or encrypted format. The Cisco NX-OS password encrypts clear text passwords before saving them to the running configuration. Encrypted format passwords are saved to the running configuration without further encryption.

TOE-common-criteria(config)# **configure terminal**

Displays the user roles available. An authorized administrator can configure other user roles, if necessary:

TOE-common-criteria(config)# (Optional) **show role**

For the username, valid characters are uppercase letters A through Z, lowercase letters a through z, numbers 0 through 9, hypen (-), period (.), underscore (_), plus sign (+), and equal sign (=). The at symbol (@) is supported in remote usernames but not in local usernames. Remote usernames would be users stored in the remote AAA server, not local database. "5" specifies that the password is in encrypted format.

TOE-common-criteria(config)# **username user-id [password [0 | 5] password] [role role-name]**

Example:
switch(config)# username NewUser password 4Ty18Rnt! network-admin

TOE-common-criteria(config)# **exit**
TOE-common-criteria(config)# (Optional) **show user-account**
TOE-common-criteria(config)# (Optional) **copy running-config startup-config**

An authorized administrator can configure up to 64 user custom user roles. Each user role can have up to 256 rules. The rule number that an administrator specifies determines the order in which the rules are applied. Rules are applied in descending order. For example, if a role has three rules, rule 3 is applied before rule 2, which is applied before rule 1. Regardless of the read-write rule configured for a user role, some commands can be executed only through the predefined network-admin role. For more information on user roles, see the Cisco Nexus 5500 Series NX-OS Security Command Reference **[6]**.

3.2.5.2 Mapping of NX-OS roles to IOS privileges[1]

To enable NX-OS to be administered by the same TACACS+ servers that administer other Cisco IOS/IOS-XE devices, an authorized administrator can map the privilege levels configured on TACACS+ servers to user roles configured on Cisco NX-OS devices by using the '**feature privilege**' command. Enables or disables the cumulative privilege of roles. Users can see the enable command only if this feature is enabled. By default this is disabled.

TOE-common-criteria(config)# **feature privilege**

Enables or disables a secret password for a specific privilege level. Users are prompted to enter the correct password upon each privilege level escalation. "5" specifies that the password is in SHA256 hashed format. By default this is disabled.

TOE-common-criteria(config)# **enable secret [0 | 5] password [priv-lvl priv-lvl | all]**

Example: **switch(config)# enable secret 5 def456 priv-lvl 15**

Enables or disables a user to use privilege levels for authorization. The default is disabled. The priv-lvl keyword specifies the privilege level to which the user is assigned. There is no default privilege level. Privilege levels 0 to 15 (priv-lvl 0 to priv-lvl 15) map to user roles priv-0 to priv-15.

TOE-common-criteria(config)# **username username priv-lvl n**

[1] Section " Configuring Privilege Level Support for Authorization on TACACS+ Servers" [3]

TOE-common-criteria# (Optional) **show privilege**

TOE-common-criteria# (Optional) **copy running-config startup-config**

TOE-common-criteria# **exit**

Enables a user to move to a higher privilege level. This command prompts for the secret password. The level argument specifies the privilege level to which the user is granted access. The only available level is 15.
TOE-common-criteria# **enable level**

3.2.6 Session Termination

Inactivity settings must trigger termination of the administrator session. These settings are configurable as follows:

TOE-common-criteria(config)# **line vty <first> <last> [4]** under section "Configuring the Console Port"

For example: TOE-common-criteria(config)# **line vty 0 4**

TOE-common-criteria(config-line)# **exec-timeout <time> [5]** *Cisco NX-OS Configuration Fundamentals Command Reference*.

TOE-common-criteria(config-line)# **line console [5]**

TOE-common-criteria(config)# **exec-timeout <time>**

To save these configuration settings to the startup configuration:

copy run start

where first and last are the range of vty lines on the box (i.e. "0 4"), and time is the period of inactivity after which the session should be terminated. Configuration of these settings is limited to the privileged administrator (see Section 4.1).

The line console setting is not immediately activated for the current session. The current console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session.

An access class should be applied to the VTY port to increase security by restricting SSH access to specific source and destination IP addresses. An access class configured on the VTY port is applicable when using an in-band or out-of-band management strategy. An access-class is configured per traffic direction, **in** applies to inbound sessions and **out** applies to outbound sessions.

Statistics can be enabled with the access list **statistics per-entry**. The following example illustrates a basic policy that permits SSH traffic from a specific subnet to all IP addresses configured. All traffic is permitted if an access-class is applied to the VTY port and the associated access-list is deleted from the configuration.

```
n5600(config)# ip access-list vty-acl-in
n5600(config-acl)# permit tcp x.x.x.x/24 any eq 22
n5600(config)# line vty
n5600(config-line)# ip access-class vty-acl-in in
```

3.3 Network Protocols and Cryptographic Settings

3.3.1 Remote Administration Protocols

Telnet for management purposes is disabled by default. By default, the Secure Shell (SSHv2) server is enabled. NX-OS only supports SSHv2. The command to enable ssh is the **feature ssh** command **[6]**. The SSH setting is configured during the initial setup. To edit the ssh configuration see "Configuring SSH" from **[3],** chapter 8. The below steps are included as a reference since SSHv2 is enabled by default.

SSH Server Configuration:

1. Generate RSA key material section "Configuring SSH" in **[3]** – choose a longer modulus length for more secure keys (i.e., 2048 for RSA and 256):

   TOE-common-criteria# **crypto key generate rsa**

   TOE-common-criteria# How many bits in the modulus [512]: **2048**

   or

   TOE-common-criteria(config)# **crypto key generate rsa keysize [1024 or 2048]**

   RSA and ECDSA keys are generated in pairs—one public RSA key and one private RSA key. This command is not saved in the switch configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.
   Note: *Only one set of keys can be configured using the* ***crypto key generate*** *command at a time. Repeating the command overwrites the old keys.*
   Note: *If the configuration is not saved to NVRAM with a "****copy run start****", the generated keys are lost on the next reload of the* switch .
   Note: *If the error "% Please define a domain-name first" is received, enter the command '****ip domain-name [domain name]****'.*

2. To enable ssh, use the enable ssh server command:

   TOE-common-criteria(config)# **feature ssh**[2]

The supervisor module mgmt0 port should be configured with an inbound access list to increase security by restricting access to specific source host/subnet addresses destined to specific management protocols configured on the Nexus 5600. The access-list entries will vary depending on the management protocols that are enabled. Access-list statistics can be tracked per

[2] **feature ssh** was introduced to replace the **ssh server enable** command

ACL entry if the ACL command **statistics per-entry** is configured. The supervisor module CPU performs access-list processing when an access-list is applied to the mgmt0 port.

```
n5600(config)# ip access-list mgmt0-access
n5600(config-acl)# statistics per-entry
n5600(config-acl)# permit tcp x.x.x.x/x b.b.b.b/32 eq 22
n5600(config-acl)# permit tcp x.x.x.x/x b.b.b.b/32 eq tacacs
n5600(config)# interface mgmt0
n5600(config-if)# ip access-group mgmt0-access in
n5600(config-if)# ip address b.b.b.b/xx
```

SSH Client Configuration:

The Nexus 5600 Series Switch with 2000 Series Fabric Extenders will support AES-CBC-128, and AES-CBC-256, both of which are permitted in the certified configuration. The Nexus 5600 Series Switch with 2000 Series Fabric Extenders will also negotiate sessions using 3DES-CBC, which is not recommended for use in the certified configuration, though it is approved for use in the FIPS validated configuration. Since security-relevant use of the SSH connection only occurs after the session parameters are negotiated (when authentication parameters are being exchanged during login, and after successful authentication), Nexus 5600 Series Switch with 2000 Series Fabric Extenders administrators configure their SSH clients to either:

- not establish connections using 3DES-CBC; or
- warn about potential use of 3DES-CBC, at which point the administrator must reject the session and reconfigure the client, or use a different client.

To configure a Linux-based SSH client to support only the following specific encryption algorithms AES-CBC-128 and AES-CBC-256 the following commands can be used.
Configure a SSH client to support only the following specific encryption algorithms:

- AES-CBC-128
- AES-CBC-256

peer#**ssh -l cisco -c aes128-cbc 1.1.1.1**
peer#**ssh -l cisco -c aes256-cbc 1.1.1.1**

1. Configure a SSH client to support message authentication. The following MACs are allowed and "None" for MAC is not allowed:
   a. hmac-sha1

   peer#**ssh -l cisco -m hmac-sha1-160 1.1.1.1**
   peer#**ssh -l cisco -m hmac-sha1-96 1.1.1.1**
   peer#**ssh -l cisco -m hmac-md5 1.1.1.1**
   peer#**ssh -l cisco -m hmac-md5-96 1.1.1.1**

2. To verify the proper encryption algorithms are used for established connections, use the **show ssh sessions** command:

   TOE-common-criteria# **show ssh sessions**

   Note: *To disconnect SSH sessions, use the* ***clear ssh session*** *command:*

*TOE-common-criteria# clear **ssh***

3. HTTP and HTTPS servers were not evaluated and must be disabled:
   TOE-common-criteria# (config)# **no ip http server**
   TOE-common-criteria(config)# **no ip http secure-server**

4. SNMP server was not evaluated and must be disabled, see **[7]**:

TOE-common-criteria(config)# **no snmp-server protocol enable**

3.3.2 Logging Configuration

The Nexus 5600 Series Switch with 2000 Series Fabric Extenders supports local logging of events which are referred to as system messages in the Cisco Nexus 5k Documentation. Logs are stored in local system files in DRAM, NVRAM, and logflash. By default messages of severity 0, 1, and 2 are logged to the console and in nvram, where nvram stores only the last 100 messages. The severity level for logging to the console can be changed by command '**logging console**', but for nvram it can't be changed. By default, messages of severity 0,1,2,3,4 and 5 get logged in log:messages (DRAM) and in the logflash file (logflash://sup-local/log/messages). The severity level for the DRAM logfile can be changed and the same will be reflected for the logflash file. Both the DRAM and logflash files will have the same severity level. The **logging logfile** global configuration command enables copying of system messages to an internal log file and optionally sets the size of the file.[3] When setting a logging level for AUTHPRIV do not set the level any higher than 4. As any higher will show usernames in the logs for low privilege users.

n5600# **show logging logfile** <- Displays the contents of the default log file.
n5600# **show logging last 10** <- Displays the last # of lines of the default log file.
n5600# **show logging NVRAM** <- Displays contents of the log file stored in NVRAM.
n5600# **show file logflash://sup-local/log/messages** <- Displays contents in logflash.

The log files are written to DRAM and logflash and are circular. In logflash, the maximum file size is 4MB on final images, while it is 10MB on GDB images. To display the system messages that are logged in the file, use the **show logging** EXEC command. The first message displayed is the oldest message in the buffer. To clear the current contents of the buffer, use the **clear debug-logfile** command.

Changing the default configuration of the logging levels can be made. See section "Configuring System Message Logging to Terminal Sessions" and "Logging System Messages to a File" in **[2]** *Cisco Nexus 5600 Series NX-OS System Management Configuration Guide.* By default, audit events are logged to the log:messages file in DRAM.

Authentication and authorization events are maintained in the local accounting log. See chapter "Configuring AAA", section "Monitoring and Clearing the Local AAA Accounting Log" of **[3]** for information on viewing and clearing these logs. In addition, for more information on configuring system logging see **[2]**, section **"**Configuring System Message Logging". The accounting log for Authentication, Authorization, and Accounting (AAA) and local, allows us to

[3] "Saving the System Messages Log" in the System messages Guide [10]

see all the config commands run on the devices from any user. In order to enable logging of all commands use the **terminal log-all** command.

#TOE-common-criteria (config)# **terminal log-all**

To view the audit events for Authentication, Authorization, and Accounting (AAA) and local:

#TOE-common-criteria (config)# **show accounting log all**

To enable Login Authentication Failure Messages:

#aaa authentication login error-enable

System events are maintained by default in the file "logflash:" filesystem. This file can be viewed and the settings for it can be modified as indicated in chapter “Configuring System Message Logging” and sections “Logging System Messages to a File” and “Displaying and Clearing Log Files” of **[2]** *Cisco Nexus 5600 Series NX-OS System Management Configuration Guide*.

TOE-common-criteria (config)# **dir logflash:**

If the logflash filesystem is not mounted, try to manually mount it:

TOE-common-criteria (config)# **mount logflash:**

TOE-common-criteria (config)# **show logging nvram** [**last** *number-lines*]

TOE-common-criteria (config)# **clear logging nvram**

To send the audit logs to a remote syslog server, see section "Configuring Syslog Servers" in the **[2]** *Cisco Nexus 5600 Series NX-OS System Management Configuration Guide.*

3.3.3 Virtual Port Channel Operations

Information related to the Virtual Device Context functions can be found in **[8]** *Cisco Nexus 5500 Series NX-OS Virtual Port Channel Command Reference*.

3.3.4 VLAN Hopping Prevention

Information related to preventing VLAN hopping can be found in **[13]** *Cisco Nexus 5600 Series NX-OS Interfaces Configuration Guide*, sections "Configuring Native 802.1Q VLANS" and "Understanding Native 802.1Q VLANS".

To prevent VLAN hopping, the **vlan dot1q tag native** command performs the following functions:

- On the ingress side, all untagged data traffic is dropped.
- On the egress side, all traffic is tagged. If traffic belongs to native VLAN it is tagged with the native VLAN ID.

switch# **configure terminal**
switch(config)# **vlan dot1q tag native**
switch# **exit**
switch# **show vlan dot1q tag native**
vlan dot1q native tag is enabled

3.3.5 Routing Protocols

The routing protocols are used to maintain routing tables. The routing tables can also be configured and maintained manually. Refer to the applicable sections in **[4]** *Fundamentals Configuration Guide* for configuration of the routing protocols.

The following routing protocols are used on all of the TOE models:

- Open Shortest Path First (OSPF) Protocol Versions 2 (IPv4) and 3 (IPv6)
- Intermediate System-to-Intermediate System (IS-IS) Protocol for IPv4
- Border Gateway Protocol (BGP) for IPv4 and IPv6
- Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv4 and IPv6
- Routing Information Protocol Version 2 (RIPv2)
- Protocol Independent Multicast (PIM)

3.3.6 Non-Approved Algorithms and Protocols

This section details the algorithms and protocols that were not evaluated. These algorithms and protocols are supported by the TOE and are disabled by default. They will not to be configured for use in the evaluated configuration.

- DES
- 3DES
- HMAC MD5
- MD5
- NDRNG
- RC4
- ftp
- telnet
- GRE
- PMTUD
- LLDP
- NX-API

4 Secure Management

Cisco NX-OS devices support Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) protocols. Based on the user ID and password combination that an authorized administrator provides, Cisco NX-OS devices perform authentication using the local database or remote authentication using one or more AAA (RADIUS or TACACS+) servers. A pre-shared secret key provides security for communication between the Cisco NX-OS device and AAA servers. An authorized administrator can configure a common secret key for all AAA servers or for only a specific AAA server. See **[3]** section "AAA Security Services" for more information.

4.1 User Roles

All users on the NX-OS are considered to be administrator users. An authorized administrator which is also referred to as a security administrator can create and manage administrator user accounts and assign roles that limit access to operations on the Cisco NX-OS device. Role Based Access Control (RBAC) allows an authorized administrator to define the rules for an assigned role that restrict the authorization that the user has to access management operations.

Administrator user roles contain rules that define the operations allowed for the user who is assigned the role. Each administrator user role can contain multiple rules and each administrator user can have multiple roles. For example, if role1 allows access only to configuration operations, and role2 allows access only to debug operations, then users who belong to both role1 and role2 can access configuration and debug operations. An authorized administrator can also limit access to specific VLANs, virtual routing and forwarding instances (VRFs), and interfaces.

The Cisco NX-OS software provides four default user roles as follows:

- network-admin - Complete read-and-write access to the entire Cisco NX-OS device
- network-operator - Complete read access to the entire Cisco NX-OS device

An authorized user cannot change these default roles and their associated privileges. NX-OS does allow for custom roles to be created. Chapter Configuring User Accounts and RBAC, section "Creating User Roles and Rules" in the **[3]** describes how to configure the administrator user accounts with the associated roles that give the administrator specific access

Information related to the System Security functions for the N5K Network-Admin and Network-Operator roles can be found in section "User Roles" in **[3]** Cisco Nexus 5600 Series NX-OS Security Configuration Guide and **[6]** Cisco Nexus 5500 Series NX-OS Security Command Reference.

4.2 Local Passwords

The password complexity is enforced by the switch by using the "**password strength-check**" command, see "Enabling Password-Strength Checking" in **[3]**.

TOE-common-criteria# **conf t**
TOE-common-criteria (config)# **password strength-check**
TOE-common-criteria (config)# **exit**
TOE-common-criteria# **copy run start**

When an authorized administrator enables password-strength checking, the Cisco NX-OS software only allows an administrator to create strong passwords. The characteristics for strong passwords include the following which are enforced by NX-OS:

- At least eight characters long
- Does not contain many consecutive characters (such as “abcd”)
- Does not contain many repeating characters (such as “aaabbb”)
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

The following configuration steps are optional, but recommended for good password complexity. The below items are recommended but are not enforced by the TOE:

1. Does not contain more than three sequential characters, such as abcd
2. Does not contain dictionary words
3. Does not contain common proper names

Administrative passwords, including any “enable” password that may be set for any privilege level, must be stored in non-plaintext form.

4.2.1 RADIUS/TACACS+

To configure the local console to work with a RADIUS or TACACS+ server see section "Configuring Console Login Authentication Methods" in **[3]**.

If using RADIUS:

TOE-common-criteria# **conf t**
TOE-common-criteria (config)# **aaa authentication login console group radius**
TOE-common-criteria (config)# **exit**
TOE-common-criteria# **copy run start**

If using TACACS+:

TOE-common-criteria# **conf t**
TOE-common-criteria (config)# **feature tacacs+**
TOE-common-criteria (config)# **exit**
TOE-common-criteria# **copy run start**

4.2.1.1 User Authorization (Roles) To Be Handled by RADIUS/TACACS

Configuring authentication and authorization methods for console logins, use the '**aaa authentication login console**' command. This example shows how to configure the

authorization authentication console login methods:

switch# **configure terminal**

switch(config)# **aaa authentication login console group [radius tacacs+]**[4]

To configure default AAA authorization methods for all EXEC commands, use the aaa authorization commands default command. This command allows for all authorization (role) data to be sent to the TACACS+ Server automatically when user accounts are created:

switch# **configure terminal**
switch(config)# **aaa authorization config-commands default group TacGroup local**

To configure the default authentication, authorization, and accounting (AAA) RADIUS server groups for authorization, use the aaa authorization cts default group command.

To use the aaa authorization cts default group command, an authorized administrator must enable the Cisco TrustSec feature using the 'feature cts' command.

switch# **feature cts**
switch# **configure terminal**
swtich(config)# **aaa authorization cts default group RadGroup**

4.3 Clock Management

Clock management is restricted to the privileged administrator.

For instructions to set the timezone for the clock, refer to section "Configuring the Time Zone" in **[4]**.

To manually set the clock see section "Manually Setting the Device Clock" in **[4]**.

TOE-common-criteria# **clock set** *time day month year*

For Example:
TOE-common-criteria# clock set 15:00:00 30 May 2008 Fri May 30 15:14:00 PDT 2008

4.4 Identification and Authentication

Configuration of Identification and Authentication settings is restricted to the privileged administrator.

The Nexus 5k can be configured to use any of the following authentication methods:

- Remote authentication (RADIUS or TACACS+)

[4] [6] aaa authentication login console

- Refer to “Authentication Server Protocols” elsewhere in this document for more details.

- Local authentication (password or SSH public key authentication);
  - Note: this should only be configured for local fallback if the remote authentication server is not available.

4.5 Login Banners

The TOE may be configured by the privileged administrators with banners using the **banner motd** command. This banner is displayed before the username and password prompts. To create a banner of text “This is a banner” use the command. See **[5]** *Cisco Nexus 5600 Series NX-OS Fundamentals Command Reference*

TOE-common-criteria# **configure terminal**

TOE-common-criteria (config)# **banner motd #Welcome to the switch#**

TOE-common-criteria (config)# **show banner motd**

Welcome to the switch

4.5.1 Information Flow Policies

The TOE may be configured by privileged administrators for information flow control using the access control functionality. Each information flow is controlled by the supervisor (permit, drop, ignore) via the ACLs, while the network traffic is mediated via the I/O network module ports. Configuration of information flow policies is restricted to the privileged administrator. See chapter "Configuring IP ACLs", section "Configuring IP ACLs" **[3].**

On the TOE, an authorized administrator can define the traffic rules on the box by configuring access lists (with permit, deny, and/or log actions) and applying these access lists to interfaces:

- The ‘discard’ option is accomplished using access lists with deny entries, which are applied to interfaces within access-groups.
- The ‘bypassing’ option is accomplished using access lists with deny entries, which are applied to interfaces.
- The ‘protecting’ option is accomplished using access lists with permit entries, which are applied to interfaces.

The TOE enforces information flow policies on network packets that are receive by TOE interfaces and leave the TOE through other TOE interfaces. When network packets are received on a TOE interface, the TOE verifies whether the network traffic is allowed or not and performs one of the following actions, pass/not pass information, as well as optional logging.

The information flow policies are configured using Access Control Lists (ACL):

- port-based ACLs [PACLs]
- VLAN-based ACLs [VACLs],
- router-based ACLs [RACLs].

4.5.1.1 PACL MAC ACL policies:

- Ingress Ethernet traffic with security attributes that match an administratively configured Layer 2 PACL permit policy for non-IP traffic rule is allowed to flow, or,
- Ingress Ethernet traffic with security attributes that match an administratively configured deny policy rule is not permitted.
- The PACL permit/deny polices for non-IP traffic are comprised of a combination of subject security attributes and information attributes and a permit/deny operation. The subject attributes that are available for the creations of PACL permit/deny policies include: slot, port, and channel-number. The information attributes that are available for the creations of PACL permit/deny policies for non-IP traffic include: Source MAC address, Destination MAC address, Protocol, Class of Service (COS), and VLAN ID.

In addition, the following policies also operate on the Layer 2 information -

4.5.1.2 Port policies:

- Network traffic flow is permitted if the source MAC address is administratively configured as secure for the Nexus 5600 interface, or,
- The source MAC address is dynamically identified as secure by the TOE.
- And, the network traffic flow is not denied by any IP Source Guard/Traffic Storm/DHCP Snooping/Dynamic ARP Inspection policies
- If a Nexus 5600 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.

4.5.1.3 Dynamic ARP Inspection (DAI) policies:

DAI ensures that only valid ARP requests and responses are relayed.

- The TOE permits ARP traffic flows received on an untrusted Nexus 5600 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 5600 switch interface if a valid IP-to-MAC address binding does not exist within the DHCP binding table.

4.5.1.4 VACL policies:

VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces. They are used in conjunction with VLANs. The Cisco Nexus 5600 Series NX-OS Layer 2 Switching Guide **[12]**, chapter "Configuring VLANS" describes how to configure a VLAN. When configuring communications between peer switches, separate VLANs should be

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

The policies associated with VACLs are:

- Ethernet traffic with security attributes that match an administratively configured permit policy rule is allowed to flow, or,
- Ethernet 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,
- Ethernet 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 polices for Ethernet 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.

The following example shows how to define and apply a VLAN access map labeled "*vmap4"* to VLANs 5 and 6 that causes the VLAN to forward an IP packet if the packet matches the conditions defined in access list labled "*al2"*:

Switch(config)# **vlan access-map vmap4**
Switch(config-access-map)# **match ip address al2**
Switch(config-access-map)# **action forward**
Switch(config-access-map)# **exit**
Switch(config)# **vlan filter vmap4 vlan-list 5-6**

For more detail on configuration of VACLs, refer to "VLAN ACLs (VACLs)" in **[12]**.

In this example, we are assuming that interface GigabitEthernet0/0 is the external interface, and is assigned an IP address of 10.200.1.1. Interface GigabitEthernet0/1 is the internal interface and is assigned an IP address of 10.100.1.1.

To prevent the passing of traffic with an internal source address on the external Interface, apply the following access control list to the external interface:

Switch# **configure terminal**

Switch(config)# **access-list 199 deny ip 10.100.0.0 0.0.255.255 any log-input**

To prevent the passing of traffic with an external source address on the internal Interface, apply the following access control list to the internal interface:

Switch# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# **access-list 100 deny ip 10.200.0.0 0.0.255.255 any log-input**

To prevent the passing of traffic with a broadcast or loopback address on either interface, apply the following access control list to both interfaces:

Switch# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# **access-list 100 deny ip 224.0.0.0 15.255.255.255 any log-input**

Switch(config)# **access-list 100 deny ip 255.255.255.255 0.0.0.0 any log-input**

Switch(config)# **access-list 100 deny ip 127.0.0.0 0.255.255.255 any log-input**

Switch(config)# **access-list 199 deny ip 224.0.0.0 15.255.255.255 any log-input**

Switch(config)# **access-list 199 deny ip 255.255.255.255 0.0.0.0 any log-input**

Switch(config)# **access-list 199 deny ip 127.0.0.0 0.255.255.255 any log-input**

If remote administration is required, ssh has to be explicitly allowed through either the internal or external interfaces.

Switch# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# **access-list 199 permit tcp host 10.200.0.1 host 10.200.0.1 eq 22 log-input**

To close ports that don't need to be open and may introduce additional vulnerabilities, implement the following acl:.

Switch(config)# **access-list 100 deny 132 any any log-input**

Switch(config)# **access-list 199 deny 132 any any log-input**

To apply the acls to the interfaces:

Switch(config)# **interface GigabitEthernet0/0**

Switch(config-if)# **ip access-group 199 in**

Switch(config)# **interface GigabitEthernet0/1**

Switch(config-if)# **ip access-group 100 in**

4.5.1.5 RACL router ACL policies:

The key difference between the RACL and PACL/VACL ACLs are that the RACL are applied to Layer 3 interfaces including the Management Interface. The commands used are the same, the particular interfaces the RACL apply to differs. See section "Configuring IP ACLs" in the **[3]** *Cisco Nexus 5600 Series NX-OS Security Configuration Guide* for more details.

4.5.2 Configuration of VRF

A VRF represents a layer 3 addressing domain. Each layer 3 interface (logical or physical) belongs to one VRF. For more information, see **[13]** *Cisco Nexus 5600 Series NX-OS Interfaces Configuration Guide* chapter Configuring Layer 3 Interfaces.

5 Auditing

The TOE is able to generate audit records that are stored internally within the TOE whenever an audited event occurs, as well as simultaneously offloaded to an external syslog server.

The administrator can set the level of the audit records to be stored in a local buffer, displayed on the console, sent to the syslog server, or all of the above. The details for configuration of these settings are covered in Section 3.3.2 above.

The local log buffer is circular. Newer messages overwrite older messages after the buffer is full. The first message displayed is the oldest message in the buffer.

5.1 Deleting Audit Records

The TOE provides the privileged Administrator the ability to delete audit records audit records stored within the TOE.

This is done with the clear logging command.

TOE-common-criteria# **clear logging**

Clear logging buffer [confirm] <ENTER>

TOE-common-criteria# **clear logging nvram**

5.2 Audit Records Description

The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table below). Each of the events is specified in syslog records in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the startup and shutdown of the audit functionality is audited.

The local audit trail consists of the individual audit records; one audit record for each event that occurred. The audit record can contain up to 80 characters and a percent sign (%), which follows the time-stamp information. The audit fields in each audit event will contain at a minimum the following:

Example Audit Event: 2014 May 14 13:12:40 india-29 %SECURITYD-2-FIPS_POWERUP_SELF_TEST_STATUS: FIPS RSA power-up self-test status : PASSED

Date: 2014 May 14

Time: 13:12:40

Type of event: %SECURITYD-2-FIPS_POWERUP_SELF_TEST_STATUS

Subject identity: Available when the command is run by an authorized TOE administrator user such as “user: admin”. In cases where the audit event is not associated with an authorized user, an IP address may be provided for the Non-TOE endpoint and/ or TOE.

Wed May 14 13:23:11 2014:type=update:id=console0:user=admin:cmd=clear accounting log (SUCCESS)

Outcome (Success or Failure): Success may be explicitly stated with “success” or “passed” contained within the audit event or is implicit in that there is not a failure or error message. More specifically for failed logins, a “Login failed” will appear in the audit event. For successful logins, a “Login success” will appear in the associated audit event. For failed events “failure” will be denoted in the audit event. For other audit events a detailed description of the outcome may be given in lieu of an explicit success or failure.

6 Modes of Operation

A N5K Family Switch has several modes of operation, these modes are as follows:

Booting – while booting, the switches drop all network traffic until the NX-OS image and configuration has loaded. This mode can transition to all of the modes below.

BIOS Loader Prompt – When the supervisor modules power up, a specialized BIOS image automatically loads and tries to locate a valid kickstart image for booting the system. If a valid kickstart image is not found, the following BIOS loader prompt displays:

loader>

System BIOS Setup – This is an interactive text based program for configuring low-level switch hardware and boot options. When this program is exited, the switch transitions to Booting mode. In this mode the switch has no IP address and therefore does not handle network traffic, thus preventing an insecure state.

Loader Prompt – This mode allows an administrator logged into the console port to specify a NX-OS image on a TFTP server to load. In this mode the switch does not handle any network traffic, apart from what is required to perform the TFTP boot, thus preventing an insecure state.

Setup – The switch enters this mode after booting if no configuration exists (eg. First boot). In this mode the switch has no IP address and therefore does not handle network traffic, thus preventing an insecure state. The switch starts an interactive setup program to allow the administrator to enter basic configuration data, such as the switch's IP address, administrator password, and management channels. When the setup program is exited, the switch transitions to the Normal mode.

Normal - The NX-OS image and configuration is loaded and the switch is operating as configured. It should be noted that all levels of administrative access occur in this mode and that all TOE security functions are operating as configured.

6.1 Module States

The Nexus5k switches can be deployed with a single or redundant pair of supervisors. The supervisor modules have some additional module states. The '**show module**' command shows the status of the supervisor or I/O cards.

Table 7 Module States[5]

show module Command Status Output	Description
powered up	The hardware has electrical power. When the hardware is powered up, the software begins booting.
testing	The switching module has established connection with the supervisor and the switching module is performing bootup diagnostics.
initializing	The diagnostics have completed successfully and the configuration is being downloaded.
failure	The switch detects a switching module failure upon initialization and automatically attempts to power-cycle the module three times. After the third attempt, the module powers down.
ok	The switch is ready to be configured.
power-denied	The switch detects insufficient power for a switching module to power up.
active	This module is the active supervisor module and the switch is ready to be configured.
HA-standby	The HA switchover mechanism is enabled on the standby supervisor module.

Table 8 Redundancy Modes: for Supervisor

Not present	The supervisor module is not present or is not plugged into the chassis.
Initializing	The diagnostics have passed and the configuration is being downloaded.
Active	The active supervisor module and the switch is ready to be configured.
Standby	A switchover is possible.
Failed	The switch detects a supervisor module failure on initialization and automatically attempts to power-cycle the module three (3) times. After the third attempt it continues to display a failed state.
Offline	The supervisor module is intentionally shut down for debugging purposes.
At BIOS	The switch has established connection with the supervisor and the supervisor module is performing diagnostics.
Unknown	The switch is in an invalid state. If it persists call TAC.

6.2 Self-Tests

When the system is booted up in FIPS mode, the FIPS power-up self-tests run on the supervisor and line cards. If any of these bootup tests fail, the whole system is moved to the FIPS error state. In this state, as per the FIPS requirement, all cryptographic keys are deleted, and all line cards are shut down. This mode is exclusively meant for debugging purposes.

[5] Section "Verifying the Status of a Module" [9]

Once the switch is in the FIPS error state, any reload of a line card moves it to the failure state. To move the switch back to FIPS mode, it has to be rebooted. However, once the switch is in FIPS mode, any power-up self-test failure on a subsequent line card reload or insertion affects only that line card, and only the corresponding line card is moved to the failure state.

All ports are blocked from moving to forwarding state during the POST[6]. Only when all components of all modules pass the POST is the system placed in FIPS PASS state and ports are allowed to forward data traffic.

If any of the POST fail, the following actions should be taken:

- Use the **system cores** command to set up core dumps on the system. This will provide additional information on the cause of the crash:

  switch# **configure terminal**

  switch(config)# **system cores slot0:core_file**

  Example:

  switch# **system cores tftp://x.x.x.x/filename**

  switch# **show system cores**

Note: The filename (indicated by filename) must exist in the TFTP server directory.

- Restart the TOE to perform POST and determine if normal operation can be resumed
- If the problem persists, contact Cisco Technical Assistance via http://www.cisco.com/techsupport or 1 800 553-2447

[6] Section "FIPS Self-tests" in [3]

7 Security Measures for the Operational Environment

Proper operation of the TOE requires functionality from the environment. It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides the necessary functions, and adheres to the environment security objectives listed below. The environment security objective identifiers map to the environment security objectives as defined in the Security Target.

Table 9 Operational Environment Security Measures

Environment Security Objective	IT Environment Security Objective Definition	Responsibility of the Administrators
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	The administrator should ensure that the Nexus 5600 series switches and the Nexus 2000 series fabric extender is only dedicated to its desired operation, and no general purpose computing capabilities (e.g., compilers or user applications) available on the switches and fabric extenders.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	The Nexus 5600 series switches and Nexus 2000 series fabric extenders must be installed to a physically secured location that only allows physical access to authorized personnel.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	Administrators must be trained and must read, understand, and follow the guidance in this document to securely install and operate the Nexus 5600 series switches and Nexus 2000 series fabric extenders.

8 Related Documentation

Use this document in conjunction with the NX-OS 15.1(3)S2 documentation at the following location:

- http://www.cisco.com/

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

8.1 World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

8.2 Ordering Documentation

Cisco documentation is available in the following ways:

Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

http://www.cisco.com/web/ordering/root/index.html

Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

http://www.cisco.com/go/subscription

Non-registered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS (6387).

8.3 Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click Feedback in the toolbar and select Documentation. After you complete the form, click Submit to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc., Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

9 Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com