53-1003494-02
23-March-15

Network OS

FIPS and Common Criteria Configuration Guide

Supporting Network OS v5.0.0 for FIPS and 5.0.1b for Common Criteria

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein or the computer programs that accompany it.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit http://www.brocade.com/support/oscd.

Contents

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names Identifies keywords and operands Identifies the names of user-manipulated GUI elements Identifies text to enter at the GUI
italic text	Identifies emphasis Identifies variables Identifies document titles
`Courier font`	Identifies CLI output Identifies command syntax examples

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
value	In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text, for example, **--show** WWN.

Convention	Description
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options. In Fibre Channel products, square brackets may be used instead for this purpose.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Brocade resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

You can download additional publications supporting your product at www.brocade.com. Select the Brocade Products tab to locate your product, then click the Brocade product name or image to open the individual product page. The user manuals are available in the resources module at the bottom of the page under the Documentation category.

To get up-to-the-minute information on Brocade products and resources, go to MyBrocade. You can register at no cost to obtain a user ID and password.

Release notes are available on MyBrocade under Product Downloads.

White papers, online demonstrations, and data sheets are available through the Brocade website.

Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

Brocade customers

For product support information and the latest information on contacting the Technical Assistance Center, go to http://www.brocade.com/services-support/index.html.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

Online	Telephone	E-mail
Preferred method of contact for non-urgent issues: • My Cases through MyBrocade • Software downloads and licensing tools • Knowledge Base	Required for Sev 1-Critical and Sev 2-High issues: • Continental US: 1-800-752-8061 • Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33) • For areas unable to access toll free number: +1-408-333-6061 • Toll-free numbers are available in many countries.	support@brocade.com Please include: • Problem summary • Serial number • Installation details • Environment description

Brocade OEM customers

If you have purchased Brocade product support from a Brocade OEM/Solution Provider, contact your OEM/Solution Provider for all of your product support needs.

- OEM/Solution Providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/Solution Provider.

- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/Solution Provider.

Document feedback

To send feedback and report errors in the documentation you can use the feedback form posted with the document or you can e-mail the documentation team.

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com.
- By sending your feedback to documentation@brocade.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

About this Document

Supported hardware and software

This document includes information specific to Network OS v5.0.0. The following hardware platforms are supported in this release:

- Brocade VDX 6740, 6740T, and 6740T-1G
- Brocade VDX 8770
  - Brocade VDX 8770-4
  - Brocade VDX 8770-8

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for Network OS v5.0.0, documenting all possible configurations and scenarios is beyond the scope of this document.

To obtain information about an OS version other than Network OS v5.0.0, refer to the documentation specific to that OS version.

Using the Network OS CLI

For complete instructions and support using the Network OS v5.0.0 command line interface (CLI), refer to the Network OS Command Reference.

What's new in this document

This document is updated with Network OS v5.0.0 specific changes. For complete information, refer to the Network OS Release Notes.

FIPS Support

FIPS overview

Federal Information Processing Standards (FIPS) specify the security standards to be satisfied by a cryptographic module utilized in Network OS v5.0.0 to protect sensitive information in the switch. As part of the FIPS 140-2 level 2 compliance, passwords, shared secrets, and the private keys used in SSL, TLS, and system login must be cleared out or *zeroized* .

Before enabling the FIPS-compliant state, a power-on self-test (POST) is executed when the switch is powered on to check for the consistency of the algorithms implemented in the switch. Known-answer tests (KATs) are used to exercise various features of the algorithm, and their results are displayed on the console for your reference. Conditional tests are performed whenever an RSA/ ECDSA key pair is generated. These tests verify the randomness of the deterministic random number generator (DRNG) and non deterministic random-number generator (non-DRNG). They also verify the consistency of RSA keys with regard to signing and verification and encryption and decryption. These conditional tests also verify that the downloaded firmware is signed.

ATTENTION

Once enabled, the FIPS-compliant state cannot be disabled.

This guide also contains instructions on how to configure a Brocade FOS switch to Common Criteria standards. Configuration instructions for Common Criteria and FIPS are mutually exclusive. Please refer to Common Criteria certification on page 25 for details on how configure the Brocade NOS switch to Common Criteria standards.

FIPS compliance can be applied to switches in standalone and fabric cluster mode. To support FIPS compliance, the CA certificate of the Active Directory server’s certificate should be installed on the switch, and FIPS-compliant TLS ciphers for Lightweight Directory Access Protocol (LDAP) should be used.

The Network OS v5.0.0 firmware is signed by means of SHA256 2048-bit keys. Firmware signatures are automatically validated during firmware download.

OpenSSL and OpenSSH has been upgraded to 1.0.1e and 6.2p2 version respectively to support Elliptical Curve based cryptography. Known vulnerabilities till the release time including Heartbleed is patched to OpenSSL 1.0.1e.

Upgrade and downgrade considerations

- Active and standby devices should have a firmware version which is FIPS compliant, otherwise FIPS mode enable operation on the active CP will fail. If standby is downgraded to a lower firmware version, HA is out of sync.
- To support SSH connections after upgrade from 4.0.1 or 4.1.1 to 5.0.0 in FIPS mode, to connect to a switch,
  - You must have a client that signs and verifies host authentication with SHA256 and supports diffie-hellman-group-exchange-sha256.
  - RSA host key size of the server should be a minimum of 2048.
  - Host keys are present after upgrade and clients that support ECC can connect using ECDSA.
- Before upgrading from 4.0.1 to later releases, you must delete the public key if the size is 1024 and replace it with 2048. After upgrade, 1024 key is not used and password is requested.
- When upgrading or downgrading between Network OS v5.0.0 and a firmware version earlier than Network OS v4.1.1, firmware download uses the SHA256 and 2048-bit key for firmware signature validation.

TABLE 1 Upgrade and downgrade support information.

From Release	To Release	FIPS	Non-FIPS
4.0.1	5.0.0	SP 800-131A configurations must be setup before upgrade. Support for Elliptical curve cryptography for SSH	Support for elliptical curve cryptography
4.1.1	5.0.0	Support for Elliptical curve cryptography for SSH	Support for elliptical curve cryptography
5.0.0	4.0.1	After downgrade, switch is not in FIPS mode.	Elliptical curve cryptography is not supported.
5.0.0	4.1.1	Elliptical curve cryptography is not supported.	Elliptical curve cryptography is not supported.

Zeroization functions

Explicit zeroization can be done at the discretion of the security administrator. These functions clear the passwords and the shared secrets. The following table lists the various keys used in the system that will be zeroized in a FIPS-compliant Network OS switch.

TABLE 2 Zeroization behavior

Keys	Zeroization CLI	Description
ECDSA K random value	No command required	Automatically zeroized on session termination.
ECDSA Private host Key	No command required	Automatically zeroized on session termination.
FCSP CHAP secrets	**fips zeroize**	Automatically zeroized on session termination. All the SFTP sessions gets terminated on zeroization.

TABLE 2 Zeroization behavior (Continued)

Keys	Zeroization CLI	Description
LDAP CA certificate	**no certutil ldapca**	The given LDAP certificate file is zeroized and deleted from module.
Passwords	**fips zeroize**	The **fips zeroize** command removes user-defined accounts in addition to default passwords for the root, factory, admin, and user default accounts. Only the admin role has permissions for this command which, in addition to removing user accounts and resetting passwords, performs the complete zeroization of the system, and reboots the switch. Passwords
RADIUS secret	**no radius-server host***host*	The **radius-server host host** command configures the radius server. The **no radius-server host host** command zeroizes the secret and deletes a configured server.
RNG seed key	No command required	/dev/urandom is used as the initial source of seed for RNG. The RNG seed key is zeroized on every random number generation.
RSA host private key	No command required	Automatically zeroized on session termination.
SFTP session keys	No command required	Automatically zeroized on session termination. All SFTP sessions are terminated on zeroization.
SSH DH private keys	No command required	Keys will be zeroized within code before they are released from memory.
SSH host keys	**fips zeroize** It is recommended that this command is executed with the administrator having physical control of the switch, rather than through remote connections.	Zeroized and deletes the existing host. A new RSA host key of size 2048 is generated.
SSH session key	No command required	This key is generated for each SSH session that is established with the host. It automatically zeroizes on session termination. All SSH sessions terminate on zeroization.
SSH EC-DH Private keys	No command required	This key is generated for each SSH session that is established with the host. It automatically zeroizes on session termination. All SSH sessions terminate on zeroization.
TLS authentication key	No command required	Automatically zeroized on session termination.
TLS pre-master secret	No command required	Automatically zeroized on session termination.

TABLE 2 Zeroization behavior (Continued)

Keys	Zeroization CLI	Description
TLS private keys	**fips zeroize** It is recommended that this command is executed with the administrator having physical control of the switch, rather than through remote connections.	Only RSA keys of size 2048 are allowed.
TLS session key	No command required	Automatically zeroized on session termination.

Power-on self-tests

A power-on self-test (POST) is invoked by powering on the switch in the FIPS-compliant state. It does not require any operator intervention. If any KATs fail, the switch goes into a FIPS Error state, which reboots the system to start the test again. If the switch continues to fail the FIPS POST, you will need to return your switch to your switch service provider for repair.

Conditional tests

The conditional tests are for the random number generators and are executed to verify the randomness of the random number generators. The conditional tests are executed each time before using the random number provided by the random number generator.

NOTE
Conditional tests are performed whenever RSA/ECDSA key pair is generated. These tests also verify the consistency of RSA/ECDSA keys with respect to Signing/Verification and Encryption/Decryption.

The results of the POST and conditional tests are recorded in the system log or are displayed on the local console. This action includes logging both passing and failing results.

FIPS-compliant state configuration

By default, the switch comes up in the non-FIPS-compliant state. You can bring up the switch in the FIPS-compliant state by enabling the known-answer tests (KATs) and conditional tests and then rebooting the switch, but you must configure the switch first. The set of prerequisites shown in the following table must be satisfied for the system to enter the FIPS-compliant state.

To be FIPS compliant, the switch must be rebooted. KATs are run on the reboot. If the KATs are successful, the switch enters the FIPS-compliant state. If the KATs fail, then the switch reboots until the KATs succeed. If the switch cannot enter the FIPS-compliant state and continues to reboot, you must return the switch to your switch service provider.

When the switch successfully reboots in the FIPS-compliant state, you must follow the restrictions listed in the following table to be FIPS compliant. The following table lists the Network OS features and their behaviors in the FIPS-compliant and non-FIPS-compliant states.

TABLE 3 FIPS-compliant state restrictions

Features	FIPS-compliant state	Non-FIPS-compliant state
autoupload of FFDC and trace support data	Not supported	Supported (FTP)
Configupload/ download/ supportsave/ firmwaredownload	SCP only	FTP and SCP
HTTP/HTTPS access	Disabled	HTTP and HTTPS
LDAP CA	CA certificate must be available. Cipher suites: AES256-SHA, AES128-SHA, DES-CBC3-SHA	CA certificate is optional.
Outbound SSH and telnet client	Not supported	Supported
RADIUS authentication protocols	PEAP-MSCHAPv2	CHAP, PAP, PEAP-MSCHAPv2
Root account	Disabled	Enabled
Signed firmware download	Mandatory firmware signature validation. Signed with 2048 key and SHA256.	Mandatory firmware signature validation. Signed with 1024/2048 key and SHA1/ SHA256.
SSH algorithms	HMAC-SHA1 (MAC), HMAC-SHA2-256, HMAC-SHA2-512 ECDSA AES128-CBC, AES256-CBC (cipher suites)	No restrictions
SSH public keys	RSA 2048 bits keys ECDSA 256 bits keys	RSA 1024/2048 bits keys, ECDSA 256 bits and DSA 1024 bits key.
TACACS+ authentication	Not supported	CHAP and PAP
Telnet/SSH access	Only SSH (RSA key size of 2048, SHA 256, and ECDSA will only be allowed)	Telnet and SSH
vCenter	Not supported	Supported

NOTE
Although SNMP is not considered to be FIPS compliant, it is not blocked. SNMP is considered to have a plain text interface without any cryptographic content. The few write operations that are supported do not affect the security of the switch. OSPF is considered a plain text interface, and no protection is claimed for protocol data exchange.

Preparing the switch for FIPS restrictions

It is important to prepare the switch for the following restrictions that exist in the FIPS-compliant state:

- The root account and all root-only functions are not available.
- Access to the Boot PROM is not available.
- HTTP, HTTPS, Telnet, and SNMP must be disabled. Once these ports are blocked, you cannot use them to read or write data from and to the switch.
- For USB interfaces, an authorized operator is required to maintain the physical possession (at all times) of the USB token and shall not provide access to unauthorized individuals or entities.

Refer to FIPS-compliant state configuration on page 14 for a complete list of restrictions between the FIPS-compliant and non-FIPS-compliant states.

ATTENTION
You need the admin role permissions to prepare the switch for the FIPS-compliant state.

Preparing a switch for FIPS-compliant state operation removes all critical security parameters from the switch. As a consequence, some parameters needed to operate the switch must be applied after enabling the FIPS-compliant state, including the following parameters:

- IP ACL rules used to block HTTP, HTTPS, and Telnet access
- CA certificates used in LDAP authentication

These parameters must be reconfigured after each zeroization of the switch.

FIPS preparation overview

The following steps summarize the FIPS preparation process.

1. Disable Boot PROM access.
2. *Optional*: Configure an LDAP server for authentication and configure FIPS-compliant ciphers for LDAP.
3. *Optional*: Configure a RADIUS server for authentication and configure FIPS-compliant ciphers for RADIUS.
4. Configure FIPS-compliant ciphers for SSH.
5. Disable root access.
6. Remove configurations of unsupported features vCenter and TACACS+ and disable Dot1x authentication.
7. If any FC-SP authentication policy attributes have been configured, configure all DH-group configuration to group 4.
8. Disable auto-upload.
9. Enable the KATs and the conditional tests.
10. Zeroize and reboot the switch into the FIPS-compliant state.
11. Disable the Telnet server.
12. Configure IP ACLs to block HTTP, HTTPS, and Telnet ports.
13. For authentication by a Microsoft Active Directory server, import and install the LDCAP CA certificate for LDAP authentication.

Enabling the FIPS-compliant state

FIPS mode cannot be disabled once configured. For disabling the FIPS mode, it is recommended that you contact Brocade Technical Support and perform the procedure under qualified guidance.

1. Log in to the switch by using an account with the admin role.
2. To enable in standalone mode, enter the **no vcs enable** command in privileged EXEC mode.

   In VCS mode, use the **vcs** [**rbridge-id** *rbridge-id*] [vcsId ID] [*enable ID*] command to configure the node.
3. Enter the **unhide** command to provide access to hidden commands. To execute this command, you must enter the password **fibranne**.

   This step is necessary to gain access to the **prom-access**, **fips root disable**, **fips selftests**, and **fips zeroize** commands.

   ```
   switch# unhide fips
   Password: *****
   ```

   CAUTION

   Once access to the Boot PROM has been disabled, you cannot re-enable it.

4. Check the status of prom-access by executing these commands.

   ```
   switch# unhide built-in-self-test
   Password: ********
   switch#
   switch# show prom-access
   PROM access Disabled
   ```

   If prom-access is enabled, disable it by running following command, proceed to Step 5 .
5. Enter the **prom-access disable** command to disable access to the Boot PROM.

   ```
   switch# prom-access disable
   You are disabling PROM access. Do you want to continue? [yes/no] (no): yes
   PROM access Disabled
   ```
6. If LDAP will be used for authentication:

   a) Configure FIPS-compliant LDAP ciphers (AES256-SHA, AES128-SHA, DES-CBC3-SHA):

   ```
   switch# cipherset ldap
   LDAP cipher list configured successfully.
   ```

   b) Delete any LDAP DSA or RSA 2048 CA certificate that already exists on the switch:

   ```
   switch# no certutil ldapca
   Do you want to delete LDAP CA certificate? [y/n]:y
   ```

   NOTE
   In the FIPS-compliant state, only RSA 1024 CA certificates are supported. This command deletes all existing LDAP CA certificates on the switch.

   For more details about configuring LDAP and the FIPS-compliant LDAP ciphers, refer to Setting up LDAP for the FIPS-compliant state *on page 23.*
7. If RADIUS will be used for authentication: Configure FIPS-compliant RADIUS ciphers (AES256-SHA, AES128-SHA, DES-CBC3-SHA):

   ```
   switch# cipherset radius
   RADIUS cipher list configured successfully.
   ```
8. Enter the **cipherset ssh** command to configure the FIPS-compliant ciphers for SSH (HMAC-SHA1 (mac), AES128-CBC, AES256-CBC).

   ```
   switch# cipherset ssh
   ssh cipher list configured successfully
   switch# show cipherset
   RADIUS Cipher List : !ECDH:!DH:HIGH:-MD5:!CAMELLIA:!SRP:!PSK:!AESGCM:!TLSv1.2
   ```

```
LDAP Cipher List : !ECDH:!DH:HIGH:-MD5:!CAMELLIA:!SRP:!PSK:!AESGCM
SSH Cipher List : aes128-cbc, aes256-cbc
```

9. Enter the **cipherset ssh sha256** command to configure ssh hash to SHA256.

   Once cipherset ssh sha256 is executed, connection to the switch will be accepted only from clients that support sha256 hash as part of RSA signature in OpenSSH. To allow other clients to connect, enter the **no cipherset ssh sha256** command to configure hash back to default(sha1).

```
switch# cipherset ssh sha256
```

NOTE
For Dual MM chassis, execute the above command both in Active and Standby MMs.

CAUTION
Once you have disabled root account access, you cannot re-enable it. To re-enable root account access, you must return your switch to your service provider.

10Enter the **fips root disable** command and enter **yes** at the subsequent prompt to disable access from the root account.

```
switch# fips root disable
This operation disables root account. Do you want to continue? [yes,NO] yes
Network OS (switch)
switch console login: 2011/09/08-17:28:34, [SEC-1197], 19073,, INFO, switch,
Changed account root.
```

NOTE
The **fips root disable** command was exposed by the **unhide** command in Step 3 . It is normally a hidden command.

11Enter the **show fips** command to confirm the status of fips.

```
switch# show fips

FIPS Selftests: Enabled
Root account: Disabled
```

12Delete the TACACS+ configuration from the switch by using the following commands.

a) Enter the **show running-config tacacs-server** command to list the existing TACACS+ configuration.

b) For each TACACS+ server listed in List item., enter the **no tacacs-server host** command and the IP address or host name to delete the TACACS+ server configuration.

```
switch# show running-config tacacs-server host ?
Description: Configure a TACACS+ Server for AAA
Possible completions:
 10.20.57.13  INETADDRESS;;Domain name or IP Address of this TACACS+ server
 |       Output modifiers
 <cr>
Possible match completions:
 port     TCP Port for Authentication (default=49)
 protocol  Authentication protocol to be used (default=CHAP)
 key    Secret shared with this server (default='sharedsecret')
 retries  Number of retries for this server connection (default=5)
 timeout  Wait time for this server to respond (default=5 sec)
switch# configure terminal
Entering configuration mode terminal
switch(config)# no tacacs-server host 10.10.20.57.13
```

13Enter the **no dot1x enable** command to disable 802.1x globally.

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# no dot1x enable
switch(config)# exit
```

14If vCenter is configured, remove the configuration using the following CLI:

```
switch(config)# no vcenter <name>
```

15. DH group 0-3 is not supported in the fips compliance state of the switch. If DH group 0-3 or '*' is configured, execute the following to configure dh group to 4 (key size 2048 bits).

```
switch(config)# fcsp auth group 4
```

16. Configure DH policy to ACTIVE/ON to make sure DH-CHAP authentication will be initiated on E-Ex port formation by executing the following CLI:

```
switch(config)#fcsp auth policy switch <on/active>
```

17. Configure hash as SHA1 by executing the following command.

```
switch(config)#fcsp auth hash sha1
```

18. If autoupload is enabled, disable it.

```
switch# autoupload disable
```

CAUTION

Once FIPS self-tests are enabled, you cannot disable them. These tests will run on the next reboot and, if successful, will place the switch into the FIPS-compliant state.

19. Enter the **fips selftests** command to enable the FIPS KAT and conditional tests.

    To ensure FIPS-compliance, the Kex algorithm diffie-hellman-group-exchange-sha256 is enforced once the **fips selftests** command is run.

    Clients that support diffie-hellman-group-exchange-sha256 are only able to connect to the switch and switch can upload config and support files only to servers that support diffie-hellman-group-exchange-sha256.

```
switch# fips selftests
self tests enabled
```

NOTE
The **fips selftests** command was exposed by the **unhide** command in Step 3 . It is normally a hidden command.

20. Enter the **fips zeroize** command and enter **yes** at the subsequent prompt to clear all passwords and secrets.

    The switch reboots and comes up in the FIPS-compliant state.

```
switch# fips zeroize
This operation erases all passwords, shared secrets, private keys etc. on the
switch . Do you want to continue? [yes,NO] yes
```

NOTE
The **fips zeroize** command was exposed by the **unhide** command in Step 3 . It is normally a hidden command. When the switch reboots, the FIPS commands will be hidden again. Zeroization should only be performed by a local operator that has physical control of the cryptographic module, with all network connections physically disconnected.

On reboot, the switch performs the KATs and conditional tests enabled in Step 19 . The following sample output indicates successful completion of these tests, after which the switch comes up in the FIPS-compliant state, as shown below:

```
FIPS-mode test application
1. Non-Approved cryptographic operation test...
a. Excluded algorithm (MD5)...successful
b. Included algorithm (D-H)...successful
2. Automatic power-up self test...
2.a. FIPS RNG selftest...successful
2.b. FIPS Rand method set...successful
3. AES-128,192,256 CBC encryption/decryption...successful
4. RSA key generation and encryption/decryption...successful
4.1. RSA 2048 with 'SHA256' testing...successful
5. TDES-CBC encryption/decryption...successful
6a. SHA-1 hash...successful
6b. SHA-256 hash...successful
```

```
6c. SHA-512 hash...successful
6d. HMAC-SHA-1 hash...successful
6e. HMAC-SHA-224 hash...successful
6f. HMAC-SHA-256 hash...successful
6g. HMAC-SHA-384 hash...successful
6h. HMAC-SHA-512 hash...successful
7. Non-Approved cryptographic operation test...
a. Excluded algorithm (MD5)...Not executed
b. Included algorithm (D-H)...successful as expected
8. Zero-ization...Successful
9. TLS 1. 0 KDF...successful
9a. TLS1.2 KDF
10. ECDSA … successful
11. ECDH…. successful
12. SSH KDF …. Successful
All tests completed with 0 errors
```

NOTE
If the output shows errors, the switch reboots. If the errors persist, you must return the switch to your service provider for repair.

21. Use IP ACLs to block the HTTP, HTTPS, Telnet, and Brocade internal ports. Enter the following commands for IPv4 and IPv6.

    a) Enter the **ip access-list extended** command and a name for the IP ACL.
    b) Enter a **seq deny** command to create a rule for blocking the HTTP port (80).
    c) Enter a **seq deny** command to create a rule for blocking the HTTPS port (443).
    d) Enter a **seq deny** command to create a rule for blocking the Telnet port (23).
    e) Enter **seq deny** commands to create rules for blocking the Brocade internal server ports 3016, 4565, 5016, 7013, 7110, 7710, 9013, 9110, 9710, and 9910 through 10110.
    f) If SSH access is required, enter seq permit commands to allow access on ports 22 and 830.
    g) If remote access is required, such as through SCP or LDAP, enter seq permit commands to allow UDP and TCP traffic on ports 1024 through 65535. Enter the **interface management** *rbridge-id/ port* command to enter the interface management subconfiguration mode.
    h) Enter the **ip access-group** command with the ACL name created in List item. to apply the ACL to the management interface.

    These commands also disable the non-FIPS-compliant vCenter feature.

    For IPv4:

```
switch(conf-ip-ext)# seq 1 deny tcp any any eq www
switch(conf-ip-ext)# seq 2 deny tcp any any eq 443

switch(conf-ip-ext)# seq 3 deny tcp any any eq telnet
switch(conf-ip-ext)# seq 4 deny tcp any any eq 2301

switch(conf-ip-ext)# seq 5 deny tcp any any eq 2401
switch(conf-ip-ext)# seq 6 deny tcp any any eq 3016
switch(conf-ip-ext)# seq 7 deny tcp any any eq 3516
switch(conf-ip-ext)# seq 8 deny tcp any any eq 4516
switch(conf-ip-ext)# seq 9 deny tcp any any eq 5016
switch(conf-ip-ext)# seq 10 deny tcp any any eq 7013

switch(conf-ip-ext)# seq 11 deny tcp any any eq 7110

switch(conf-ip-ext)# seq 12 deny tcp any any eq 7710

switch(conf-ip-ext)# seq 13 deny tcp any any eq 9013
switch(conf-ip-ext)# seq 14 deny tcp any any eq 9110

switch(conf-ip-ext)# seq 15 deny tcp any any eq 9710
switch(conf-ip-ext)# seq 16 deny tcp any any range 9910 10110
switch(conf-ip-ext)# seq 17 deny udp any any eq 33351

switch(conf-ip-ext)# seq 18 deny udp any any eq 36851
switch(conf-ip-ext)# seq 19 deny udp any any eq 37731

switch(conf-ip-ext)# seq 20 deny udp any any eq 50690
switch(conf-ip-ext)# seq 21 permit tcp any any range 1024 65535
switch(conf-ip-ext)# seq 22 permit udp any any range 1024 65534
switch(conf-ip-ext)# seq 23 permit udp any any eq 65535
switch(conf-ip-ext)# seq 100 permit tcp any any eq 22
switch(conf-ip-ext)# seq 101 permit tcp any any eq 830
switch(conf-ip-ext)# exit
switch(config)#
```

For IPv6:

```
switch(conf-ip-ext)# seq 1 deny tcp any any eq 80
switch(conf-ip-ext)# seq 2 deny tcp any any eq 443
switch(conf-ip-ext)# seq 3 deny tcp any any eq 23
switch(conf-ip-ext)# seq 4 deny tcp any any eq 2301
switch(conf-ip-ext)# seq 5 deny tcp any any eq 2401
switch(conf-ip-ext)# seq 6 deny tcp any any eq 3016
switch(conf-ip-ext)# seq 7 deny tcp any any eq 3516
switch(conf-ip-ext)# seq 8 deny tcp any any eq 4516
switch(conf-ip-ext)# seq 9 deny tcp any any eq 5016
switch(conf-ip-ext)# seq 10 deny tcp any any eq 7013
switch(conf-ip-ext)# seq 11 deny tcp any any eq 7110
switch(conf-ip-ext)# seq 12 deny tcp any any eq 7710
switch(conf-ip-ext)# seq 13 deny tcp any any eq 9013
switch(conf-ip-ext)# seq 14 deny tcp any any eq 9110
switch(conf-ip-ext)# seq 15 deny tcp any any eq 9710
switch(conf-ip-ext)# seq 16 deny tcp any any range 9910 10110
switch(conf-ip-ext)# seq 17 deny udp any any eq 33351
switch(conf-ip-ext)# seq 18 deny udp any any eq 36851
switch(conf-ip-ext)# seq 19 deny udp any any eq 37731
switch(conf-ip-ext)# seq 20 deny udp any any eq 50690
switch(conf-ip-ext)# seq 21 permit tcp any any range 1024 65535

switch(conf-ip-ext)# seq 22 permit udp any any range 1024 65534
switch(conf-ip-ext)# seq 23 permit udp any any eq 65535
switch(conf-ip-ext)# seq 100 permit tcp any any eq 22
switch(conf-ip-ext)# seq 101 permit tcp any any eq 830
switch(conf-ip-ext)# exit
switch(config)#
```

For inband management IPv4 ports, use the following rules:

```
switch(conf-ip-ext)# seq 5 hard-drop tcp any any eq 80
switch(conf-ip-ext)# seq 10 hard-drop tcp any any eq 443
switch(conf-ip-ext)# seq 15 hard-drop tcp any any eq 23
switch(conf-ip-ext)# seq 20 hard-drop tcp any any eq 2301
switch(conf-ip-ext)# seq 25 hard-drop tcp any any eq 2401
switch(conf-ip-ext)# seq 30 hard-drop tcp any any eq 3016
switch(conf-ip-ext)# seq 35 hard-drop tcp any any eq 3516
switch(conf-ip-ext)# seq 40 hard-drop tcp any any eq 4516
switch(conf-ip-ext)# seq 45 hard-drop tcp any any eq 5016
switch(conf-ip-ext)# seq 50 hard-drop tcp any any eq 7013
switch(conf-ip-ext)# seq 55 hard-drop tcp any any eq 7110
switch(conf-ip-ext)# seq 60 hard-drop tcp any any eq 7710
switch(conf-ip-ext)# seq 65 hard-drop tcp any any eq 9013
switch(conf-ip-ext)# seq 70 hard-drop tcp any any eq 9110
switch(conf-ip-ext)# seq 75 hard-drop tcp any any eq 9710
switch(conf-ip-ext)# seq 80 hard-drop tcp any any range 9910 10110
switch(conf-ip-ext)# seq 85 hard-drop udp any any eq 33351
switch(conf-ip-ext)# seq 90 hard-drop udp any any eq 36851
switch(conf-ip-ext)# seq 95 hard-drop udp any any eq 37731
switch(conf-ip-ext)# seq 100 hard-drop udp any any eq 50690
switch(conf-ip-ext)# seq 105 permit tcp any any range 1024 65535
switch(conf-ip-ext)# seq 110 permit udp any any range 1024 65534
switch(conf-ip-ext)# seq 115 permit udp any any eq 65535
switch(conf-ip-ext)# seq 120 permit tcp any any eq 22
switch(conf-ip-ext)# seq 125 permit tcp any any eq 830
switch(conf-ip-ext)# exit
switch(config)#
```

NOTE

For the switch to remain FIPS compliant, the HTTP, HTTPS, Telnet, and Brocade internal server ports (80, 443, 23, 2301, 2401, 3016, 3516, 4516, 5016, 7013, 7110, 7710, 9013, 9110, 9710, 9910 through 10110, 33351, 36851, 37731, and 50690) must be blocked after every zeroization operation.

22 Disable the Telnet server.

```
switch(config)# telnet server shutdown
switch(config)#
```

23 If RADIUS authentication is required, execute the following CLI in config mode to configure Radius server to use only PEAP-MSCHAPv2. Radius server with PAP and CHAP is not allowed in FIPS compliant state.

```
switch(config)#radius-server host <host> protocol peap-mschapv2
```

24 If LDAP authentication is required, in global configuration mode, enter the following command syntax to import the LDAP CA certificate:

certutil import ldapca directory *ca-certificate-directory* **file** *filename* **protocol** {**FTP** |**SCP** } **host***remote-ip-address***user***user-account***password***password*

NOTE
The CA certificate imported must be RSA2048 with SHA256 encrypted.

25 Specify SCP for the protocol.

```
switch# certutil import ldapca directory /usr/ldapcacert file cacert.pem
        protocol SCP host 10.23.24.56 user jane password ******
```

26 Enter the **copy running-config startup-config** command to save all settings to the startup configuration file.

```
switch# copy running-config startup-config
```

NOTE
After the switch is in the FIPS-compliant state, do not use any non-FIPS-compliant algorithms such as FTP, DHCHAP, MD5. With regards to SCP client on the switch, the remote SCP server must employ RSA host keys with a minimum length of 1024 bits.

Zeroizing for FIPS

1. Log in to the switch using an account with admin role permissions.
2. In privileged EXEC mode, enter the**fips zeroize** command**.**

   The switch reboots automatically. If the KATs and conditional tests are enabled, then the switch will reboot in the FIPS-compliant state. If the tests are not enabled, the switch comes up in the non-FIPS-compliant state.

NOTE
For the switch to remain FIPS compliant, the HTTP, HTTPS, telnet, and Brocade internal server ports (3016, 4565, 5016, 7013, 7110, 7710, 9013, 9110, 9710, and 9910 through 10110 inclusive) must be blocked after every zeroization operation.

NOTE
Passwords of the default accounts (admin and user) must be changed after every zeroization operation to maintain FIPS 140-2 compliance.

LDAP in the FIPS-compliant state

You can configure your Microsoft Active Directory server to use the Lightweight Directory Access Protocol (LDAP) while in the FIPS-compliant state.

The following table lists the differences between the FIPS-compliant and non-FIPS-compliant states of operation.

TABLE 4 FIPS-compliant and non-FIPS-compliant states of operation

FIPS-compliant state	non-FIPS-compliant state
The certificate for the CA that issued the Microsoft Active Directory server certificate must be installed on the switch.	There is no mandatory CA certificate installation on the switch.
Configure FIPS-compliant TLS ciphers [TDES-168, SHA256, and RSA-2048] on the Microsoft Active Directory server. The host needs a reboot for the changes to take effect.	On the Microsoft Active Directory server, there is no configuration of the FIPS-compliant TLS ciphers.
The switch uses FIPS-compliant ciphers regardless of the Microsoft Active Directory server configuration. If the Microsoft Active Directory server is not configured for FIPS ciphers, authentication will still succeed.	The Microsoft Active Directory server certificate is validated if the CA certificate is found on the switch.
The Microsoft Active Directory server certificate is validated by the LDAP client. If the CA certificate is not present on the switch, then user authentication will fail.	If the Microsoft Active Directory server is configured for FIPS ciphers and the switch is in the non-FIPS-compliant state, then user authentication will succeed.

When setting up an LDAP server for FIPS, you will need to perform the following tasks:

- Add a DNS server.
- Configure a Microsoft Active Directory server as the authentication device.
- Import the RSA 2048 LDAP CA certificate from the Microsoft Active Directory server to the switch.

Configuring the DNS server and the Microsoft Active Directory server should be performed before bringing up the switch in the FIPS-compliant state. Any DSA CA certificates must be deleted from the switch.

Setting up LDAP for the FIPS-compliant state

1. Log in to the switch by using an account with admin role permissions.
2. In privileged EXEC mode, enter the **configure terminal** command to enter global configuration mode.
3. Enter the **ip dns domain-name** and **ip dns name-server** commands to configure DNS on the switch.

   Specify the DNS IP address in either IPv4 or IPv6 format. This address is required for the switch to resolve the domain name to the IP address, because LDAP initiates a TCP session to connect to your Microsoft Active Directory server. A Fully Qualified Domain Name (FQDN) is needed to validate the server identity as mentioned in the common name of the server certificate.

```
switch# configure
Entering configuration mode terminal
switch(config)# ip dns domain-name sec.brocade.com
switch(config)# ip dns name-server 10.70.20.1
```

4. Enter the **aaa authentication login ldap** command to set the switch authentication mode for LDAP.

   ```
   switch(config)# aaa authentication login ldap local
   ```

5. Enter the **ldap-server host** command to add your LDAP server. Provide the FQDN of the Microsoft Active Directory server for the host name parameter while configuring LDAP. The maximum supported length for the host name is 40 characters.

   ```
   switch(config)# ldap-server host GEOFF5.ADLDAP.LOCAL basedn sec.brocade.com port
   389 retries 3
   switch(config-ldap-server-GEOFF5.ADLAP.LOCAL)# exit
   switch (config) exit
   switch# show running-config ldap-server host GEOFF5.ADLDAP.LOCAL

   ldap-server host GEOFF5.ADLDAP.LOCAL
    port        389
    domain      security.brocade.com
    retries     3
   !
   ```

6. Enter the **cipherset ldap** command to configure the FIPS-compliant ciphers for LDAP operation.

   ```
   switch# cipherset ldap
   ldap cipher list configured successfully
   ```

7. Set up LDAP according to the instructions in the “External Server Authentication” chapter of the *Network OS Administrator’s Guide* and then perform the following additional Microsoft Active Directory settings.

   a) To support FIPS-compliant TLS cipher suites on the Microsoft Active Directory server, allow the SCHANNEL settings listed in the following table.

   TABLE 5 Active Directory keys to modify

Key	Sub-key
Ciphers	3DES
Hashes	SHA256
Key exchange algorithm	PKCS
Protocols	TLSv1.0, TLSv1.2

   b) Enable the FIPS algorithm policy on the Microsoft Active Directory.

Common Criteria certification

Overview

This chapter contains steps for configuring the Brocade Network OS switch for Common Criteria (CC) standards with version 5.0.1b1 (NDPP -Protection profile for Network Devices) .

Common Criteria certification for a device enforces a set of security standards and feature limitations on a device to be compliant with the Common Criteria standards, similar to placing the device in FIPS mode. To better understand the Common Criteria certification and the associated security functions that have been subject to certification, refer to the*Brocade Communications Systems, Inc. Brocade Switches 5.0.1b1 (NDPP11e3) Security Target* document.

The Network OS device management functions are isolated through authentication. Once administrators log in with specific credentials, their access is limited to commands for which they have privileges and role-based permissions. Additionally, network management communication paths are protected against modification and disclosure using SSHv2.

FIPS 140-2 level2 specifies the security requirements that are satisfied by a cryptographic module utilized within a security system protecting sensitive information of the system.

Brocade Network OS switches running version 5.0.1b1 are designed to support FIPS compliance mode. All cryptographic algorithms required and used in CC are certified by FIPS certifications.

NOTE
To determine if the Network OS device and current software version is Common Criteria certified, see https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm.

Firmware update

Firmware packages are signed using the 2048 bit RSA key with SHA256 during firmware build and verified during firmware installation as specified below.

1. RPM packages are signed with the private key to create a SHA256 digest when the firmware package is generated.
2. Public key is packaged in an RPM package as part of the firmware and is downloaded as the first file.
3. As part of firmware download, each package is validated by verifying the signature.

4. Installation begins after the packages are validated.
5. The switch restarts after the successful installation.

NOTE
If the installation fails, an error with details are displayed and the download procedure is terminated.

The public key file on the switch contains only one public key. It is only able to validate firmware signed using one corresponding private key. If the private key changes in future releases, you must change the public key on the switch by using the **firmware download** command. When a new firmware is downloaded, firmware download always replaces the public key file on the switch with what is in the new firmware. This allows you to have planned firmware key changes.

You can download the signed firmware with its associated MD5 from MyBrocade.

Configuring Common Criteria mode

To configure Brocade Network OS switch for CC compliance mode, execute the following steps.

NOTE
Configuring a Brocade Network OS switch for CC compliance mode using NETCONF operations is not supported. NETCONF interface must be blocked before configuring the CC compliance mode.

1. Login to the switch as admin.
2. Enter **unhide fips** command. Enter password as `fibranne` when prompted.
   ```
   device# unhide fips
   ```
   You will have access to all FIPS commands like **fips zeroize** command.
3. Enter **fips zeroize** command to zeroize all the existing security configurations and parameters.
   ```
   device# fips zeroize
   ```
4. Login as admin and configure the system for crypto compliance.
   a) Enter **cipherset ssh** command to configure SSH Server and Client ciphers and MACs.
   ```
   device# cipherset ssh
   ```
   b) Enter the **cipherset ldap** command to configure TLS ciphers for LDAP authentication.
   ```
   device# cipherset ldap
   ```
   c) Enter the **cipherset radius** command to configure TLS ciphers for RADIUS authentication.
   ```
   device# cipherset radius
   ```
   d) Enter the global configuration mode.
   ```
   device# configure terminal
   ```
   e) Enter the **ssh server key-exchange dh-group-14** command to configure SSH Server key-exchange protocol.
   ```
   device(config)# rbridge-id 1
   device(config-rbridge-id-1)# ssh server key-exchange dh-group-14
   ```
   f) Enter the **ssh client key-exchange dh-group-14** command to configure SSH Client key-exchange protocol.
   ```
   device(config-rbridge-id-1)# ssh client key-exchange  dh-group-14
   ```
   g) Enter the **no ssh server key dsa** command to remove SSH DSA host key.
   ```
   device(config-rbridge-id-1)# no ssh server key dsa
   ```
   h) Enter the **ssh server shutdown** and **no ssh server shutdown** commands to restart the SSH server.
   ```
   device(config-rbridge-id-1)# ssh server shutdown
   device(config-rbridge-id-1)# no ssh server shutdown
   ```
5. Use IP ACLs to block Telnet, HTTP, HTTPS, SNMP, NETCONF, and Brocade internal ports 7110, 7710, 8008, 9110, and 9710 for IPv4 and IPv6. If SSH access is required, enter **seq permit** commands to allow access on port 22. If remote access is required, such as through SCP or LDAP,

enter **seq permit** commands to allow UDP and TCP traffic on ports 1024 through 65535. Configure IP ACLs using **ip access-list** command and use **ip access-group** command to apply the rules to the management interface.

```
device(config)# ip access-list extended ccextACL
device(config-ip-ext)# seq 1 deny tcp any any eq 23
device(config-ip-ext)#seq 2 deny tcp any any eq 80
device(config-ip-ext)#seq 3 deny tcp any any eq 443
device(config-ip-ext)#seq 4 deny tcp any any eq 830
device(config-ip-ext)#seq 5 deny tcp any any eq 7110
device(config-ip-ext)#seq 6 deny tcp any any eq 7710
device(config-ip-ext)#seq 7 deny tcp any any eq 8008
device(config-ip-ext)#seq 8 deny tcp any any eq 9110
device(config-ip-ext)#seq 9 deny tcp any any eq 9710
device(config-ip-ext)#seq 10 deny udp any any eq 161
device(config-ip-ext)#seq 11 permit tcp any any range 1024 65535
device(config-ip-ext)#seq 12 permit udp any any range 1024 65535
device(config-ip-ext)#seq 13 permit tcp any any eq 22
device(config-ip-ext)#exit
device(config)# interface tengigabitethernet 1/0/49
device(conf-if-fo-1/0/49)# ip access-group ccextACL in

device(config)# ipv6 access-list extended ccextACL6
device(config-ip-ext)# seq 1 deny tcp any any eq 23
device(config-ip-ext)#seq 2 deny tcp any any eq 80
device(config-ip-ext)#seq 3 deny tcp any any eq 443
device(config-ip-ext)#seq 4 deny tcp any any eq 830
device(config-ip-ext)#seq 5 deny tcp any any eq 7110
device(config-ip-ext)#seq 6 deny tcp any any eq 7710
device(config-ip-ext)#seq 7 deny tcp any any eq 8008
device(config-ip-ext)#seq 8 deny tcp any any eq 9110
device(config-ip-ext)#seq 9 deny tcp any any eq 9710
device(config-ip-ext)#seq 10 deny udp any any eq 161
device(config-ip-ext)#seq 11 permit tcp any any range 1024 65535
device(config-ip-ext)#seq 12 permit udp any any range 1024 65535
device(config-ip-ext)#seq 13 permit tcp any any eq 22
device(config-ip-ext)#exit
device(config)# interface tengigabitethernet 1/0/49
device(conf-if-fo-1/0/49)# ipv6 access-group ccextACL6 in
```

NOTE
Do not use FTP mode for the operations such as copying startup or running configuration, copy support, and firmware download.

NOTE
Do not configure TACACS+ protocol for authentication.

6. Configure PEAP MS-CHAP for RADIUS authentication, if required.
   a) If RADIUS server is configured for authentication, obfuscate the RADIUS shared secret during configuration.
   b) Enter the **radius-server host** *ip-address* **protocol peap-mschap** [**port** *portnum*] [**key** *shared-key*] [**timeout** *secs*] [**retransmit** *num*] command in global configuration mode to configure RADIUS server.
   ```
   device(config)# radius-server host 10.24.65.6 protocol peap-mschap retransmit 100
   ```
   c) Enter the **aaa authentication login radius local-auth-fallback** command.
   ```
   device(config)# aaa authentication login radius local-auth-fallback
   ```
7. Configure LDAP if required.
   a) Enter the **certutil import ldapca directory** *ca-certificate-directory* **file** *filename* **protocol SCP host** *remote-ip* **user** *user-account* **password** *password* command in privileged EXEC mode to import LDAP CA certificate.
   ```
   device# certutil import ldapca directory /usr/ldapcacert file cacert.pem
   protocol SCP host 10.23.24.56 user admin password *****
   ```

The CA certificate imported must be RSA2048 with SHA1/SHA256 encryption.

b) Enter the **ldap-server host** *ip-address* **basedn** *domain-name* [**port** *portnum*] [**retransmit** *num*] command in global configuration mode to configure the LDAP server.

```
device(config)# ldap-server host padl12r2.la12security.xyz.com basedn
la12security.xyz.com
```

c) Enter the ip dns command to configure the DNS domain and server.

```
device(config)# ip dns domain-name la12security.xyz.com
device(config)# ip dns name-server 10.38.37.183
```

d) Enter the **aaa authentication login ldap local-auth-fallback** command.

```
device(config)# aaa authentication login ldap local-auth-fallback
```

8. Enable secure logging using syslog server.

a) Enter the **certutil import syslogca directory** *ca-certificate-directory* **file** *filename* **protocol SCP host** *remote-ip* **user** *user-account* **password** *password* command in privileged EXEC mode to import the Syslog CA certificate.

```
device# certutil import syslogca directory /usr/ldapcacert/ file cacert.pem
protocol SCP host 10.23.24.56 user admin password
password:
device#
```

The CA certificate imported must be RSA2048 with SHA1/SHA256 encryption.

b) Enter the **logging syslog-server host** *ip-address* command in global configuration mode to configure syslog server.

```
device(config)# logging syslog-server 10.20.238.120  secure port 1999
```

9. Enter the **certutil import sshkey directory** *pubkey-directory* **file** *filename* **protocol SCP host** *remote-ip* **user** *user-account password password* command to import public key.

```
device# certutil import sshkey user admin host 10.70.4.106 directory /users/
home40/bmeenaks/.ssh file id_rsa.pub login fvt
Password: ***********
switch# 2012/11/14-10:28:58, [SEC-3050], 75,, INFO, VDX, Event: sshutil, Status:
success, Info: Imported SSH public key from 10.70.4.106 for user 'admin'.
```

To support passwordless SSH authentication, externally generated RSA key pairs shall only be imported if they are RSA 2048.

10Enter the **telnet server shutdown** command in global configuration mode to disable Telnet server.

```
device(config-rbridge-id-1)# telnet server shutdown
```

11Enter the **copy running-config startup-config** command to save all settings to the startup configuration file.

```
device# copy running-config startup-config
This operation will modify your startup configuration. Do you want to continue?
[Y/N]: Y
```

Self tests

The table provides detailed information about the tests that are executed during the boot up of the switch to confirm the authenticity of the algorithms.

NOTE
During a self test failure, Brocade recommends that you restart the system and test again. If the failure persists, then proceed with the Return Materials Authorization (RMA) request for the device.

Algorithm	Description
TDES	This module implements a KAT for the encrypt and decrypt operations of Triple DES in the CBC mode of operation. The test passes only if the calculated output equals the known output for both operations. The Triple DES KAT must execute successfully before using Triple DES functionality

Algorithm	Description
AES	This module implements a known answer test (KAT) for encrypt/ decrypt operation of AES-128 block size and 256 key size in the CBC mode of operation. The test passes only if the calculated result equals the known result for both encryption/decryption. The AES KAT must execute successfully before accessing AES functionality.
HMAC SHA-1	This module implements the short messages test as part of KAT for SHA-1 and later the HMAC validation testing is done. Short Messages Test-tests the ability to correctly generate message digests for messages of smaller length.
HMAC SHA-256	This module implements the short messages test as part of KAT for SHA-256 and later the HMAC validation testing is done. Short Messages Test-tests the ability to correctly generate message digests for messages of smaller length.
DRNG	This module tests whether the random number generated is deterministic. This test compares a known seed and known output against the random number generated.
RSA sign/verify	This module implements a KAT for signing and verification operation of RSA. The test passes only if the signature is verified. The KAT must execute successfully before the operator can access RSA functionality.
AES GCM	This module implements a KAT for AES encryption and decryption using GCM.
SHA512	This module implements the SHA 512 short message test as of KAT.
HMAC SHA512	This module implements the short messages test as part of KAT for SHA-512 and later the HMAC validation testing is done. Short Messages Test-tests the ability to correctly generate message digests for messages of smaller length.
TLS	Implements the KDF for TLS as per the SP800-131A.
SSH	Implements the KDF for SSH as per the SP800-131A.
EC DSA	Implements the EC DSA pair wise consistency test.
EC DH	Implements the EC DH test.

Processes supported on the network interface

The device running Network OS software is managed through an Ethernet port where the following processes respond to process the network packets. All processes are executed under root privilege.

- Secd: It is the primary process for major security related functionality. It supports the following:
  - Authentication and authorization with LDAP and RADIUS server.
  - Authentication, authorization and accounting with TACACS.
  - Role based access control.
  - Authentication and authorization with the local user database management.
  - ACL through IP filter on the TCP/UDP connections.
- Authd: It is the process that supports authentication by DH-CHAP.

- TCP/IP stack: Network OS IP stack from kernel that accepts all packets from network interface and apply IP filter rules as configured.
- Syslog-ng: It is the process that supports logging of audit messages through TLS tunnel on a remote server.
- SSHd: It is the process available on port 22 that provides a terminal session after authentication using the SSH protocol.
- Telnetd: It is the process available on port 23 that provides a terminal session after authentication.

Cryptographic Configurations in Common Criteria

The Network OS device in Common Criteria mode supports the following cryptographic configurations.

TLS

- TLSv1.0, TLSv1.1, and TLSv1.2 protocol version for TLS communication are supported.
- TLS v1.2 is not supported on RADIUS.
- The AES-128 and AES-256 encryption algorithm (with SHA1 and SHA256 as MAC) are supported.
- RSA is used for authentication.
- DES-based cipher suites are not supported.

SSH

The following algorithm are supported:

- Host authentication - ssh-rsa, and ecdsa-sha2-nistp256.
- Ciphers - aes128-cbc and aes256-cbc.
- Keyed-Hash Message Authentication code (HMAC)- hmac-sha1 and hmac-sha2-256
- Key exchange- diffie-hellman-group14-sha1.

Commands supported in Common Criteria

The following commands are provided for administration purpose:

Privileged EXEC mode commands:

- **unhide fips**
- **fips zeroize**
- **cipherset**
- **certutil**
- **copy**

Global configuration mode commands:

- **ip access-list**
- **ip access-group**
- **ldap-server**
- **radius-server**

RBridge configuration mode commands:

- **ssh server key-exchange**
- **ssh client key-exchange**