BROCADE

CONFIGURATION GUIDE

Network OS FIPS

Supporting Network OS v6.0.2

53-1003993-01
31 December 2015

Contents

Copyright Statement

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.
[ ]	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.

Convention	Description
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 6.0.2. The following hardware platforms are supported in this release:

- Brocade VDX6940-24Q, VDX 6940-36Q, Brocade VDX6940-64S, VDX6940-96S, and VDX 6940-144S
- Brocade VDX 8770
  - Brocade VDX 8770-4
  - Brocade VDX 8770-8
- Brocade VDX 6740, 6740T, and 6740T-1G

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for Network OS 6.0.2, documenting all possible configurations and scenarios is beyond the scope of this document.

To obtain information about an OS version other than Network OS 6.0.2, refer to the documentation specific to that OS version.

What's new in this document

This document is updated with changes specific to Network OS 6.0.2. 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 6.0.2 to protect sensitive information in the switch.

As part of the FIPS 140-2 Security Level 2 compliance,

1. Passwords, shared secrets, and the private keys used in SSL, TLS, and system login must be *zeroized*.
2. Power-up self tests are executed when the switch is powered on or re-booted to check for the consistency of the algorithms implemented in the switch.

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.

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

The Network OS 6.0.2 firmware is signed by means of a RSA 2048-bit SHA-256 Signature. Firmware signatures are automatically validated during firmware download.

OpenSSL and OpenSSH have been updated to resolve known vulnerabilities.

SP 800-131A support

NOS 6.0.2 adheres to SP 800-131A standard for FIPS certification.

1. Digital Signature (generation and verification) should be signed with key size >=2048 and hash >= SHA256.
2. SHA1 can be used as HMAC.

The table below shows the algorithm key sizes and hash sizes supported.

TABLE 1 Algorithm and hash sizes supported

Protocol	FIPS mode (NOS 6.0.2)
DH CHAP	Group 4 (2048 bits) and SHA1 hash
LDAP (TLS client)	1. The LDAP protocol supports TLS 1.0/1.1 and TLS 1.2. Ciphers are configured for !ECDH:!DH:HIGH:-MD5:!CAMELLIA:!SRP:!PSK:!AESGCM :!SSLv3 2. CA certificate is a must and should be generated with 2048 keys and signed with SHA256 3. Certificates generated with 1024/2048 and signed with SHA1 can be imported only for downgrade purpose
RADIUS (TLS client)	1. The RADIUS protocol supports TLS 1.0/1.1 and TLS 1.2. Ciphers are configured for !ECDH:!DH:HIGH:-MD5:!CAMELLIA:!SRP:!PSK:!AESGCM:! SSLv3
SSH in Server mode	The following parameters are configurable. 1. Kex algorithm should be ECDH-SHA2-NISTP256, ECDH-SHA2-NISTP384, ECDH-SHA2-NISTP521, Diffie-Hellman-group-exchange-SHA256 2. Ciphers should be AES128-CBC, AES256-CBC 3. MACs should be HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-512 4. SHA Value should be 2, which is SHA256
Firmware download	Firmware signed with SHA256 and RSA2048 key is supported

The table below lists the ciphers supported by TLS 1.0 and TLS 1.2 protocols.

TABLE 2 Ciphers supported by TLS 1.0 and TLS 1.2 protocols

Protocol	FIPS mode (NOS 6.0.2)
TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA

Upgrade and downgrade considerations

You can upgrade or downgrade the devices in the FIPS mode as well. In the FIPS mode, you must ensure the following.

- Active and standby devices must have a firmware version which is FIPS-compliant, otherwise, the FIPS mode enable operation on the active CP will fail. If the standby device is downgraded to a lower firmware version, High Availability (HA) will be out of sync.
- To support SSH connections after upgrading from Network OS 5.0.1 to Network OS 6.0.2 in FIPS mode, you must adhere to the following guidelines to connect a switch.
  - You must have a client that signs and verifies host authentication with SHA-256 and supports Diffie-Hellman-group-exchange-SHA256 (OpenSSH 5.4 and above).

NOTE
Support to sign/verify with SHA256 for host authentication for SSH will be deprecated from next FIPS approved NOS release.

  - The RSA host key size of the server must be a minimum of 2048 bits.
  - Host keys are present after upgrading and clients that support ECC can connect using ECDSA.
- Before upgrading from Network OS 5.0.1 to later releases, you must delete the public key if the size is 1024 bits and replace it with 2048-bit key. After the upgrade, 1024-bit key is not used and a password is requested.
- When upgrading or downgrading between Network OS v6.0.2 and a firmware version earlier than Network OS v5.0.1, firmware download uses the SHA-256 and 2048-bit key for firmware signature validation.

TABLE 3 Upgrade and downgrade support information

From Release	To Release	FIPS	Non-FIPS
5.0.1	6.0.2	RADIUS and LDAP ciphers will support both TLSv1.0 and TLSv1.2	RADIUS and LDAP ciphers will support both TLSv1.0 and TLSv1.2

NOTE
Firmware Downgrade from NOS 6.0.2 to NOS 5.0.1 is not supported in FIPS Mode.

Zeroization functions

Explicit zeroization can be done at the discretion of the security administrator. The zeroization 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 4 Zeroization behavior

Keys	Zeroization CLI	Description
SSHv2 and SCP Protocol Keys		
DH Private Keys (256 bits) for use with 2048 bit modulus	Session termination and **fips zeroize** command	Used in DHCHAP, and SSHv2 to establish a shared secret.
SSHv2/SCP/SFTP Session Keys - 128 and 256 bit AES CBC	Session termination or **fips zeroize** command	AES encryption key used to secure SSHv2/SCP/SFTP sessions
SSHv2/SCP/SFTP Authentication Key	Session termination or **fips zeroize** command	Session authentication key used to authenticate and provide integrity of SSHv2 session (HMAC-SHA-1,HMAC-SHA-256, HMA-SHA-512)
SSHv2 KDF Internal State	Session termination or **fips zeroize** command	Used to generate Host encryption and authentication key
SSHv2 DH Shared Secret Key (2048 bits)	Session termination or **fips zeroize** command	Shared secret from the DH Key agreement primitive - (K) and (H). Used in SSHv2 KDF to derive (client and server) session keys
SSHv2 ECDSA Host Private Key (P-256)	**fips zeroize** command	Used to authenticate SSHv2 server to client
Value of K during SSHv2 256 ECDSA session	Session termination or **fips zeroize** command	ECDSA K Value
SSHv2 ECDH Shared Secret Key (P-256, P-384 and P-521)	Session termination or **fips zeroize** command	Shared secret from the ECDH Key Agreement primitive. Used in SSHv2 KDF to derive (client and server) session keys
SSHv2 ECDH Shared Private Key (P-256, P-384 and P-521)	Session termination or **fips zeroize** command	Private key from the ECDH Key Agreement primitive. Used in SSHv2 KDF to derive (client and server) session keys
SSHv2 RSA 2048 bit Host Private Key	**fips zeroize** command	Used to authenticate SSHv2 server to client
TLS Protocol Keys		

TABLE 4 Zeroization behavior (continued)

Keys	Zeroization CLI	Description
TLS pre-master secret	Session termination or **fips zeroize** command	Secret value used to establish the Session and Authentication key
TLS Master Secret	Session termination or **fips zeroize** command	48 bytes secret value used to establish the Session and Authentication key
TLS KDF Internal State	Session termination or **fips zeroize** command	Values of the TLS KDF internal state
TLS Session Keys 128, 256 bit AES CBC, TDES 3 key CBC	Session termination or **fips zeroize** command	TDES or AES key used to secure TLS sessions
TLS Authentication Key for HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384	Session termination or **fips zeroize** command	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 key used to provide data authentication for TLS sessions
DRBG CSPs		
DRBG Seed	**fips zeroize** command	Seeding material for the SP800-90A DRBG (CTR_DRBG AES-256)
DRBG Value V	**fips zeroize** command	Internal State of SP800-90A DRBG (CTR_DRBG AES-256)
DRBG Key	**fips zeroize** command	Internal State of SP800-90A DRBG (CTR_DRBG AES-256)
DRBG Internal State	**fips zeroize** command	Internal State of SP800-90A DRBG (CTR_DRBG AES-256)
Operator Authentication/Passwords		
Passwords	**fips zeroize** command	Password used to authenticate operators (8 to 40 characters)
RADIUS Secret	**fips zeroize** command	Used to authenticate the RADIUS Server (8 to 40 characters)
NTP Password	**fips zeroize** command	Used to authenticate the NTP client with the server (0-15 characters)

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 and verification, and encryption and decryption.

The results of the POST and conditional tests are recorded in the system log or displayed on the local console including 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 restrictions 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.

The following table lists the Network OS features and their behaviors in the FIPS-compliant and non-FIPS-compliant states.

TABLE 5 FIPS-compliant state restrictions

Features	FIPS-compliant state	Non-FIPS-compliant state
Auto-upload of FFDC and trace support data	Not supported	Supported (FTP)
configUpload, configDownload, supportSave, and firmwareDownload	SCP only	FTP and SCP
Fibre Channel Data	Not supported	Supported
HTTP and HTTPS access	Disabled	HTTP and HTTPS
LDAP CA	CA certificate must be available. Cipher suites: AES256-SHA256 AES256-SHA DES-CBC3-SHA AES128-SHA256 AES128-SHA	CA certificate is optional.
NTP	SHA1	MD5 and SHA1
OSPFv3	Supported as plain text	Not supported
Outbound SSH and Telnet (client)	Not supported	Supported
RADIUS authentication protocols	PEAP-MSCHAPv2 Cipher suites: AES256-SHA256 AES256-SHA DES-CBC3-SHA AES128-SHA256 AES128-SHA	CHAP, PAP, PEAP-MSCHAPv2
Root account	Disabled	Enabled
SCPUser (SCP of config files from/to switch)	Not supported	Supported
Signed firmware download	Mandatory firmware signature validation. Signed with 2048 key and SHA-256.	Mandatory firmware signature validation. Signed with 2048 key and SHA-256.
SNMPv3	Not supported	Read and write operations
SSH algorithms	HMAC-SHA1 (MAC), HMAC-SHA2-256, HMAC-SHA2-512 ECDSA AES128-CBC, AES256-CBC (cipher suites)	No restrictions

TABLE 5 FIPS-compliant state restrictions (continued)

Features	FIPS-compliant state	Non-FIPS-compliant state
SSH public keys	RSA 2048-bit keys ECDSA 256-bit keys	RSA 1024- or 2048-bit keys, ECDSA 256-bit and DSA 1024-bit key.
Syslog-ng	Cipher suites: AES256-SHA256 AES256-SHA DES-CBC3-SHA AES128-SHA256 AES128-SHA	
TACACS+ authentication	Not supported	CHAP and PAP
Telnet/SSH access	SSH (RSA key size of 2048, SHA-256) and SSH with ECDSA pCurve_SHA256 supported	Telnet and SSH
vCenter	Not supported	Supported

Preparing the switch for FIPS restrictions

You must prepare the switch for the following FIPS-compliant state restrictions:

- The root account and all root-only functions are not available.
- Access to the Boot PROM is not available.
- HTTP, HTTPS, Telnet, and SNMP ports 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, only an authorized operator is required to maintain the physical possession (at all times) of the USB token and must not provide access to unauthorized individuals or entities.

Refer to FIPS-compliant state configuration on page 17 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 (CSPs) 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, SNMP, 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. Enable the KATs and the conditional tests.
2. Zeroize and reboot the switch into the FIPS-compliant state.

3. Disable Boot PROM access.
4. (Optional) Configure an LDAP server for authentication and configure FIPS-compliant ciphers for LDAP.
5. (Optional) Configure a RADIUS server for authentication and configure FIPS-compliant ciphers for RADIUS.
6. Configure FIPS-compliant ciphers for SSH.
7. Remove configurations of unsupported features vCenter and TACACS+ and disable Dot1x authentication.
8. If any FC-SP authentication policy attributes have been configured, configure all DH-group configuration to group 4.
9. Disable auto-upload.
10. For VDX 6740, 6740T, and 6740T-1G, disable ag mode.
11. Disable the Telnet server.
12. Configure IP ACLs to block HTTP, HTTPS, SNMP, and Telnet ports.
13. For authentication by a Microsoft Active Directory server, import and install the LDAP CA certificate for LDAP authentication.

Enabling the FIPS-compliant state

The cryptographic module may be configured for FIPS 140-2 mode via execution of the following procedures:

CAUTION
FIPS mode cannot be disabled once configured.

1. Crypto-Officer must Apply tamper labels as specified in Security policy Appendix A
2. Log in to the switch as Crypto-Officer.
3. Enable **fips selftests** using the following commands.

```
sw0#unhide fips
sw0#fips selftests
```

4. Enter the **fips zeroize** command to zeroize all the existing security configurations and parameters.

```
sw0#fips zeroize
```

5. After the module successfully reboots and performs all Power-Up Self-tests successfully, login as Crypto-Officer to configure the system into a FIPS 140-2 Approved mode of Operation.
6. Enter the **cipherset ldap** command to configure TLS ciphers for LDAP authentication.

```
sw0#cipherset ldap
```

7. Enter the **cipherset radius** command to configure TLS ciphers for RADIUS authentication.

```
sw0#cipherset radius
```

8. Enter the **cipherset ssh sha256** command to configure SHA2 hash value for SSH server.

```
sw0#cipherset ssh sha256
```

9. Enter the local **rbridge-id** specific configuration mode.

```
sw0(config)# rbridge-id-1
```

10. Enter the **ssh server key-exchange** command to configure SSH server key exchange protocol.

```
sw0(config-rbridge-id-1)# ssh server key-exchange ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-
nistp521,diffie-hellman-group-exchange-sha256
```

11. Enter the **ssh client key-exchange** command to configure SSH client key exchange protocol.

```
sw0(config-rbridge-id-1)# ssh client key-exchange ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-
nistp521,diffie-hellman-group-exchange-sha256
```

12. Enter the **ssh server cipher** command to configure SSH server ciphers.

```
sw0(config-rbridge-id-1)# ssh server cipher aes128-cbc,aes256-cbc
```

13. Enter the **ssh client cipher** command to configure SSH client ciphers.

```
sw0(config-rbridge-id-1)# ssh client cipher aes128-cbc,aes256-cbc
```

14. Enter the **ssh server mac** command to configure SSH server MACs.

```
sw0(config-rbridge-id-1)# ssh server mac hmac-sha1,hmac-sha2-256,hmac-sha2-512
```

15. Enter the **ssh client mac** command to configure SSH client MACs.

```
sw0(config-rbridge-id-1)# ssh client mac hmac-sha1,hmac-sha2-256,hmac-sha2-512
```

16. Enter the following commands to restart the SSH server, for the configured algorithms to take effect.

```
sw0(config-rbridge-id-1)# ssh server shutdown
sw0(config-rbridge-id-1)# no ssh server shutdown
```

17. Use IP ACLs to block Telnet, HTTP, HTTPS, SNMP, 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 <User defined name (i.e.FIPS-ACL4)>
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 7110
device(config-ip-ext)#seq 5 deny tcp any any eq 7710
device(config-ip-ext)#seq 6 deny tcp any any eq 8008
device(config-ip-ext)#seq 7 deny tcp any any eq 9110
device(config-ip-ext)#seq 8 deny tcp any any eq 9710
device(config-ip-ext)#seq 9 deny udp any any eq 161
device(config-ip-ext)#seq 10 permit udp any any eq 123
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)#seq 14 permit tcp any any eq 830

device(config-ip-ext)#exit
device(config)# interface Management  <ID for Management Interface (i.e. 1/0)>
device(conf-if-fo-1/0/49)# ip access-group <User defined name (i.e.FIPS-ACL4)> in

device(config)# ipv6 access-list extended <User defined name (i.e.FIPS-ACL6)>
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 7110
device(config-ip-ext)#seq 5 deny tcp any any eq 7710
device(config-ip-ext)#seq 6 deny tcp any any eq 8008
device(config-ip-ext)#seq 7 deny tcp any any eq 9110
device(config-ip-ext)#seq 8 deny tcp any any eq 9710
device(config-ip-ext)#seq 9 deny udp any any eq 161
device(config-ip-ext)#seq 10 permit udp any any eq 123
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)#seq 14 permit tcp any any eq 830

device(config-ip-ext)#exit
device(config)# interface Management  <ID for Management Interface (i.e. 1/0)>
device(conf-if-fo-1/0/49)# ipv6 access-group <User defined name (i.e.FIPS-ACL6)>  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.

18. Enter the following command to remove any TACACS+ server configuration.

```
sw0(config)# no tacacs-server <host>
```

19. Depending on the desired aaa Authentication method, perform one of the steps below:
    - Do not configure RADIUS or LDAP authentication; this will result in local authentication by default.
    - Configure PEAP MS-CHAP V2 for RADIUS authentication:

    a) 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 the RADIUS server.

    ```
    device(config)# radius-server host 10.24.65.6 protocol peap-mschap
    ```

    b) Enter the **aaa authentication login radius local-auth-fallback** command.

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

    - Configure LDAP authentication:

    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 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
    ```

20. If required to set up a syslog server, follow the steps below to enable secure logging:

    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 Syslog CA certificate.

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

    The CA certificate imported must be RSA2048 with SHA256 encryption.

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

21. Enter the **certutil import sshkey directory** *pubkey-directory* **file** *filename* **protocol SCP host** *remote-ip* **login** *login-id* **password** *password* **user** user-account command in privileged EXEC mode to import SSH public key, if required:

    ```
    device# certutil import sshkey directory /usr/sshkeys file id_rsa.pub protocol SCP host 10.23.24.56
    user admin login remoteuser password *****.
    ```

    To support password-less SSH authentication, externally generated RSA key pairs must be RSA2048 only.

22. Configure ntp server using commands in global configuration mode, if required:
    a) Enter the **ntp authentication key** *key-id* **sha1** *key-string* to configure NTP authentication key of type SHA1.

```
device(config)# ntp authentication key 1 sha1 ntpsecret
```

    b) Enter the **ntp server** *ip-address* **key** *key-id* **secure** command to configure the Syslog server.

```
device(config)# ntp server 10.20.8.1 key 1
```

23. Configure VDX 6740, 6740T, and 6740T-1G to disable AG mode using the following command in local rbridge-id specific configuration mode.

```
device(config-rbridge-id-1)# ag
device(config-rbridge-id-1-ag)# no enable
```

24. Vcenter, dot1x(802.1x) and OSPF features are not FIPS compliant.
    a) If dot1x is enabled, execute the following command to disable 802.1x globally.

```
switch(config)# no dot1x enable
```

    b) If vCenter is configured, remove the configuration using the following command.

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

25. Execute the following command to disable all the trap ports.

```
switch(config)# no snmp-server enable trap
```

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

```
sw0#username admin password <enter password> role admin
sw0#username user password <enter password> role user
```

27. Disable telnet service with the following command.

```
sw0(config-rbridge-id-1)#telnet server shutdown
```

28. Disable boot prom access using the following commands.

```
sw0#unhide fips
sw0#prom-access disable
```

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

```
sw0#copy running-config startup-config
```

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.

Appendix: SP800-90A DRBG Implementation

DRBG support information

Here is some additional information about the DRBG support implementation in Network OS 6.0.2.

1. There are no interfaces for external users to collect the DRBG generated by the crypto module. Applications that run as part of crypto module request and obtain the DRBG generated through library API calls. All the DRBG functions required for SP800-90A are invoked to generate and test the random bytes before providing it to the application.
2. Design of the implementation mandates validating every bit of the random value generated during the generation and timely re-seeding. Implementation also handles the un-instantiation to ensure that the residual values are not used for seeding.

   The implementation includes Health testing during all stages of DRBG generation: instantiate, seed, generate, reseed and un-instantiate.
3. The implementation utilizes CTR based DRBG mechanism with AES 256 cryptographic primitive for the generation of random numbers.
4. The implementation uses multiple entropy input sources to ensure that the entropy pool is full for generation of random bytes. In addition, the implementation always employs /dev/random to ensure the security strength of the entropy bits.
5. The implementation employs CTR-based DRBG mechanism with AES-256 cryptographic primitive with additional features to ensure stronger DRBG. Features included are predication resistance, additional input and personalization string.
6. DRBG mechanism functions are distributed in the implementation and hence no mechanisms are required to protect confidentiality and Integrity of the internal state.
7. The implementation uses CTR-based DRBG mechanism with derivation function.
8. In addition to the health test listed in SP800-90A, continuous random number generation tests are run on the bytes that are generated.
9. The DRBG health tests are run at an interval of every (1<<24) iterations of DRBG generation, which ensures that even the larger requirement for random numbers are validated.

   DRBG health tests are instantiated, seeded and generated for every requirement to generate the random number.
10. The DRBG functions can be tested in the implementation by power-cycle of the switch, key generation or any request for random numbers.
11. The SP800-90A DRBG implementation is part of the library whose installation is controlled within Brocade and can be downloaded on the crypto-module only through RSA 2048 and SHA256 verification.