CONFIGURATION GUIDE

Extreme Network OS FIPS Configuration Guide

Supporting Network OS v7.3.0aa

9035611
December 2018

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks

Software Licensing

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: www.extremenetworks.com/support/policies/software-licensing

Contents

Preface

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks® publications.

Conventions

This section discusses the conventions used in this guide.

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.

Text formatting conventions

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

Format	Description
bold text	Identifies command names.
	Identifies keywords and operands.
	Identifies the names of GUI elements.
	Identifies text to enter in the GUI.
italic text	Identifies emphasis.
	Identifies variables.
	Identifies document titles.

Format	Description
`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.
[ ]	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.
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.

Documentation and Training

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
The Hub	A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
Call GTAC	For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form with your information (all fields are required).
3. Select the products for which you would like to receive notifications.

   NOTE
   You can modify your product selections or unsubscribe at any time.

4. Click **Submit**.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please 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

In those instances in which procedures or parts of procedures documented here apply to some devices but not to others, this guide identifies exactly which devices are supported and which are not.

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

The following hardware platforms are supported by this release of Network OS:

- ExtremeSwitching VDX 6740-48
- ExtremeSwitching VDX 6740T
  - ExtremeSwitching VDX 6740T-64
  - ExtremeSwitching VDX 6740T-1G
- ExtremeSwitching VDX 6940-144S
- ExtremeSwitching VDX 6940-36Q
- ExtremeSwitching VDX 8770
  - ExtremeSwitching VDX 8770-4
  - ExtremeSwitching VDX 8770-8

To obtain information about a Network OS version other than this release, refer to the documentation specific to that version.

Using the Network OS CLI

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

What's new in this document

This document is updated with changes specific to Network OS 7.3.0aa. For complete information, refer to the Network OS Release Notes.

The new features for this release are:

- Keychain Management
- FIPS 140-2 Level 1 compliance
- x.509v3 digital certificate-based SSH authentication support
- SSH rekey based on time and traffic volume
- SSH authentication retry configuration

- SSH authentication timeout configuration
- OSPFv2/V3 Authentication Changes

FIPS Support

FIPS overview

Federal Information Processing Standards (FIPS) specify the security standards to be satisfied by a cryptographic module utilized in Network OS 7.3.0aa to protect sensitive information in the switch.

As part of the FIPS 140-2 Security Level 1 compliance,

1. Passwords, shared secrets, and the private keys used in 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 for pairwise consistency are performed whenever an RSA/ ECDSA key pair is generated. Other conditional 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. The firmware integrity test verifies 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 server's certificate must be installed on the switch.

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

SP 800-131A support

Network OS 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.
3. All the algorithms must require security strength of at least 112 bits.

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

TABLE 1 Algorithm and hash sizes supported

Protocol	FIPS mode
LDAP and Syslog	CA certificate should be generated with RSA-2048 and signed with SHA256 and must be installed on the device.
SSH in Server mode	The following parameters are configurable. 1. Key algorithm should be Diffie-Hellman-group-exchange-SHA256 or Diffie-Hellman-group14-sha1 2. MACs should be HMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-512
Firmware download	Firmware signed with SHA256 and RSA2048 key is supported

The table below lists the ciphers supported by TLSv1.1 and TLSv1.2 protocols. Other versions of SSL or TLS protocols are not supported.

TABLE 2 TLS protocols

Protocol	FIPS mode
TLSv1.1	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA
TLSv1.2	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256

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 previous versions of Network OS 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).
  - The RSA host key size of the server must be a minimum of 2048 bits.
- Before upgrading from previous releases, you must delete the SSH public keys installed for public-key authentication 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 the current firmware version 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.

Upgrading/Downgrading FROM firmware	Upgrading/Downgrading TO firmware		
	5.0.1	6.0.2	7.3.0aa
5.0.1	n/a	Yes	No
6.0.2	Yes	n/a	Yes
7.3.0aa	No	Yes	n/a

TABLE 3 Upgrade and downgrade support information

FIPS	Non-FIPS
LDAP and Syslog ciphers will support both TLSv1.1 and TLSv1.2	LDAP ciphers will support both TLSv1.1 and TLSv1.2

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 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		
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

TABLE 4 Zeroization behavior (continued)

Keys	Zeroization CLI	Description
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 (1-15 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 executed in two places within the random number generation engine:

1. raw entropy generation or non-deterministic Random Number Generator (NDRNG)
2. o/p of Deterministic RNG (DRBG)

In this test, each time new data is generated, it is compared with the previous value. If the values are same, then the new data is discarded and another new data is generated and compared.

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.

Self-tests

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

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

Algorithm	Description
AES	This module implements a known answer test (KAT) for encrypt and decrypt operation of AES-128 block size in the CBC mode of operation. The test passes only if the calculated result equals the known result for both encryption and decryption. The AES KAT must execute successfully before accessing the AES functionality.
HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	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.
DRBG	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 the RSA functionality.
SHA-512	This module implements the SHA-512 short message test as part of KAT.
TLS	Implements the KDF for TLS as per the SP800-131A.
SSH	Implements the KDF for SSH as per the SP800-131A.
ECDSA	Implements the ECDSA pair-wise consistency test.
ECDH	Implements the ECDH test.

Pairwise Consistency

In this test, after a RSA or ECDSA key pair is generated while executing the command **ssh server key rsa|ecdsa**..", the module will verify the consistency of the keypair by encrypting a known plaintext string with the private key and then decrypting that data with the public key, which is what happens when they are actually used. The decrypted string should match the original plaintext string. Thus, the generated keypair are consistent; otherwise, the test is considered to fail and a new keypair is generated.

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
HTTP access	Disabled	Supported
HTTP and HTTPS access	HTTPS in server mode is allowed in FIPS mode as it uses TLS TLS cipher suites for server: TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA	Supported
LDAP and Syslog CA	CA certificate must be available. TLS cipher suites for client: TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA	CA certificate is optional.
NTP	SHA1	MD5 and SHA1
OSPFv3 and OSPFv2	Supported as HMAC-SHA1, HMAC SHA-256,HMAC-SHA384 and HMAC-SHA512	Supported
Outbound SSH	Supported	Supported
Telnet (client)	Disabled	Disabled
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	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
SSH public keys	RSA 2048-bit keys ECDSA P256 curve	RSA 1024- or 2048-bit keys, ECDSA 256-bit and DSA 1024-bit key.
TACACS+ authentication	Not supported	CHAP and PAP
RADIUS authentication	Not supported	CHAP, PAP, and PEAP
Telnet	Not supported	Supported
SSH	SSH (RSA key size of 2048, SHA-256) SSH with ECDSA P-256 with SHA-256	Supported
vCenter	Not supported	Supported

Configuring the switch in FIPS mode

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, Telnet, and SNMPv1 and SNMPv2 ports must be disabled. (SNMPv3 is allowed.) 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 15 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 and Telnet access
- CA certificates used in LDAP and SYSLOG 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 (including pairwise consistency 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 Syslog server for audit purposes.
6. Configure FIPS-compliant ciphers for SSH.
7. Remove configurations of unsupported features vCenter and TACACS+ and disable Dot1x authentication.
8. Disable auto-upload.
9. Specify the SSH server.
   a) Enter the **ssh server key-exchange** command to configure the SSH Server key-exchange protocol.

```
device(config)# rbridge-id 1
device(config-rbridge-id-1)# ssh server key-exchange diffie-hellman-group-14-sha1
```

   b) Enter the **no ssh server key dsa** command to remove the SSH DSA host key.

```
device(config-rbridge-id-1)# no ssh server key ds
```

   c) Enter the **ssh server cipher** command to configure the SSH server cipher.

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

10. For VDX 6740, 6740T, and 6740T-1G, disable ag mode.
11. Disable the Telnet server.
12. Configure IP ACLs to block HTTP and Telnet ports.
13. For authentication by a Microsoft Active Directory server, import the LDAP CA certificate for LDAP authentication.
14. To support TLS for Syslog, import the CA certificate of the Syslog server.

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. Log into the switch as an admin.
2. Enable the **unhide fips** command to unhide FIPS-specific commands.

```
device#unhide fips
```

3. Enter the **fips selfttests** command to move the crypto module to FIPS mode.

   NOTE
   This command cannot be undone.

```
device#fips selftests
```

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

```
device#fips zeroize
```

   This command will reboot the switch.

5. After the module successfully reboots and performs all Power-Up Self-tests successfully, login as an administrator to disable the boot prom.

```
device#prom-access disable
```

6. Enter the **cipherset ldap** command to configure TLS ciphers for LDAP authentication.

```
device#cipherset ldap
```

7. Enter global configuration mode.

```
device#configure terminal
```

8. Enable strict password checking by issuing the following commands. Password policies are described in the section "User Accounts and Passwords" of the *Network OS Security Configuration Guide*.

```
device(config)# password-attributes max-retry 4
device(config)# password-attributes max-lockout-duration 5000
device(config)# password-attributes character-restriction upper 1
device(config)# password-attributes character-restriction lower 2
device(config)# password-attributes character-restriction numeric 1
device(config)# password-attributes character-restriction special-char 1
```

   The command above requires the user to provide a strong password.

9. Use IP ACLs to block Telnet, HTTP, and Extreme Networks 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 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 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 1/0
device(config-Management-1/0)# 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 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 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 1/0
```

```
device(config-Management-1/0)# 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. Firmware upgrade or downgrade should be done to a FIPS-approved code.

NOTE
Do not configure the TACACS+ protocol for authentication.

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

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

11. Configure LDAP authentication:
    a) Enter the **crypto import** command in privileged EXEC mode to import the LDAP CA certificate.

```
device# crypto import ldapca protocol SCP host <IP> user <user-id> directory /<full-path> crypto
file cacert.pem
Password: **********
```

    The CA certificate imported must be generated using RSA-2048 with SHA-256.
    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 <name, eg. pad112r2.1a12security.xyz.com> basedn <domain, eg.
1a12security.xyz.com>
```

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

```
device(config)# ip dns domain-name <name, eg. 1a12security.xyz.com>
device(config)# ip dns name-server <server IP>
```

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

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

12. If required to set up a syslog server, follow the steps below to enable secure logging:
    a) Enter the **crypto import** command in privileged EXEC mode to import the SYSLOG CA certificate.

```
device# crypto import syslogca protocol SCP host <IP> user <user-id> directory /<full-path>
crypto file cacert.pem
Password: **********
```

    The CA certificate imported must be RSA-2048 with SHA-256 encryption.

    NOTE
    The syslog server certificate must use an IP-address for both Common Name (CN) and Subject Alternative Name (SAN).

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

13. If SSH public key authentication is required, 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.

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

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

14. 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
    ```

15. 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
    ```

16. Vcenter and dot1x(802.1x) features are not FIPS compliant.

    a) If dot1x is enabled, execute the following command to disable 802.1x globally.

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

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

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

17. If SNMP needs to be used, enter the **snmp-server v3host** *ip username* command to allow only SNMPv3 notifications to be sent. To configure the SNMP agent, use SNMPv3 with both authentication and privacy enabled.

    See the *Extreme Network OS Command Reference* for information on SNMPv3 configuration.

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

    ```
    device(config)#username admin password <enter password> role admin
    device(config)#username user password <enter password> role user
    ```

19. Disable telnet service with the following command.

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

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

    ```
    device#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.

   If the FIPS-approved mode has been enabled, the switch will reboot in the FIPS-compliant state.

   NOTE
   For the switch to remain FIPS-compliant, the HTTP, Telnet, and device 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.

Configuring x.509v3 digital certificate-based SSH authentication support

Configures SSH authentication using X.509v3 digital certificates so that users are authenticated using a X.509v3 certificate.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Configure the algorithm accepted by the SSH client for server authentication.

```
device(config)# ssh server algorithm hostkey x509v3-ssh-rsa
```

3. Configure the algorithm that is negotiated with the SSH client for user authentication. Only the configured algorithm is accepted by the SSH client for user authentication.

```
device(config)# ssh server algorithm publickey x509v3-ssh-rsa
```

4. Configure the server certificate profile and enter SSH certificate profile server configuration mode.

```
device(config)# ssh server certificate profile server
```

5. Configure trustpoint to the server certificate profile that is used to verify the incoming server certificate.

```
device(ssh-server-cert-profile-server)# trustpoint sign trust1
```

   NOTE
   Configure the trustpoint "trust1" first; thereafter, import the certificate (cert-type https) using the same trustpoint.

```
device(config-rbridge-id-1)# crypto key label mykey1 rsa modulus 2048
device(config-rbridge-id-1)# crypto ca trustpoint trust1
device(config-ca-t1)#keypair mykey1
device(config-ca-t1)# exit

device#crypto ca authenticate trust1 cert-type https protocol SCP host 10.24.15.200 directory /root/
jdoe/certs file ca.cert.pem user root password pass
device#crypto ca enroll trust1 cert-type https protocol SCP country US state CA locality San Jose
organization Engg orgunit Engg common jdoe directory /root/jdoe/certs host 10.24.15.200 user root
password pass
device#crypto ca import trust1 certificate cert-type https protocol SCP directory /root/jdoe/certs
file jdoe.pem host 10.24.15.200 user root password pass
```

6. Use the **ssh server** command to configure the server certificate profile and enter SSH server certificate profile user configuration mode.

```
device(config)# ssh server certificate profile user
```

7. Use the **trustpoint** command to configure the trustpoint that is used to verify the incoming user certificate. The SSH server uses the certificate associated with this trustpoint for user authentication.

```
device(ssh-server-cert-profile-user)# trustpoint verify trust2
```

Configuring keychain support

Key chains are sequences of keys. Users can configure key chains and can use keys with features that secure communications with other devices by using key-based authentication and optionally perform periodic key rotations within the chain.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enter keychain configuration mode. Up to 128 keychains can be configured. Valid name length is from 4 characters through 32 characters. No special characters are allowed, except for the underscore and hyphen.

```
device(config)# keychain  keychain1
device(config-keychain1)#
```

3. Configure the acceptance tolerance for the key.

```
device(config-keychain1)# accept-tolerance 500
```

   The range of valid values is from 0 through 600 seconds.

4. Enter key configuration mode. The range of valid values is from 1 through 65535.

```
device(config-keychain1)# keyID 10
device(config-keychain-key)#
```

   The keychain configurations contain only the default values until modified by other commands.

5. Set the encryption level for the key.

```
device(config-keychain-key)# key-string Mystring1 encryption-level 0
```

   The valid values are 0 and 7. The default value is 7.

6. Configure the acceptance lifetime for the key.

```
device(config-keychain-key)# accept-lifetime local true 00:00:00|07/04/2018 23:59:59|12/04/2018
```

   Default value for this parameter is 0, which means that the key is not active until the lifetime is configured. By default this command is not set.

7. Set the hash algorithm for the key.

```
device(config-keychain-key)# key-algorithm HMAC-SHA-384
```

   The valid algorithms are HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512. The default algorithm is HMAC-SHA-256.

8. Use the **show running-config keychain** command to verify your settings.

```
device(config-keychain-key)# do show running-config keychain keychain1
keychain child
 accept-tolerance 500
 keyID 10
  key-string $9$XutLBELmbQ765dsLycIP/A== encryption-level 0
  accept-lifetime local true 00:00:00|07/04/2018 23:59:59|12/04/2018
  key-algorithm HMAC-SHA-384
 !
```

The following is an example of configuring a single keychain and key.

```
device# configure terminal
device(config)# keychain  keychain1
device(config-keychain1)# accept-tolerance 500
device(config-keychain1)# keyID 10
device(config-keychain-key)# key-string Mystring1 encryption-level 4
device(config-key-chain-key)# accept-lifetime local true 00:00:00|07/04/2018 23:59:59|12/04/2018
device(config-keychain-key)# do show running-config keychain keychain1
keychain keychain1
 accept-tolerance 500
 key 1
  key-string $9$XutLBELmbQ765dsLycIP/A== encryption-level 4
  accept-lifetime local true 00:00:00|07/04/2018 23:59:59|12/04/2018
  key-algorithm HMAC-SHA-256
 !
device(config-keychain-key)# exit
device(config)#
```

Configuring keychain for OSPFv2

Key chains are sequences of keys (shared secrets). Users can configure key chains and can use keys with features that secure communications with other devices by using key-based authentication and optionally perform periodic key rotations within the chain.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enter the **rbridge-id** command with an RBridge ID to enter RBridge ID configuration mode.

```
device(config)# rbridge-id 122
```

3. Enter the **router ospf** command to enter OSPF router configuration mode and enable OSPFv2 on the device.

```
device(config-rbridge-id-122)# router ospf
```

4. Enter the **area** command to assign an OSPFv2 area ID.

```
device(config-router-ospf-vrf-default-vrf)# area 0
```

5. Enter the **area** command to assign a second OSPFv2 area ID.

```
device(config-router-ospf-vrf-default-vrf)# area 1
```

6. Enter interface configuration mode.

```
device(config)# interface tengigabitethernet 1/0/1
device(conf-if-te-1/0/1)# ip ospf area 0
```

7. Activate the OSPF plugin using the **ip ospf authentication key-chain** ipv6 ospf authentication key-chain*keychainname* command.

```
device(conf-if-te-1/0/1)# ip ospf authentication key-chain keychain1
```

   The keychain is authorized for the configured settings. For information on configuring keychains, refer to Configuring keychain support on page 23.

8. Enter the **area virtual-link** command and the ID of the OSPFv2 device at the remote end of the virtual link to configure the virtual link endpoint.

```
device(config-router-ospf-vrf-default-vrf)# area 1 virtual-link 3.3.3.3
device(config-router-ospf-vrf-default-vrf)# area 1 virtual-link 10.2.2.2 authentication key-chain
keychain1
```

9. On the peer device, enter the **configure terminal** command to access global configuration mode.

```
device# configure terminal
```

10. Enter the **rbridge-id** command with an RBridge ID to enter RBridge ID configuration mode.

```
device(config)# rbridge-id 104
```

11. Enter the **router ospf** command to enter OSPFv2 router configuration mode and enable OSPFv2 on the device.

```
device(config-rbridge-id-104)# router ospf
```

12. Enter the **area** command to assign an OSPFv2 area ID.

```
device(config-router-ospf-vrf-default-vrf)# area 1
```

13. Enter the **area** command to assign an OSPFv2 area ID.

```
device(config-router-ospf-vrf-default-vrf)# area 2
```

14. Enter the **area virtual-link** command and the ID of the OSPFv2 device at the remote end of the virtual link to configure the virtual link endpoint.

```
device(config-router-ospf-vrf-default-vrf)# area 1 virtual-link 3.3.3.3
```

Configuring Keychain for OSPFv3

Key chains are sequences of keys (shared secrets). Users can configure key chains and can use keys with features that secure communications with other devices by using key-based authentication and optionally perform periodic key rotations within the chain.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enter the **rbridge-id** command with an RBridge ID to enter RBridge ID configuration mode.

```
device(config)# rbridge-id 122
```

3. Enter the **ip router-id** command to specify the router ID.

```
device(config-rbridge-id-122)# ip router-id 3.3.3.3
```

4. Return to global configuration mode.

```
device(conf-if-te-1/0/1)# exit
device(config)#
```

5. Enter the **ipv6 router ospf** command to enter OSPFv3 router configuration mode and enable OSPFv3 on the device.

```
device(config-rbridge-id-122)# ipv6 router ospf
```

6. Enter the **area** command to assign an OSPFv3 area ID.

```
device(config-ipv6-router-ospf-vrf-default-vrf)# area 0
```

7. Enter the **area** command to assign an OSPFv3 area ID.

```
device(config-ipv6-router-ospf-vrf-default-vrf)# area 1
```

8. Enter interface configuration mode.

```
device(config)# interface tengigabitethernet 1/0/1
device(conf-if-te-1/0/1)# ipv6 ospf area <area-id>
```

9. Activate the OSPFv3 plugin using the **ipv6 ospf authentication key-chain** *keychainname* command.

```
device(conf-if-te-1/0/1)# ipv6 ospf authentication key-chain keychain1
```

   The keychain is authorized for the configured settings. For information on configuring keychains, refer to Configuring keychain support on page 23.

10. Enter the **area virtual-link** command and the ID of the OSPFv3 device at the remote end of the virtual link to configure the virtual link endpoint.

```
device(config-ipv6-router-ospf-vrf-default-vrf)# area 1 virtual-link 3.3.3.3
device(config-ipv6-router-ospf-vrf-default-vrf)# area 1 virtual-link 10.2.2.2 authentication key-
chain keychain1
```

11. On the peer device, enter the **configure terminal** command to access global configuration mode.

```
device# configure terminal
```

12. Enter the **rbridge-id** command with an RBridge ID to enter RBridge ID configuration mode.

```
device(config)# rbridge-id 104
```

13. Enter the **ip router-id** command to specify the router ID.

```
device(config-rbridge-id-104)# ip router-id 10.2.2.2
```

14. Enter the **ipv6 router ospf** command to enter OSPFv3 router configuration mode and enable OSPFv3 on the device.

```
device(config-rbridge-id-104)# ipv6 router ospf
```

15. Enter the **area** command to assign an OSPFv3 area ID.

```
device(config-ipv6-router-ospf-vrf-default-vrf)# area 1
```

16. Enter the **area** command to assign an OSPFv3 area ID.

```
device(config-ipv6-router-ospf-vrf-default-vrf)# area 2
```

17. Enter the **area virtual-link** command and the ID of the OSPFv3 device at the remote end of the virtual link to configure the virtual link endpoint.

```
device(config-ipv6-router-ospf-vrf-default-vrf)# area 1 virtual-link 3.3.3.3
```

Appendix: SP800-90A DRBG Implementation

DRBG support information

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

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 Extreme and can be downloaded on the crypto-module only through RSA 2048 and SHA256 verification.