53-1003198-02
09 May 2014

FastIron FIPS and Common Criteria

Configuration Guide

Supporting FastIron Software Release 08.0.01c

BROCADE

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.

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
FIPS and Common Critieria Configuration Guide for FastIron Devices	*53-1003198-02*	Added TLS encrypted syslog server configuration and validation	09 May 2014
FIPS and Common Critieria Configuration Guide for FastIron Devices	*53-1003198-01*	New document	10 February 2014

Contents

About This Guide

Chapter 1 Federal Information Processing Standards

Chapter 2 Upgrading Software on FIPS-enabled devices

Chapter 3 FIPS Configuration

About This Guide

This chapter contains the following sections:

Introduction

This guide includes procedures for configuring FIPS and Common Criteria on FastIron devices. Check the Brocade Release Notes for the version you are running to see if that version supports FIPS and Common Criteria.

Tamper-evident security seals must be applied to the product. For details on how to place the seals, see the platform-specific *FIPS Security Seal Procedures* document available on the MyBrocade website.

Audience

This document is designed for network engineers with a working knowledge of Layer 2 and Layer 3 switching and routing.

If you are using a Brocade Layer 3 Switch, you should be familiar with the following protocols if applicable to your network – IP, RIP, OSPF, BGP, ISIS, IGMP, PIM, DVMRP, and VRRP.

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords Identifies text to enter at the GUI or CLI
italic text	Provides emphasis Identifies variables Identifies document titles
`code` text	Identifies CLI output

For readability, command names in the narrative portions of this guide are presented in bold: for example, **show version**.

Command syntax conventions

Command syntax in this manual follows these conventions:

command and parameters	Commands and parameters are printed in bold.
[ ]	Optional parameter.
variable	Variables are printed in italics.
...	Repeat the previous element, for example “member[;member...]”
|	Choose from one of the parameters.

Notes, cautions, and danger notices

The following notices and statements are used in this manual. They are listed below in 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.

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.

Related publications

The Brocade FastIron Ethernet Switch Configuration Guides available at http://www.brocade.com/ethernetproducts, supplements the information in this guide.

Getting technical help

To contact Technical Support, go to http://www.brocade.com/services-support/index.page for the latest e-mail and telephone contact information.

Document feedback

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. Forward your feedback to:

documentation@brocade.com

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.

Chapter

Federal Information Processing Standards 1

This chapter contains information about the Federal Information Processing Standards (FIPS) mode on the Brocade device that is compliant with standards established by the United States government and the National Institute of Standards and Technology (NIST). The sections in this chapter describe an overview about FIPS mode, and how FIPS works.

NOTE
All software releases do not support FIPS. Refer to the Release notes for the sofware you are running to see if it supports FIPS.

Overview

FIPS 140-2 are security standards developed by the United States government and NIST for use by all non-military government agencies and by government contractors. Due to their importance within the security industry, these standards form a baseline for many security requirements.

The FIPS Publication 140-2 is a technical standard and worldwide de-facto standard for the implementation of cryptographic modules. In FIPS mode, the network processing occurs in the kernel and in privileged daemons.

NOTE
To determine if the FastIron device and current software version is FIPS certified, see http://csrc.nist.gov/groups/STM/cmvp/validation.html.

You can configure the Brocade device to run in FIPS mode to ensure that the device is operating according to the standards stated in FIPS Publication 140-2.

A Brocade device is FIPS 140-2-compliant when the following requirements have been met:

- -resistant labels are applied to the device according to the instructions included in the -resistant accessory kit. The accessory kit is purchased separately.
- The device software is placed in FIPS mode with the FIPS security policy applied.

NOTE
Tamper-evident security seals must be applied to the product. For details on how to place the tamper-evident security seals, see the platform-specific *FIPS Security Seal Procedures* document available on the MyBrocade website.

How FIPS works

You place a device in FIPS mode by entering the **fips enable** CLI command on the management station while the station is connected to the device console port with a serial cable. After you enter the **fips enable** command, the device is administratively in FIPS mode and by default runs in strict FIPS-compliant mode upon reload.

The default FIPS policy is for the system to run in a strict mode that fully supports FIPS 140-2 specifications. However, the device allows you the flexibility to configure a modified FIPS policy according to your network requirements. A FIPS policy that varies from the default policy weakens the intent of the FIPS 140-2 specifications; when implemented, the device is not operating in full compliance with these specifications. Refer to "Modifying the FIPS policy" on page 22.

The default FIPS policy enforces the following actions for strict FIPS compliance:

- Disables TFTP access
- Disables monitor access to memory access commands
- Returns 0 or null for SNMP MIBs for passwords or keys
- Zeroizes shared secrets and passwords

The device performs the following functions automatically during reboot after the **fips enable** command is entered:

- Disables Telnet
- Enables SCP access
- Disables the HTTP server
- HTTPS server:
  - Disables SSL 3.0 and uses only TLS version 1.0 and greater
  - Disables the RC4 cipher
  - Removes the **web-management allow-no-password** command from the configuration
- Disables SNMP access to Critical Security Parameter (CSP) MIB objects

After defining the FIPS policy, save the configuration, and reboot the device. While the device is booting, several tests are run to ensure the device is FIPS compliant. After these tests are completed successfully, the device reloads and is operationally in FIPS mode.

All the optional FIPS policy commands are provided to perform various FIPS non-approved operations when FIPS is enabled. It should be noted that if this any of these policy commands are configured, the module is not operating in the approved FIPS mode.

Chapter

Upgrading Software on FIPS-enabled devices 2

This chapter contains the software upgrade and downgrade information for FIPS devices. The sections in this chapter describe how to upgrade or downgrade the software.

CAUTION

After enabling the FIPS mode on your device, you cannot disable it without losing the device configuration. For disabling the FIPS mode, it is recommended that you contact Brocade Technical Support and perform the procedure under qualified guidance.

Upgrading FIPS-enabled devices

This section lists the information and steps to prepare a non-FIPS device for FIPS compliance.

FIPS compliance

FIPS 140-2 compliance is a combination of implemented hardware procedures and the activation of a software-based security policy.

FIPS 140-2 certification is achieved when the device meets certain physical security and software conditions:

- FIPS physical security requirements: Tamper-evident security seals (available in Brocade FIPS kit purchased separately) must be applied to the product, based on FIPS Security Seal Procedure document (available on my.brocade.com).
- FIPS software compliance: The devices are configured to run in FIPS operational mode with the default FIPS security policy.

NOTE
Although commands to alter the FIPS security policy exist, altering the default FIPS security policy is not recommended.

Standard factory pre-loaded images and locations

Table 1 lists the locations and types of factory-loaded software.

TABLE 1 Factory pre-loaded images and locations

Device	Primary Flash	Secondary Flash
FSX 800 FSX 1600	Layer 2	Base Layer 3
FSX 800 PREM FSX 1600 PREM	Full Layer 3	Layer 2
FCX	Layer 2	Layer 3
ICX 6610	Layer 2	Layer 3
ICX 6430	Layer 2	Layer 3
ICX 6450 ICX 6450-C12 ICX 6450-C12-PD	Layer 2	Layer 3
ICX 6650	Layer 2	Layer 3

Preparing for a FIPS software upgrade

Before upgrading the software on the device, following are some important notes to be considered.

- FSX and FCX devices can store two Full Layer 3 image or two Layer 2 or Base Layer 3 images.
- You can upgrade FastIron SX family products only if a new 0-port management module is installed.
- All units in a stack must be running the same software release. Verify the images using the **show flash CLI** command.

NOTE
Signature file auto-copy is not supported. Only image files will be updated and fips check would fail if the corresponding signature file is not present in the same partition.

Performing a FIPS or CC software upgrade

To upgrade the IronWare software image to support a FIPS or CC environment, perform the following steps.

1. Place the new flash signature file and the new flash image on a SCP client directory to which the Brocade device has access.
2. If the device has 8 MB of flash memory or if you want to install a Full Layer 3 image on an FCX or SX device, you must delete the primary and secondary images before upgrading the image. To delete images from the flash, enter the following commands:

```
Device# erase flash primary
Device# erase flash secondary
```

3. To copy the signature file from SCP client into flash memory, enter the copy command:

Syntax: Syntax: scp <signaturefilename> username@ipaddress:file:<primary.sig | secondary.sig>

```
C:\Program Files\PuTTY62>pscp FCXR08001.sig test@1.20.2.2:file:secondary.sig
```

4. To copy the flash code from scp client into flash memory, enter the copy command.

   Syntax: Syntax: scp <image.bin> username@ipaddress:flash:<pri|sec>:<filename>

   ```
   C:\Program Files\PuTTY62>pscp FCXR08001.bin
   test@1.20.66.70:flash:sec:FCXR08001.bin
   ```

5. Verify that the flash code has been successfully copied by examing the console log or entering the show flash command at any level of the CLI.

   ```
   --FIPS: secondary image verification success
   ```

6. To enable FIPS or CC, see the“FIPS Configuration” chapter.
7. Save the running configuration by entering the **write memory** command.
8. Reload the configuration to run the FIPS-supported or CC-supported image by entering the **reload** command. During system initialization, firmware verification for a specified signature occurs. If verification fails, the following actions occur:
   - The system fails to initialize.
   - A log message appears on the console.
   - The device begins a self-reload.
9. For devices in an IronStack, make sure all devices are running the same software image.

Troubleshooting a failed software image installation

When FIPS is enabled and a signature file does not pass the validation check (does not match the binary file) or is corrupt, the device does not allow the code to finish loading. In this case, cascade reloads occur. You can interrupt a reload to recover and install another image from the TFTP server at the boot loader prompt.

NOTE
You cannot copy a signature file from the boot loader prompt. Before attempting recovery through boot loader prompt, you must ensure that the correct signature file is already loaded.

1. Reboot the device and press 'b' enter the boot loader prompt.
2. Do the following to configure the network setting in boot loader:

   ```
   Brocade>> setenv ipaddr A.B.C.D
   Brocade>> setenv gatewayip W.X.Y.Z
   Brocade>> setenv netmask E.F.G.H
   Brocade>> saveenv
   ```

   NOTE
   The IP address A.B.C.D must be different from the management IP address of the switch.

3. Configure FastIron image name and upgrade primary or secondary image:

   ```
   Brocade>> setenv image_name <path/filename>
   Brocade>> saveenv
   ```

```
Brocade>> update_primary
Or
Brocade>> update_secondary
```

If the software installation fails, the switch might reboot continuously. Do the following to recover from an failed image installation:

1. Enter "b" to interrupt the reload and enter the boot loader prompt.
2. Boot from the other partition. If your software installation was to the primary partition, you can boot from the other partition, which was unaffected. Enter the following command at the boot loader prompt:

   ```
   Brocade>>boot_secondary
   Or
   Brocade>>boot_primary
   ```

   In case the FastIron device is on a rolling reboot due to signature mismatch, use the **factory set-default** command to reset the configuration and reboot.

   NOTE
   During the recovery method, the existing configuration and keys will be lost after reboot.

Downgrading from FIPS to non-FIPS

While a FIPS-supported image is running on the device, at any given time, the image can be running in FIPS or non-FIPS operational mode. When change from FIPS mode to non-FIPS, copy signature file also. If the image is 07.03.00c or older, signature copy may not be needed. Downgrading from FIPS mode to non-FIPS mode will clear all shared secrets, host passwords, ssh and https host keys and https certificate.

NOTE
Before upgrading or downgrading a major software verson, zeroize the keys by executing the **crypto key zeroize** command before executing upgrade or downgrade.

To place a device in non-FIPS mode and then use TFTP or SCP to download and initialize an older image, complete the following steps.

1. Logon to the device by entering your user name and password.
2. Disable FIPS by entering the **no fips enable** or **no fips enable common-criteria** command respectively at the prompt.
3. To copy the desired non-FIPS binary image into flash, enter the following command:

   Syntax: **copy tftp flash** <*ip-addr*> <*image-name*>

   NOTE
   The device will perform a checksum validation on the newly downloaded image because the currently running image does not support FIPS and does not require a signature file.

4. Reload the configuration by entering the **reload** command.

   If the unit goes into rolling reboots when there is a mismatch between image and signature files, the following command can be used at the boot loaded prompt:

   ```
   Monitor>remote address A.B.C.D/M
   ```

```
Monitor>remote default-gateway W.X.Y.Z
Monitor>copy tftp flash <ip-addr> <filename> <primary | secondary>
factory set-def
Monitor>boot system flash <primary | secondary>
```

The above commands brings switch configuration to the factory default state and it means that FIPS configuration is also removed and the switch image can be copied and switch will load with this image without signature verification.

Once the switch is rebooted, see "Placing the device in FIPS mode" section to enable FIPS.

SSH connection after upgrading a FIPS or CC operational device to 08.0.01 or higher software versions

After upgrading a 08.0.00a or lower version FastIron device in FIPS or CC operational mode to 08.0.01 or higher software versions, you should re-import the new format public keys into the device if you are using key authentication for SSH connection. For details on how to import public keys, see *Importing authorized public keys into the Brocade device* section in the *FastIron Ethernet Switch Security Configuration Guide*.

SSH connection after upgrading a FIPS or CC operational device to 08.0.01 or higher software versions

Chapter

FIPS Configuration

3

This chapter contains steps for configuring FIPS mode on the Brocade device in compliance with standards established by the United States government and the National Institute of Standards and Technology (NIST). The sections in this chapter describe FIPS mode, how to enable and disable FIPS mode on the device, and the behavior of the device in FIPS mode.

User roles in FIPS mode

A Brocade device in FIPS mode supports three user roles:

- Crypto Officer Role: The Crypto Officer Role on the device in FIPS mode is equivalent to the administrator role, or the super-user, in non-FIPS mode.
- Port Configuration Administrator Role: The Port Configuration Administrator on the device in FIPS mode is equivalent to the port configuration user in non-FIPS mode and has write access to the interface configuration mode only.
- User Role: The User Role on the device in FIPS mode has read-only privileges and no configuration mode access.

Also, concurrent operators are supported but no limit is enforced. The number of concurrent users is only limited by the system resources.

Commands disabled in FIPS mode

The device in FIPS mode does not support the following commands:

- enable password-display
- enable strict-password-enforcement

NOTE
Strict password enforcement is enabled by default, when the device is in FIPS mode and it cannot be disabled. The password must be at least eight characters long.

- web-management allow-no-password
- telnet server
- ip ssh scp disable
- iip ssh encryption aes-only
- ip ssh key-authentication no
- ip ssh permit-empty-password no
- web-management http

A device in FIPS mode does not support TFTP commands, including:

- copy tftp flash *<ip>*
- boot system tftp *<ip>* *<file>*

- **ip ssh pub-key-file tftp** *<ip> <file* | *pubkey>*
- **ip ssl certificate-data-file tftp** *<ip> <file>*
- **ip ssl private-key file tftp** *<tftp> <file>*

Hidden files in FIPS mode

Hidden files are not displayed when the device is in FIPS mode. Hidden files are displayed only when the device is in non-FIPS mode.

Cryptographic algorithms in FIPS mode

The device in FIPS mode supports the following FIPS 140-2 approved cryptographic algorithms:

- Advanced Encryption Algorithm (AES)
- Secure Hash Algorithm (this includes all SHA variants the module supports: SHA-1, SHA-256, SHA-384, and SHA-512)
- Keyed-Hash Message Authentication code (HMAC)
- Deterministic Random Bit Generator (DRBG)
- Digital Signature Algorithm (DSA)
- Rivest, Shamir, and Adleman public key encryption Algorithm (RSA))
- Elliptic curve Digital Signature Algorithm (ECDSA)

Allowed exceptions include:

- RSA Key Wrapping
- Diffie-Hellman (DH)
- SNMPv3
- Message Digest 5 (MD5) as used in TLSv1.0
- Hashed Message Authentication codes - Message Digest 5 (HMAC-MD5) as used in RADIUS.
- Non-Deterministic Random Number Generator (NDRNG)
- SSHv2 Key Derivation Function (KDF)

The device in FIPS mode does not support the following cryptographic algorithms:

- RC4
- DES

Usernames and SSH public key authentication

Currently in FastIron 07.3.00f CVR branch, the device stores or uses the username that is provided by the SSH client when public-key authentication is used. Therefore, the username is mentioned in the login/logout syslogs. The FastIron devices support the following:

1. We will save the username from the public-key authentication request. This will be used in the login/logout syslogs.
2. When FIPS mode is operational, we will use this username to match against a username attached with the SSH client public key that is stored on the device. If the username does not match, then the authentication request is denied.

Implementation

The client public key file format allows for a username to be provided in the "Subject:" field. Additional private headers can be used. The following public key example shows the two headers that will be used by the device.

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20121206"
Subject: brcd
x-brocade-privilege-level: 0
AAAAB3NzaC1yc2EAAAABJQAAAQEAkwiApY1x4T/DHII5JzR2OgqcF5vjlubNcvSE
UjkGmiRBDSOicjxS0ZLm1b2xFpVzw8XxSSy8cxvntfs5ortOt80QzynqgL+H2zJa
Lb4Qbu6/1vakJbPb/VUJE66Zezh0c8mze6zTbiP4iQ/Wn2lxpSmlS5cdowmFlZ7B
97xcagJIBl+7JKuvj8P+85ESUf2/pcrogqx7gdr1IpP2nev5s4xwCWFGtr2R/yMF
Q9h0xLcc4A7vLTDuY/h1GzLdICgtNYdqpUhpw+w0DkTKbQuDPd0gkwHkoFwg85lE
4VCDevdC/DeOCNJjNp9NbVD+SW6uL4NymmV7/i0YbPyl3gTESQ==
---- END SSH2 PUBLIC KEY ----
```

After decoding the base64 encoded public keys to binary format, a SHA1 hash of the binary format key is created. This hash is saved to memory. We verify that this hash is unique across the hashes of client public keys that have already been parsed. Additionally, non-empty usernames are also verified to be unique across the usernames already parsed in the public key. Access is denied, if the username is mismatched.

The username has following restrictions:

- It cannot contain control characters, spaces, ", ?, |, or characters above ASCII code 0x7F.
- It needs to be less than or equal to 48 characters.
- No continuation lines are allowed in the file for these headers.
- The username has to be specified with the public key for that key to allow access. The user must specify a non-empty username in the login request.

Restrictions

- **No exec authorization from AAA**: No exec authorization through AAA server is available because the privilege level is obtained from the public key file private header field (x-brocade-privilege-level) as shown in the public key example in the section "Implementation" on page 11.
- **No exec accounting from AAA**
- **No system accounting from AAA**

Protocol changes in FIPS mode

Table 2 lists the protocols that undergo changes while the device is in FIPS mode with the default policy applied.

TABLE 2 Protocol changes

Protocols/ Algorithms	Supported in FIPS mode	Supported in Non-FIPS mode	For more information on individual protocol changes, refer to the following sections:
BGP	Yes	Yes	"BGP" on page 12
HTTP	No	Yes	"HTTP" on page 13
HTTPS	Yes, with limitations	Yes	"HTTPS" on page 13
IPsec	Yes, with limitations	Yes	"IPsec" on page 14
MD5 password encryption	Yes, with limitations. MD5 password encryption is supported for SNTP, VRRP, and VRRP-E.	Yes	
OSPFv3	Yes	Yes	"OSPFv2" on page 14
Proprietary 2-way encryption algorithms	No	Yes	"Proprietary 2-way encryption algorithms" on page 14
RADIUS	Yes, with limitations	Yes	"RADIUS" on page 14
SCP	Yes	Yes	"SCP" on page 15
SNMP	Yes, with limitations	Yes	"SNMP" on page 16
SSHv2	Yes, with limitations	Yes	"SSHv2" on page 18
Telnet	No	Yes	"Telnet" on page 18
TFTP	No	Yes	"TFTP" on page 18
Web Authentication	No	Yes	"Web Authentication" on page 18

BGP

Border Gateway Protocol (BGP) allows peer-to-peer authentication or client-to-server authentication. To authorize an authentication, use a command such as the following to configure shared secret keys for BGP:

```
Brocade(config-bgp-router)# neighbor 192.168.1.2 password P@$$w0rd
```

Syntax: [no] **neighbor** <*ip-addr*> | <*peer-group-name*> **password** <*string*>

For more information on BGP authentication commands, refer to FastIron Configuration Guide.

HTTP

HTTP is not supported on the device in FIPS mode.

The **web-management http** command is disabled if it is included in the device's configuration. When the HTTP server is enabled because the **web-management http** command has been configured, the system removes the command from the configuration and the device displays the following messages:

```
FIPS Compliance: HTTP service will been disabled
```

HTTPS continues to be enabled in FIPS mode and the configuration changes the **web-management http** command to the **web-management https** command.

HTTPS

The following HTTPS configurations are affected in FIPS mode:

- The **web-management https** command is maintained and offers equivalent functionality to the disabled **web-management http** command. Note that in addition to port 443, port 280 is also open for access by HP ProCurve Manager. You can disable this port using the **no web-management hp-top-tools** command.
- The **web-management allow-no-password** command is disabled.
- The AAA authentication method **none** option is not allowed in FIPS mode. For example, the **aaa authentication enable none** command (the **none** option designated as the authentication method) is disabled. In addition, you cannot enable FIPS when AAA authentication method **none** option is used. You must disable the **none** option before you can enable FIPS on the device.
- The **ip ssl certificate-data-file tftp** command is disabled when TFTP operation is disabled in FIPS mode. SCP supports this command's functionality. Refer to "SCP" on page 15.
- The **ip ssl private-key-file tftp** command is disabled when TFTP operation is disabled in FIPS mode. SCP supports the functionality of this command. Refer to "SCP" on page 15.
- The **crypto-ssl certificate zeroize** command zeroes out the RSA key pair and removes the digital certificate.
- SSL version 3 and earlier versions are disabled and TLS 1.0 or later versions are enabled.
- RC4 in TLS is disabled.

The FIPS 140-2 cipher suites consist of the following algorithms:

- Triple-DES (FIPS 46-3) or AES (FIPS 197) for symmetric key encryption and decryption.
- Secure Hash Standard (SHA-1, SHA-256, SHA-384, and SHA-512) (FIPS 180-2) for hashing.
- HMAC (FIPS 198) for keyed hash.
- Random number generator Hash DRBG (NIST SP800-90).
- Diffie-Hellman, EC Diffie-Hellman, or Key Wrapping using RSA keys for key establishment.
- DSA (FIPS 186-2 with Change Notice 1), RSA (PKCS #1 v2.1), or ECDSA (ANSI X9.62) for signature generation and verification.

The following cipher suites are allowed in FIPS mode:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

- TLS_RSA_WITH_AES_256_CBC_SHA

The cipher suite TLS_RSA_WITH_AES_256 is the default cipher suite.

IPsec

FIPS 140-2 does not allow null encryption.

OSPFv2

The OSPFv2 protocol uses IPsec with IP ESP and HMAC-SHA-196, and is allowed in FIPS mode.

OSPF allows peer-to-peer authentication or client-to-server authentication. To authorize an authentication, use commands such as the following to configure shared secret keys for OSPF:

```
Brocade(config-if-e1000-1/1)# ip ospf authentication-key P@$$w0rd
```

Syntax: **ip ospf authentication-key** <*string*>

```
Brocade(config-if-e1000-1/2)# ip ospf md5-authentication key-id 1 key P@$$w0rd>
```

Syntax: **ip ospf md5-authentication key-id** <num> **key** <*string*>

```
Brocade(config-ospf-router)# area 2 virtual-link 2.3.4.5 md5-authentication
key-id 2 key P@$$w0rd
```

Syntax: **[no] area** <*ip-addr*> | <*num*> **virtual-link** <*router-id*> [**authentication-key** <*string*> | **md5-authentication key-id** <*num*> **key** [0|1] <*string*>]

```
Brocade(config-if-e1000-1/1)#ipv6 ospf authentication ipsec spi 256 esp sha1
1234567890123456789012345678901234567890
```

Syntax: **[no] ipv6 ospf authentication ipsec spi** <*spinum*> **esp sha1** [**no-encrypt**] <*key*>

Proprietary 2-way encryption algorithms

The routing protocols OSPFv2, BGP, and the management protocol SNMP save authentications parameters using one of the following two proprietary algorithms:

- Global encoding scheme
- Base 64 encoding scheme

These proprietary algorithms are not supported in FIPS mode. When the default FIPS policy is applied, these authentication parameters are zeroized.

RADIUS

HMAC-MD5 authentication used in RADIUS is allowed in FIPS mode.

RADIUS allows peer-to-peer authentication or client-to-server authentication. To authorize an authentication, use commands such as the following to configure shared secret keys for RADIUS:

```
Brocade(config)# radius-server host 1.2.3.4 auth-port 1812 acct-port 1813 default
key 1 Example01
```

Syntax: [no] radius-server host *<ip-addr>* | *<server-name>* [auth-port *<number>* acct-port *<number>*[authentication-only accounting-only default] [key [0 1 2] *<string>* [dot1x]]]

```
Brocade(config)# radius-server key 1 Example01
```

Syntax: [no] radius-server key [0 | 1] *<string>*

SCP

Table 3 lists the Secure Copy (SCP) commands that are available to compensate for equivalent existing functionality of TFTP commands disabled in FIPS mode.

TABLE 3 Corresponding TFTP and SCP commands

Command functionality	TFTP commands not allowed in FIPS mode	SCP commands with corresponding functionality in FIPS mode
Import a digital certificate	**ip ssl certificate-data-file tftp** *<ip-address>* *<certificate-filename>*	**scp** *<certificate-filename>* *<user>*@*<ip-address>*:**sslCert**
Import an RSA private key from a client	**ip ssl private-key-file tftp** *<ip-address>* *<key-filename>*	**scp** *<key-filename>* *<user>*@*<ip-address>*: **sslPrivKey**
Load a DSA public key file from a client	**ip ssh pub-key-file tftp** *<ip-address>* *<key-filename>*	**scp** *<key-filename>* *<user>*@*<ip-address>*: **sshPubKey**

Importing a digital certificate

To import a digital certificate using SCP, enter a command such as the following one:

```
C:> scp certfile user@192.168.89.210:sslCert
```

Syntax: **scp** *<certificate-filename>* *<user>*@*<ip-address>*:**sslCert**

The *<ip-address>* variable is the IP address of the server from which the digital certificate file is downloaded.

The *<certificate-filename>* variable is the file name of the digital certificate that you are importing to the device.

The functionality of the **scp** command is equivalent to that of the disabled **ip ssl certificate-data-file tftp** command.

For more information on the **scp** command, refer to FastIron Configuration Guide.

Importing an RSA private key from a client

To import an RSA private key from a client using SCP, enter a command such as the following one:

```
C:> scp keyfile user@192.168.9.210:sslPrivKey
```

Syntax: **scp** *<key-filename>* *<user>*@*<ip-address>:* **sslPrivKey**

The *<ip-address>* variable is the IP address of the server that contains the private key file.

The <*key-filename*> variable is the file name of the private key that you want to import into the device.

The functionality of the **scp** command is equivalent to that of the disabled **ip ssl private-key-file tftp** command.

For more information on the **scp** command, refer to FastIron Configuration Guide.

Loading a DSA public key file from a client

To load a DSA public key file from a client using SCP, enter a command such as the following one:

```
C:> scp pkeys.txt user@192.168.1.234:sshPubKey
```

Syntax: **scp** <*key-filename*> <*user*>@<*ip-address*>:**sshPubKey**

The <*ip-address*> variable is the IP address of the server that contains the public key file.

The <*key-filename*> variable is the name of the DSA public key file that you want to import into the device.

The functionality of the **scp** command is equivalent to the disabled **ip ssh pub-key-file tftp** command.

For more information on the **scp** command, refer to FastIron Configuration Guide.

SNMP

In the FIPS mode of operation, the device uses the existing SNMP configuration. However, MIB objects related to keys and passwords output NULL or a 0 value. Refer to "SNMP CSP objects" on page 17.

SNMP allows peer-to-peer authentication or client-to-server authentication. To authorize an authentication, use commands such as the following to configure shared secret keys for SNMP:

```
Brocade(config)# snmp-server community brocadeSNMP ro
```

Syntax: [**no**] **snmp-server community** <*string*> [**ro** | **rw**]

```
Brocade(config)# snmp-server host 10.1.53.181 version v2c 1 $Si2^=d
```

Syntax: [**no**] **snmp-server host** <*ip-addr*> <*string*> [**port** <*value*>]

```
Brocade(config)# snmp-server group admingrp v3 priv read all write all notify all
```

Syntax: [**no**]**snmp-server group** <*groupname*> **v1**| **v2**| **v3 auth** | **noauth** | **priv** [**access** <standard-ACL-id>] [**read** <viewstring> | **write** <viewstring> | **notify** <viewstring>]

```
Brocade(config)# snmp-server user adminuser admingrp v3 encrypted auth md5
c1c510d4f3c6bec15ff14f9c0f3ec120 priv encrypted aes
b0c4c6c05cded8cfe3a335299347c71b
```

Syntax: [**no**] **snmp-server user** <*name*> <*groupname*> **v3** [[**access** <*standard-ACL-id*>] [[**encrypted**] [**auth md5** <*md5-password*> | **sha** <*sha-password*>] [**priv** [**encrypted**] **des** <*des-password-key*> | **aes** <*aes-password-key*>]]]

SNMP CSP objects

The following SNMP MIB objects represent the Critical Security Parameter (CSP) entities that are restricted in FIPS mode:

Enterprise MIB objects:

- snRadiusKey
- snRadiusServerRowKey
- snVrrpIfAuthPassword
- snAgGblPassword
- snAgGblReadOnlyCommunity
- snAgGblReadWriteCommunity
- snAgGblTelnetPassword
- snAgentUserAccntPassword
- fdryRadiusServerRowKey
- snOspfIfAuthKey
- snOspfIfMd5AuthKey
- snOspfIf2AuthKey
- snOspfIf2Md5authKey
- snOspfVirtIfAuthKey
- snOspfVirtIfMd5AuthKey
- snOspfIfStatusAuthKey
- snOspfIfStatusMd5AuthKey
- snOspfVirtIfStatusAuthKey
- snOspfVirtIfStatusMd5AuthKey
- snBgp4NeighGenCfgPass
- snVrrpIf2AuthPassword
- snVsrpIfAuthPassword

Standard MIB objects:

- rip2IfConfAuthKey
- vrrpOperAuthKey
- dvmrpInterfaceKey

SSHv2

Secure Shell version 2 (SSHv2) is allowed in FIPS mode.

The following SSH configurations are affected when the Brocade device is in FIPS mode:

- The **ssh server** command enables the SSH server. The SSH server is always enabled; however, to start it, use the **crypto key generate** command to create host keys.
- The **ip ssh encryption aes-only** command is disabled.
- The **ip ssh key-authentication** command is disabled.
- The **ip ssh permit-empty-password** command is disabled.
- The **ip ssh pub-key-file tftp** command is disabled.
- The **ip ssh scp** command ensures that SCP is enabled to run in FIPS mode. SCP is needed for file communication and the **ip ssh scp disable** command is disabled in FIPS mode and displays the following message:

  ```
  FIPS Compliance: SCP needs to be enabled
  ```

- The **crypto key zeroize** command removes configured SSH keys.

Use the command **show ip ssh config** to display SSH configuration information.

SSH key generation time is affected by the increased security of authentication and encryption algorithms both in and out of FIPS mode.

Telnet

Telnet is disabled in FIPS mode as part of the default FIPS policy on the device. Attempts to start the Telnet server fail in FIPS mode.

TFTP

The following TFTP commands are disabled and return an error when TFTP operation is not allowed on the device in FIPS mode:

- All **copy tftp** commands
- The command **boot system tftp** <*ip-address*> <*filename*>

The following TFTP commands are disabled. Use SCP commands with equivalent functionality instead. Refer to "SCP" on page 15.

- **ip ssl certificate-data-file tftp** <*ip-address*> <*certificate-filename*>
- **ip ssl private-key-file tftp** <*ip-address*> <*key-filename*>
- **ip ssh pub-key-file tftp** <*ip-address*> <*key-filename*>

Web Authentication

Web Authentication is not supported when FIPS mode is enabled on the device.

System reset and boot in FIPS mode

Firmware digital signature verification and POST testing takes place as the device progresses through the boot sequence.

The following actions and limitations take effect when the device is operationally in FIPS mode according the FIPS default policy:

- Boot from TFTP is disabled.
- Monitor mode memory access command set is disabled. Configure an alternative FIPS policy to the default policy to access the command set. Refer to "Modifying the FIPS policy" on page 22.
- Boot Monitor access during cold boot is disabled with the exception of the option to access monitor mode during the boot sequence. Refer to "Accessing monitor mode in the event of continuous failure" on page 28.
- Access to memory test mode is disabled.
- Debug commands are disabled from the application prompt in FIPS mode.

Debugging in FIPS mode

The device reloads automatically when it encounters a system reset and enters FIPS failure state. The cause of failure logs on the console and the device performs a self-reboot.

You can conduct debugging in monitor mode when a flexible FIPS policy is applied on the device and in the event of continuous failure. Refer to "Access to monitor mode" on page 27.

Placing the device in FIPS mode

Placing the device in FIPS mode is a multiple part process that begins with enabling FIPS mode on the device. This places the device administratively in FIPS mode. To operate the device in FIPS mode, save the configuration, and reboot the device. Always back-up the desired configuration to ensure it is saved in the event of a system reset.

General steps to place the device in FIPS mode

1. Disable the AAA authentication method **none** option if used in the device configuration.
2. Copy the signature files. Refer to step 3 in section "Performing a FIPS or CC software upgrade" on page 4.
3. Perform a FIPS self test to verify the right signature files were copied. Refer to "Perform a FIPS self-test" on page 22.
4. Enable FIPS mode. Refer to "Enabling FIPS mode" on page 20.
5. Optionally, modify the default FIPS policy. Refer to "Modifying the FIPS policy" on page 22.
6. Optionally, zeroize shared secrets and host keys. Refer to "Zeroizing shared secrets and host keys" on page 23.
7. Save the configuration. Refer to "Saving the configuration" on page 24.
8. Reload the device. Refer to "Reloading the device" on page 25.

Enabling FIPS mode

1. Attach a management station (PC or terminal) to the management module serial (console) port using a serial cable.

   When the device is not in a console session, FIPS-related commands return errors.

2. Verify that the device is in non-FIPS mode using the following command:

   ```
   Brocade(config)#fips show
   ```

   Syntax: **fips show**

   The **fips show** command lists the current configuration of the device and can be run in both FIPS and non-FIPS modes to establish whether the device is truly in FIPS mode.

   The output of the **fips show** command confirms that the device is in FIPS mode and identifies the device as either administratively or operationally in FIPS mode.

   The following example shows the output of the **fips show** command before the **fips enable** command is entered, and administrative status is off and operational status is off:

   ```
   Brocade(config)#fips show
   FIPS mode:  Administrative Status: OFF, Operational Status: OFF
   ```

   If the device is already in administrative FIPS mode, you can modify the FIPS policy. Refer to "Modifying the FIPS policy" on page 22.

3. Use the following command to place the device administratively in FIPS mode:

   ```
   Brocade(config)# fips enable
   ```

   Syntax: **[no] fips enable**

   The following example shows a sample output of the **fips enable** command.

   ```
   Brocade(config)# fips enable
   All keys incompatible with FIPS 140-2 standard will be deleted.

   RSA Key pair not found

   RSA client Key pair not found
   This device is now running in FIPS administrative mode.
   At this time you can alter this system's FIPS default security policy
   and then enter FIPS operational mode.

   Note: Making changes to the default FIPS security policy weakens
   the security of the device and makes the device non-compliant with
   FIPS 140-2 Level 2, design assurance Level 3
   The default security policy defined in the FIPS
   Security Policy Document ensures that the device complies with all
   FIPS 140-2 specifications. Commands to alter the default security policy
   are available to the crypto-officer; however, Brocade does not recommend
   making changes to the default security policy at any time.
   =====================================

   To enter FIPS mode, complete the following steps:
   1. Install the signature file now if not already done. Failure to install
      signature or wrong signature file can cause continuous resets.
      Also, optionally, configure FIPS policy commands that meets your network
   ```

```
   requirements. You must explicitly configure the following services if you
want
   to use them when the device is operational in FIPS mode:
FIPS: SCP is already enabled

      - Allow TFTP access.
          Current status: Disabled
     - Allow SNMP Access to the Critical Security Parameter (CSP) MIB objects.
          Current status : Disabled
      - Allow access to all commands within the monitor mode.
          Current status: Disabled
      - Retention of shared secret keys for all protocols and the host
passwords.
          Current status: Clear
      - Retention of SSH DSA host keys.
          Current status: Clear
      - Retention of SSH RSA host keys and HTTPS certificate.
          Current status: Clear

2. Enter the "fips zeroize all" command, which zeroes out the shared secrets
    used by various networking protocols, including the host access passwords,
    SSH and HTTPS host-keys with the digital signature based on the configured
    FIPS Security Policy.
3. Save the running configuration.
4. Reload the device.
5. Do not press "b" during reload, else FIPS or CC will not be enabled
properly.
6. Enter the "fips show" command to verify that the device entered
    FIPS or CC operational mode.
=====================================

The system will disable the following services or commands after reload:
1. Telnet server will be disabled. The "telnet server" command will be
removed.
2. SCP will be enabled. The "ip ssh scp disable" command will be removed.
3. HTTP server will be disabled. The "web-management http" command will be
removed.
4. HTTPS server will change as follows:
      -SSL 3.0 will be disabled.
      -TLS version 1.0 and greater will be used.
      -RC4 cipher will be disabled.
      -Passwords will be required; the "web-management allow-no-password"
        command will be removed.
Passwords/Keys which dont comply FIPS standards will be removed on reload.
Please see FIPS config guide for complete details.
```

4. You can verify the status of the device as administratively in FIPS mode by using the **fips show** command.

   The following example shows the output of the **fips show** command on a FastIron device after the **fips enable** command is entered and administrative status is on and operational status is off:

```
Brocade#fips show
Cryptographic Module Version: FIFIPS07300_0314121830
FIPS mode: Administrative status ON: Operational status OFF
Common-Criteria: Administrative status OFF: Operational status OFF
System Specific
OS monitor access status is: Disabled
```

```
Management Protocol Specific:
Telnet server: Disabled
Telnet client: Disabled
TFTP client: Disabled
HTTPS SSL 3.0: Disabled
SNMP Access to security objects: Disabled

Critical security Parameter updates across FIPS boundary:
Protocol Shared secret and host passwords: Clear
Password Display: Disabled

HTTPS RSA Host Keys and Signature: Clear
SSH DSA Host keys: Clear
SSH RSA Host keys: Clear
```

5. You can use the **no web-management hp-top-tools** command to disable the TCP port 280 that allows access to the device by HP ProCurve Manager. See FastIron Configuration Guide for more details.

Perform a FIPS self-test

Use FIPS self-test to verify the sanity of FIPS software. For more information on the FIPS self-test, refer to “Running FIPS self-test” on page 26.

NOTE
During FIPS self-test, the CPU usage is high.

1. From Privileged EXEC level of the CLI on the console, execute fips self-test to verify that the FIPS Software and Firmware Integrity Test passes:

   Syntax: **fips self-tests**

   The following examples shows the FIPS Software and Firmware Integrity Test as passed:

   ```
   Brocade#fips self-test
   Running FIPS Power On Self Tests and Software/Firmware Integrity Test.
   FIPS Power On Self Tests and Software/Firmware Integrity tests successful.
   .....<output truncated>.......
   ```

2. If the test fails, make sure that the correct signature file was copied for the correct image file and version, and recopy as needed.

NOTE
This check must pass before saving the configuration and reloading the device.

Modifying the FIPS policy

After the device is administratively in FIPS mode, you can modify the default FIPS policy.

NOTE
Making changes to the default FIPS policy on the device is not recommended and weakens the security of the device. Any modification of the default FIPS policy places the device in a state that is not in compliance with FIPS 140-2.

The output of the **fips enable** command displays which protocols that constitute the FIPS policy are set in compliance with FIPS standards by default and can be adjusted to set a more flexible policy. The remaining protocols that constitute the FIPS policy are set to the appropriate status automatically during reload due to the **fips enable** command. The default FIPS policy is detailed in "How FIPS works" section.

When you make no changes to the FIPS policy, the default FIPS policy is applied on the device and the device operates in strict FIPS mode upon reload, in full compliance with FIPS 140-2 specifications.

To set a more flexible FIPS policy on the Brocade device, use the following commands as desired to modify the default FIPS policy.

- Allow TFTP access:

  ```
  Brocade(config)# fips policy allow tftp-access
  ```

  Syntax: **[no] fips policy allow tftp-access**

- Allow SNMP access to the Critical Security Parameter (CSP) MIB objects:

  ```
  Brocade(config)# fips policy allow snmp-csp-access
  ```

  Syntax: **[no] fips policy allow snmp-csp-access**

- Allow access to monitor mode for debugging both from application and from boot prompts:

  ```
  Brocadeconfig)# fips policy allow monitor-full-access
  ```

  Syntax: **[no] fips policy allow monitor-full-access**

  NOTE
  During an application reset, monitor access is restored to allow debugging. Refer to "Access to monitor mode" on page 27.

- Retain the shared secret keys for all protocols and the host passwords:

  ```
  Brocade(config)# fips policy retain shared-secrets
  ```

  Syntax: **[no] fips policy retain shared-secrets**

- Retain the SSH DSA host keys:

  ```
  Brocade(config)# fips policy retain dsa-host-keys
  ```

  Syntax: **[no] fips policy retain dsa-host-keys**

- Retain the HTTPS RSA host keys and the HTTPS Server digital certificate:

  ```
  Brocade(config)# fips policy retain rsa-host-keys
  ```

  Syntax: **[no] fips policy retain rsa-host-keys**

Zeroizing shared secrets and host keys

After you have reviewed the FIPS policy, use the following command to zeroize the shared secrets and host keys used by various networking protocols.

```
Brocade# fips zeroize all
```

Syntax: **[no] fips zeroize all | shared-secret | host-keys**

The **all** option zeroizes all shared secrets and host keys. The **shared-secret** option zeroizes shared secret keys only. The **host-keys** option zeroizes host keys only.

For example, entering the **fips zeroize shared-secret** zeroizes only the shared secret keys of various networking protocols and host access passwords.

NOTE
This command may cause operational failure within networking protocols using shared secrets and should be used with careful consideration.

The default FIPS policy calls for the zeroization of all keys using the **fips zeroize all** command option.When you apply a less strict FIPS policy than the default, zeroize at your discretion.

NOTE
The **fips zeroize all** option zeroizes all keys irrespective of the configured FIPS policy.

Table 4 lists the various keys used in the system that are zeroized in compliance with FIPS.

TABLE 4 Key zeroization

Keys used	Command option handling
DH Private Keys	Host-keys
FCSP Challenge Handshake Authentication Protocol (CHAP) Secret	Host-keys
SSH Session Key	Host-keys
SSH RSA Private Key	Host-keys
RNG Seed key	N/A
Passwords	Shared-secret
TLS Private Key	Host-keys
TLS pre-master secret	Host-keys
TLS session key	Host-keys
TLS authentication key	Host-keys
RADIUS secret	Shared-secret
Authentication passwords for various networking protocols	Shared-secret

Saving the configuration

After zeroizing, use the **write memory** command to save the configuration.

```
Brocade(config)# write memory
```

Syntax: **write memory**

NOTE
Keep a backup copy of the startup configuration in the event of system reset.

Reloading the device

NOTE
Before upgrading to a new image in FIPS mode, ensure that the corresponding signature file is available in the flash.

After you have saved the configuration, reload the device using the **reload** command:

```
Brocade# reload
```

Syntax: **reload**

Various tests, including Power-On Self Tests (POSTs) and Known Answer Tests (KATs), are run by the Brocade device during reload, during the transition between non-FIPS and FIPS mode.

POSTs check for the consistency of the FIPS approved algorithms implemented on the device.

KATs are used to exercise various features of FIPS-approved algorithms.

All interfaces on the device are down until the tests are completed successfully.

Possible POST failure messages indicating that the tests did not pass successfully include:

```
Crypto module initialization and KNown Answer Test (KAT) failed with reason:(Error
Code 0x80000000)’CKR_VENDOR_DEFINED’

FIPS: Primary image verification failed


FIPS: Secondary image verification failed
```

If there is a failure while the POSTs are being run, the device will be rebooted. Monitor mode can be accessed to troubleshoot the issue. For information on access to monitor mode to perform debugging, refer to “Access to monitor mode” on page 27.

After all tests are completed successfully, the device reloads in FIPS mode and FIPS mode is successfully enabled and operational on the Brocade device.

NOTE
Due to FIPS functionality, the device has changed to more secure both in and out of FIPS mode. As a result, boot time is slower upon reload for all FastIron devices release 7.2.01a and later.

You can verify the status of the device as operationally in FIPS mode by using the **fips show** command.

```
Brocade(config)# fips show
```

Syntax: **fips show**

The following is the output of the **fips show** command after the device reloads successfully in the default strict FIPS mode and administrative status is on and operational status is on:

```
Brocade#fips show
Cryptographic Module Version: FIFIPS07300_0314121830
```

```
FIPS mode: Administrative status ON: Operational status ON
Common-Criteria: Administrative status OFF: Operational status OFF
System Specific
OS monitor access status is: Disabled

Management Protocol Specific:
Telnet server: Disabled
Telnet client: Disabled
TFTP client: Disabled
HTTPS SSL 3.0: Disabled
SNMP Access to security objects: Disabled

Critical security Parameter updates across FIPS boundary:
Protocol Shared secret and host passwords: Clear
Password Display: Disabled

HTTPS RSA Host Keys and Signature: Clear
SSH DSA Host keys: Clear
SSH RSA Host keys: Clear
```

Disabling FIPS mode

Use the following command to disable FIPS mode on the Brocade device.

```
Brocade(config)# no fips enable
```

After you enter the command, a warning displays that FIPS mode will be disabled.

This command performs the following policy-related operations:

- Enables TFTP access.
- Re-enables SNMP access to Critical Security Parameter (CSP) MIB objects.
- Re-enables SNMPv3 encryption protocol DES for future SNMPv3 user configuration.
- Re-enables access to monitor mode.
- Zeroizes shared secrets, SSH and HTTPS host keys, and the HTTPS certificate based on the configured FIPS policy.

This command also performs the non-policy-related operation of re-enabling the RC4 cipher for the HTTPS server.

Changes to the running configuration are not saved to the startup configuration; therefore, when the device reloads it returns to FIPS mode.

Use the **write memory** command to save the running configuration.

Running FIPS self-test

Use the following command either in FIPS or non-FIPS mode to run the Known Answer Tests (KATs) and conditional tests on demand in both FIPS and non-FIPS mode:

```
Brocade(config)# fips self-test
```

Syntax: fips self-test

The following log message is only outputted to the console terminal and no trap messages are generated as the system is not fully operational when this event happens:

```
"Crypto module initialization and Known Answer Test (KAT) passed".
```

Access to monitor mode

The device in strict FIPS mode with the default policy applied does not allow access to monitor mode commands that perform memory access.

When the device is operating in FIPS mode, you can access all monitor mode commands, including memory debug commands, in the following instances:

- A flexible FIPS policy with the command **fips policy allow monitor-full-access** configured allows access memory debug commands.
- A strict FIPS policy does not allow access to memory debug commands. To apply a more flexible policy and allow access to all monitor commands, either configure a more flexible FIPS policy or disable FIPS mode to enter monitor mode. Refer to "Accessing monitor mode from FIPS mode" on page 27.

  NOTE
  Making changes to the default FIPS policy on the device is not recommended and weakens the security of the device.

- In the event of continuous reboot or failure on the Brocade device you can access monitor mode to perform troubleshooting. Refer to "Accessing monitor mode in the event of continuous failure" on page 28.

Perform the necessary operations after allowing the device access to the memory debug commands. Refer to "Debugging in monitor mode" on page 28.

To enable FIPS mode on the device after you have completed your use of monitor mode, refer to "Returning to FIPS mode from monitor mode" on page 28.

Accessing monitor mode from FIPS mode

A flexible FIPS policy with the command **fips policy allow monitor-full-access** configured allows access to monitor mode memory debug commands.

When the default FIPS policy is applied and the device is in strict FIPS mode, take the following steps to set a more flexible FIPS policy and allow access to debug commands:

NOTE
Making changes to the default FIPS policy on the device is not recommended and weakens the security of the device. Any modification of the default FIPS policy places the device in a state that is not in compliance with FIPS 140-2.

1. Clear the Critical Security Parameters (CSP). The device zeroizes the CSP based on the configured FIPS zeroization policy. Use the following command.

   ```
   Brocade(config)# fips zeroize all
   ```

   Syntax: [no] fips zeroize all | shared-secret | host-keys

2. Allow access to the restricted memory commands within monitor mode by using the following FIPS policy command.

   ```
   Brocade(config)# fips policy allow monitor-full-access
   ```

   Syntax: **fips policy allow monitor-full-access**

All commands in monitor mode, specifically the previously restricted memory access commands, are available for use. Refer to “Debugging in FIPS mode” on page 19.

If you do not want to apply any FIPS policy but the default and still need to enter monitor mode, disable FIPS mode on the device using the **no fips enable** command. Refer to “Disabling FIPS mode” on page 26.

Once FIPS is disabled, all monitor mode commands are available.

Accessing monitor mode in the event of continuous failure

In the event of continuous failure, enter monitor mode by pressing **b** during a boot cycle. Only a restricted CLI is available in monitor mode if the device was previously running in FIPS mode. This restricted CLI does not allow the use of commands that refer to reading or writing memory location.

If you intend to run the memory access commands, erase the startup configuration file using the command **erase startup-config**.

```
Brocade# erase startup-config
```

Syntax: **erase startup-config**

In this mode, you can download a new image to the device if required.

Debugging in monitor mode

After allowing access to monitor mode, the memory debug commands disabled in strict FIPS mode are available for use.

The monitor mode command set allows you to perform the following actions:

- debug the system reset
- erase the configuration (reset CSPs)
- set an IP address
- boot from TFTP

Returning to FIPS mode from monitor mode

After the necessary actions are performed in monitor mode, take the following steps to return to FIPS mode:

1. Use **Ctrl + Z** during reboot to exit monitor mode and return to the application prompt.
2. Re-create the CSP values.

Use the **fips enable** command to re-enable FIPS mode on the device. Refer to “Enabling FIPS mode” on page 20.

Chapter

4

Common Criteria Certification

NOTE
Common Criteria mode becomes available once a device is FIPS-enabled.

This chapter contains steps for configuring Common Criteria (CC) mode on Brocade devices in compliance with the Common Criteria standards. Because Common Criteria mode enforces security restrictions additional to the FIPS mode, procedures and information are provided in relation to those for the FIPS mode. For information about enabling FIPS mode on the device, see Chapter 3, “FIPS Configuration”.

The Brocade FastIron platforms FSX, FCX, ICX 6430, ICX 6450, ICX 6450-C12, ICX 6650, and ICX 6610 support Common Criteria certification requirements.

Overview

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. These restrictions are in addition to the requirements of the FIPS mode. When the device is placed in the Common Criteria mode, several security features that are available in the FIPS mode are unavailable on the device.

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

You can enable the Common Criteria mode on a device directly from non-FIPS mode, or on a device already in FIPS mode. The following table summarizes the transitions:

TABLE 5 Transition to Common Criteria mode

From	To non-FIPS mode	To FIPS mode	To Common Criteria mode
Non-FIPS mode	Not Applicable	Use the **fips enable** command	Use the **fips enable common-criteria** command
FIPS mode	Use the **no fips enable** command	Not Applicable	Use the **fips enable common-criteria** command
Common Criteria mode	Use the **no fips enable** or **no fips enable common-criteria** command	Use the following commands in a sequence: **no fips enable** **reload device** **fips enable**	Not Applicable

Notice the following:

- Disabling FIPS mode from the Common Criteria mode using the **no fips enable** command downgrades the device directly into non-FIPS mode.

- You cannot directly transition from Common Criteria mode to FIPS mode. To transition to FIPS mode, you should disable FIPS mode, reload the device, and then enable FIPS mode.

Features unavailable in Common Criteria mode

Some of the security features that are allowed in FIPS mode are disabled in Common Criteria mode:

1. **SSHv2:** Host and client key generation methods using DSA and RSA-1024 key size are not supported (Only RSA 2048 and higher key sizes are supported). Therefore, the following commands are not supported:
   - **crypto key generation dsa**
   - **crypto key client generation dsa**
   - **crypto key zero dsa**
   - **crypto key client zero dsa**
   - **crypto key gen rsa modulus 1024**
   - **crypto key zero rsa modulus 1024**
2. **TLS/HTTPS:** RSA 1024 key size for SSL or TLS private key generation is not supported (FastIron devices support only 2048 and above key sizes).
3. **SSH key exchange:** SSH key exchange method `DiffieHellmanGroup1Sha1` is not supported. Only `DiffieHellmanGroup14Sha1` is supported.
4. **Syslog:** Logging to host that uses UDP for transport is not supported. Only TLS host is supported. Therefore, the **logging host [ipv4 | ipv6] <ip-address> | <ipv6-address> udp-port <port>** command is not supported. See "Configuring an encrypted syslog server" on page 35 for more information.
5. **RADIUS**: Authentication using RADIUS is not supported.
6. **Web Management**: Web Management is not supported.

Features available in Common Criteria mode

1. **SSHv2**: Secure Shell is used for secure remote communication and is available with RSA 2048 keys and uses `DiffieHellmanGroup14Sha1`for key exchange. This uses management port to receive and send packets and provides access to the device similar to that provided by remote shell. The login user's privilege level determines the privilege level of access.
2. **Secure Syslog**: Secure syslog feature uses TLS to securely send the log messages to the log server.
3. All services and features that are available in FIPS mode and which are not disallowed by the section "Features unavailable in Common Criteria mode" on page 30, are also available in Common Criteria mode. For more information on these services and features, see the *FastIron Configuration Guides*.

Supported algorithms for SSH Client

An SSH client can connect to a device in Common Criteria mode only with the AES-128 and AES-256 encryption algorithms.

Supported cipher suites

The mandatory cipher suites supported for TLS 1.0 protocol in Common Criteria mode are as follows:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Enabling Common Criteria mode

When you enable Common Criteria mode on the device, it enters the Common Criteria Administrative mode. Similar to FIPS, Common Criteria also has administrative and operational modes:

- **Common Criteria Administrative mode:** Log in to the device console and enable the Common Criteria mode. You can optionally modify the default Common Criteria security policy in this mode.

  NOTE
  When you execute the command to reload the device, the validation of software image with the signature file is triggered. Failure in signature verification results in the device continuously rebooting after device reload.

- **Common Criteria Operational mode:** Transition to Common Criteria Operational mode from Common Criteria Administrative mode. After you transition the device to the Operational mode, you must save the configuration and reboot the device.

Entering the Common Criteria Administrative mode

You can enable Common Criteria mode on a device with the following command:

```
Brocade(config)# fips enable common-criteria
```

Syntax: [no] fips enable common-criteria

The device prompt displays the detailed banner information as follows.

```
Brocade(config)#fips enable common-criteria
This device is now running in CC administrative mode.
At this time you can alter this system's CC default security policy
and then enter CC operational mode.

Note: Making changes to the default policy makes the device non-compliant
with CC and FIPS 140 Level 2. The default security policy defined in the FIPS
Security Policy Document ensures that the device complies with all
FIPS 140-2 specifications. Commands to alter the default security policy
are available to the crypto-officer; however, Brocade does not recommend
making changes to the default security policy at any time.
=====================================

To enter CC mode, complete the following steps:
1. Optionally, configure FIPS policy commands that meets your network
   requirements. You must explicitly configure the following services if you
   want to use them when the device is operational in CC mode:

      - Allow TFTP access.
          Current status: Disabled
      - Allow SNMP Access to the Critical Security Parameter (CSP) MIB objects.
          Current status : Disabled
      - Allow access to all commands within the monitor mode.
          Current status: Disabled
      - Retention of shared secret keys for all protocols and the host passwords.
          Current status: Clear
      - Retention of SSH DSA host keys.
          Current status: Clear
      - Retention the HTTPS RSA host keys and certificate.
          Current status: Clear

2. Enter the "fips zeroize all" command, which zeroes out the shared secrets
    used by various networking protocols, including the host access passwords,
    SSH and HTTPS host-keys with the digital signature based on the configured
    FIPS Security Policy.
3. Save the running configuration.
4. Reload the device.
5. Enter the "fips show" command to verify that the device entered
    FIPS or CC operational mode.
=====================================

The system will disable the following services or commands after reload:
1. Telnet server will be disabled. The "telnet server" command will be removed.
2. SCP will be enabled. The "ip ssh scp disable" command will be removed.
3. HTTP server will be disabled. The "web-management http" command will be
removed.
4. HTTPS server will change as follows:
      -SSL 3.0 will be disabled.
      -TLS version 1.0 and greater will be used.
      -RC4 cipher will be disabled.
      -Passwords will be required; the "web-management allow-no-password"
        command will be removed.
Please see FIPS config guide for complete details.

=====================================
Additionally, in CC mode, the system will disable the following
services or commands after reload:
UDP Syslog servers will be deleted from configuration(only in the CC operational
mode).
DSA keys will be deleted from configuration, and will be disabled .
RSA key sizes will be restricted to 2048 and above in the configuration.
```

Entering the Common Criteria Operational mode

When the device is in the Common Criteria Administrative mode, perform the following steps to place the device into the Common Criteria Operational mode:

1. Configure the local user accounts as secure and delete non-secure user accounts. A local user account is secure when it has password with characters from three or more character classes. These character classes are upper case, lower case, numeric, and ASCII non-alphanumeric characters.

2. Configure secure logging by setting up the encrypted syslog server. For details, see the Appendix A “Configure an encrypted syslog server”.

3. Run the **enable aaa console** command to ensure user authentication during the next reload. This also requires that you have enabled AAA authentication with the **aaa authentication login default** command.
4. Run the **logging cli-command** command. This allows you to log all syntactically valid CLI commands from each user session into the system log.
5. Run the **write memory** command to save the configuration.
6. Reload the device.

On successful completion of the above steps, the device will be in Common Criteria Operational mode.

Displaying Common Criteria information

After you have enabled Common Criteria Administrative mode on the device, you can display the relevant information with the **fips show** command.

```
Brocade#fips show
Cryptographic Module Version: FIFIPS08000_0314121830
FIPS mode: Administrative status ON: Operational status OFF
Common-Criteria: Administrative status ON: Operational status OFF
Some shared secrets inherited from non-fips mode may
    not be fips compliant and has to be zeroized
The system need to be reloaded to operationally enter FIPS mode.
System Specific
OS monitor access status is: Disabled

Management Protocol Specific:
Telnet server: Disabled
Telnet client: Disabled
TFTP client: Disabled
HTTPS SSL 3.0: Disabled
SNMP Access to security objects: Disabled

Critical security Parameter updates across FIPS boundary:
Protocol Shared secret and host passwords: Clear
Password Display: Disabled

HTTPS RSA Host Keys and Signature: Clear
SSH DSA Host keys: Clear
SSH RSA Host keys: Clear
```

After you have enabled Common Criteria operational mode by reloading the device, enter the **fips show** command to verify the operational mode status:

```
Brocade#fips show
Cryptographic Module Version: FIFIPS08000_0314121830
FIPS mode: Administrative status ON: Operational status ON
Common-Criteria: Administrative status ON: Operational status ON
System Specific
OS monitor access status is: Disabled

Management Protocol Specific:
Telnet server: Disabled
Telnet client: Disabled
TFTP client: Disabled
HTTPS SSL 3.0: Disabled
```

```
SNMP Access to security objects: Disabled

Critical security Parameter updates across FIPS boundary:
Protocol Shared secret and host passwords: Clear
Password Display: Disabled

HTTPS RSA Host Keys and Signature: Clear
SSH DSA Host keys: Clear
SSH RSA Host keys: Clear
```

Encrypted syslog servers in Common Criteria mode

FastIron devices in any mode send the generated syslog messages in real time to the local log storage on the device and to a syslog server (only if a syslog server is configured and available).

A FastIron device running in Common Criteria operational mode queues the syslog messages if a syslog server is not available or configured for the device. This queue is not related to the local syslog messages store and it is cleared when the syslog messages in the queue are forwarded to the syslog server. The queue cannot hold more than 3,000 syslog messages. On reaching the maximum message limit, the device displays an error message and no further syslog messages are queued.

FastIron devices, when enabled for Common Criteria mode, do not support syslog servers that use UDP transport. However, other parameters that are defined for syslog server connections, such as specifying the hold time for queued messages and traps when the device reloads or switches over are applicable for encrypted syslog connections as well.

When you enable Common Criteria mode on a device, the device is in the Common Criteria Administrative mode, where syslog server configuration that uses UDP transport is retained. You can configure encrypted syslog server connections in this mode. However, syslog messages that are generated when the device is in the Administrative mode are sent to the UDP syslog servers, not to the encrypted syslog server that you have configured. However, when the device is put in the Common Criteria Operational mode, existing syslog servers that use UDP transport are removed, and only encrypted syslog server connections are accepted.

Conversely, when a device is downgraded from Common Criteria mode, the encrypted syslog server connections that were configured are removed, and the device supports only unencrypted UDP syslog servers. The following table summarizes these transitions:

TABLE 6 Syslog server connections during transition to and from Common Criteria mode

From	To non-FIPS mode	To FIPS mode	To Common Criteria Operational mode
Non-FIPS mode	Not Applicable.	No change. FIPS mode does not support encrypted syslog servers.	All the UDP servers are removed when the device is put in CC Operational mode. Only encrypted syslog server connections are allowed in the CC Operational mode.

TABLE 6 Syslog server connections during transition to and from Common Criteria mode

From	To non-FIPS mode	To FIPS mode	To Common Criteria Operational mode
FIPS mode	No change	Not applicable.	All the UDP servers are removed when the device is put in CC Operational mode. Only encrypted syslog server connections are allowed in the CC Operational mode.
Common Criteria mode	All the SSL servers are removed. Non-FIPS mode does not support encrypted syslog server connections.	Not allowed. You must disable Common Criteria mode to revert to Non-FIPS mode, and then re-enable FIPS mode. FIPS mode does not support encrypted syslog server connections.	Not applicable.

Configuring an encrypted syslog server

You can configure up to six encrypted syslog servers, but only one is active at any time, with the other servers acting as standby. When you add an encrypted syslog server, if there is no active syslog server, a session is established with the configured server. If a new connection is added when an active session exists, a new session with another encrypted syslog server is not attempted.

A new syslog server session is attempted in the following scenarios:

- Current active encrypted syslog server configuration is removed or the SSL connection to the active syslog server is closed
- During a device reload
- During switch over of the management module
- No active syslog server is found when the device sends syslog messages

Attempts to connect to a new syslog server starts with the first configured syslog server. The device attempts to establish an SSL connection with a server until a successful SSL connection is established. During this interval, the trap hold down timer is started and all the syslog messages are queued. When the timer expires, the device sends queued log messages to the connected syslog server.

Refer to Appendix A, “Configure an encrypted syslog server” in this document for configuration examples.

Adding an encrypted syslog server

To configure an encrypted server connection, enter the following command:

```
Brocade(config)# logging host 10.25.105.201 ssl-port 60514
```

Syntax: **logging host [ipv6] <ip-address> | <ipv6-address> ssl-port <port>**

The **ip-address** keyword specifies the syslog server. The **ssl-port** keyword specifies the SSL port that will be used to connect to the specified syslog server.

NOTE
You can configure an encrypted syslog server connection only after the device has been placed in to Common Criteria mode. While you can configure these when the device is in the Administrative mode, the configuration takes effect only after the device is put in the Common Criteria Operational mode.

Displaying the configured server connections

You can display the active encrypted syslog server connection with the **show ip ssl** command:

```
Brocade# show ip ssl
Session   dst address          dst port   src port
1           10.25.105.201        60514      633
```

In addition, you can use the show logging command to display the active SSL-encrypted syslog server along with the logging level information.

```
Brocade# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
    Buffer logging: level ACDMEINW, 27 messages logged
    level code: A=alert C=critical D=debugging M=emergency E=error
                I=informational N=notification W=warning
Current active SSL syslog server: 10.25.105.201:60514
```

Testing TLS cipher suites on a Linux Syslog Server

To test a TLS cipher suite, perform the following steps on the Linux syslog server:

1. Kill all the stunnel process instances.
2. Generate openssl certificate and key.
3. Configure device with the **ssl-port** *port-number* command.
4. Start Wireshark capture.
5. Start the stunnel service using the **openssl** command. For example:

   ```
   #openssl req  -new  -x509  -days  3650  -nodes  -out  /etc/stunnel/stunnel.pem
   -keyout  /etc/stunnel/stunnel.pem
   ```

6. Run one of the following four commands to test one of the four different cipher suites:

   ```
   openssl s_server -accept 60519 -cert
   /usr/local/src/rsyslog-7.4.1/contrib/gnutls/cert.pem
   -key  /usr/local/src/rsyslog-7.4.1/contrib/gnutls/key.pem -cipher
   DHE-RSA-AES128-SHA

   openssl s_server -accept 60519 -cert
   /usr/local/src/rsyslog-7.4.1/contrib/gnutls/cert.pem
   -key  /usr/local/src/rsyslog-7.4.1/contrib/gnutls/key.pem -cipher
   DHE-RSA-AES256-SHA

   openssl s_server -accept 60519 -cert
   /usr/local/src/rsyslog-7.4.1/contrib/gnutls/cert.pem
   -key  /usr/local/src/rsyslog-7.4.1/contrib/gnutls/key.pem -cipher AES128-SHA
   ```

```
openssl s_server -accept 60519 -cert
/usr/local/src/rsyslog-7.4.1/contrib/gnutls/cert.pem
-key  /usr/local/src/rsyslog-7.4.1/contrib/gnutls/key.pem -cipher AES256-SHA
```

7. Perform some action that generates syslog messages on the Brocade device.

The following example shows the successful configuration of a Linux syslog server with the `DHE-RSA-AES128-SHA` cipher suite.

```
Linux-Server# openssl s_server -accept 60519 -cert
/usr/local/src/rsyslog-7.4.1/contrib/gnutls/cert.pem -key
/usr/local/src/rsyslog-7.4.1/contrib/gnutls/key.pem -cipher
DHE-RSA-AES128-SHA

Using default temp DH parameters
Using default temp ECDH parameters
ACCEPT
bad gethostbyaddr
-----BEGIN SSL SESSION PARAMETERS-----
MHUCAQECAgMBBAIAMwQgaSzY5ccUFdf5UO+fRsfbF5pnveVgwVnom+YRP9uC054E
MKYPvnjPfD2T9ymC3hqxWVYssriZWBFkEnpwlbUWS/gBZHHCe3gsA2y+j+Sf/QaG
aaEGAgRSXavPogQCAgEspAYEBAEAAAA=
-----END SSL SESSION PARAMETERS-----
Shared ciphers:AES128-SHA:AES256-SHA:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA
CIPHER is DHE-RSA-AES128-SHA
Secure Renegotiation IS NOT supported
<14>2013 Oct 15 13:55:03 KL-75-CC System: Syslog server 10.20.65.72 added by
test from console session
<14>2013 Oct 15 13:55:03 KL-75-CC CLI CMD: "logging host 10.20.65.72 ssl-port
60519" by test from co
nsole
<14>2013 Oct 15 13:55:10 KL-75-CC System: SSL server 10.20.65.72:60519 is now
connected
<14>2013 Oct 15 13:55:13 KL-75-CC System: SSL server 10.20.65.72:60519 is
disconnected
<14>2013 Oct 15 13:55:44 KL-75-CC System: SSL server 10.20.65.72:60519 is now
connected
<14>2013 Oct 15 13:55:55 KL-75-CC CLI CMD: "show ip" by test from console
<14>2013 Oct 15 13:56:00 KL-75-CC CLI CMD: "show logging" by test from console
<14>2013 Oct 15 13:56:09 KL-75-CC CLI CMD: "show memory" by test from console
<14>2013 Oct 15 13:56:16 KL-75-CC CLI CMD: "show version" by test from console
```

AAA servers in Common Criteria mode

Common Criteria mode requires that devices support NDPP version 1.1. This protocol defines the communication of the device with AAA servers to take place over a TLS-encrypted session.

Even though you can configure multiple TLS-encrypted TACACS+ servers, but only one connection can be active at any time. If another TLS-encrypted TACACS+ session is attempted at the same time as the first TACACS+ session, the connection attempt is rejected.

When the device is in the Common Criteria Operational mode, and the device has been configured for TLS encrypted TACACS+ server for authentication, only one administrator will be able to administer the device. In addition, accounting and authorizing using the TLS-encrypted TACACS+ server will be disabled.

NOTE
You can modify the default Common Criteria policy to allow non-TLS-encrypted TACACS+ server, but this will make the device non-compliant to Common Criteria requirements.

Configuring a TLS-encrypted TACACS+ server

To configure a TACACS+ server connection that uses TLS encryption, enter the following command:

```
Brocade# tacacs-server host 10.25.105.201 ssl-auth-port 2323 authentication-only
```

Syntax: **[no] tacacs-server host** <ip-addr> | <server-name> [{**ssl-auth-port**} <number> [**authentication-only** | **authorization-only** | **accounting-only** | **default**] [**key** <string>]]

The **ssl-auth-port** keyword specifies that the TACACS+ server uses a TLS-encrypted TCP connection.

Even though the command supports adding a TACACS server that uses UDP for transport, for the device to work in Common Criteria mode, you must configure a TLS-encrypted TCP connection. If you do not specify the port number, the default option of **auth-port** (port 49 with no TLS encryption) is used.

Modifying the Common Criteria policies to use non-encrypted AAA servers

If required, you can modify the Common Criteria policies to allow AAA servers that do not use TLS encryption to be configured, such as RADIUS servers. When non-encrypted AAA servers are allowed, you cannot configure TLS-encrypted TACACS+ servers on the device.

NOTE
Modifying the default Common Criteria policy will make the device non-compliant to Common Criteria standards.

To allow any AAA server to work with the device in Common Criteria mode, enter the following command:

```
Brocade# fips policy allow common-criteria aaa-server-any
```

Syntax: **[no] fips policy allow common-criteria aaa-server-any**

Use the **[no]** version of this command to remove non-encrypted AAA servers. If any non-encrypted AAA servers were available on the device, they are removed when Common Criteria mode is enabled on the device.

Downgrading from Common Criteria mode to non-FIPS mode

Downgrading a device from Common Criteria mode to either FIPS or non-FIPS mode uses the same command. You cannot directly downgrade to FIPS mode: you first downgrade to non-FIPS mode, then enable FIPS mode using the procedures detailed in the earlier chapter.

After the device is placed in non-FIPS mode, you can use SCP to download and initialize an older image. Use the following steps to revert to a non-FIPS compliant image:

1. Log on to the device by entering your user name and password.
2. Disable Common Criteria mode by entering the **no fips enable** command at the prompt.
3. Regenerate SSH host keys or other shared secrets as needed for access after reload.
4. To replace the startup configuration with the **no fips enable** configuration, enter the **write memory** command.

   ```
   Brocade# write memory
   ```

5. Reload the configuration by entering the **reload** command.

logging cli-command

Enables logging of all syntactically valid CLI commands from each user session into the system log.

Syntax

logging cli-command

no logging cli-command

Parameters

None

Command Modes

Global configuration mode

Examples

You can enable logging of CLI commands on the device as follows:

```
Brocade(config)# logging cli-command
```

The following example shows a valid command that is executed successfully on the CLI and the corresponding system log.

```
Brocade(config)#interface ethernet 1/1

SYSLOG: <14>8d02h28m16s   : Brocade CLI CMD: "interface ethernet 1/1" by
un-authenticated user from console
```

The following example shows a valid command that throws an error and the corresponding system log.

```
Brocade (config)#ip route 0.0.0.0/0 10.20.64.1
Error - Conflicting static route entry!

SYSLOG: <14>8d02h28m43s   : Brocade CLI CMD: "ip route 0.0.0.0 0.0.0.0 10.20.64.1"
by un-authenticated user from console
```

To view the system log records, you can run the **show log** command as follows:

```
Brocade (config)#show log
Syslog logging: enabled (0 messages dropped, 0 flushes, 5 overruns)
    Buffer logging: level ACDMEINW, 50 messages logged
    level code: A=alert C=critical D=debugging M=emergency E=error
                I=informational N=notification W=warning

Dynamic Log Buffer (50 lines):
8d02h28m43s:I:CLI CMD: "ip route 0.0.0.0 0.0.0.0 10.20.64.1" by un-authenticated
user from console
8d02h28m24s:I:System: Interface ethernet 1/1, state up
8d02h28m22s:I:CLI CMD: "enable" by un-authenticated user from console
8d02h28m22s:I:PORT: 1/1 enabled by un-authenticated user from console session
8d02h28m19s:I:CLI CMD: "disable" by un-authenticated user from console
8d02h28m19s:I:PORT: 1/1 disabled by un-authenticated user from console session
8d02h28m16s:I:CLI CMD: "interface ethernet 1/1" by un-authenticated user from
console
```

Related Commands

show log

Appendix

Configure an encrypted syslog server A

The information available in this appendix is a representative configuration example of the many types of Syslog servers available. It describes how to setup an encrypted syslog server running on Ubuntu 10.4. The setup procedure for encrypted syslog server on other Linux operating systems such as Red Hat or Centos is the same as mentioned in this document except for difference in commands.

You will need to set up stunnel as a server and client in your server. As a server, stunnel listens on port 60516 to connections from its client peers, and all connections are forwarded to the locally-running rsyslog listening at port 61514. As a client, rsyslog forwards message to stunnel local portal at port 61514, and local stunnel forwards data via the network to port 60514 to its remote peer.

Set up stunnel

1. Install the stunnel utility with the following command:

   ```
   $ sudo apt-get install stunnel4
   ```

2. Edit the file with path `/etc/default/stunnel4` to start the service on system startup. Use an editor such as vi.

   ```
   $ sudo vi /etc/default/stunnel4
   ```

3. Change the line `Enabled=0` to `Enabled=1`.

Create a certificate with the openssl tool

1. Enter the following command:

   ```
   cd /etc/stunnel
   ```

2. Enter the following command to create the `/etc/stunnel/stunnel.pem` file with certificate and key for SSL:

   ```
   $openssl req -new -x509 -days 365 -nodes -out stunnel.pem -keyout
    /etc/stunnel/stunnel.pem
   ```

3. Enter the following command to change the permissions for the certificate that you generated.

   ```
   $ sudo chmod 600 /etc/stunnel/stunnel.pem
   ```

Create a configuration file

1. Enter the following command to open the stunnel.conf file:

   ```
   $sudo vi /etc/stunnel/stunnel.conf
   ```

2. Comment out the features that you don't require, such as [pop3s], [ssmtp], and [imaps] sections.

3. Change the line `cert=/etc/stunnel/mail.pem` to `cert=/etc/stunnel/stunnel.pem`.
4. Add the following lines and save the file.

```
; Certificate/key is needed in server mode
cert = /etc/stunnel/stunnel.pem
key = /etc/stunnel/stunnel.pem

; Some debugging stuff useful for troubleshooting
debug = 7
foreground=yes

[ssyslog]
accept  = 60514
connect = 61514
```

Change the stunnel4 startup file

1. Enter the command `cd /etc/init.d/stunnel4` and change `ENABLED=0` to `ENABLED=1`.

Restart the stunnel service

1. Enter the following command:

```
$sudo  /etc/init.d/stunnel4 restart
```

Configure rsyslog

Ubuntu 10.04.3 comes with Rsyslog 4.2.0 as its default logger. You can add MySQL output support and the Reliable Event Logging Protocol (RELP). Enter the following command:

```
root@linux:~$sudo apt-get install rsyslog-mysql rsyslog-relp
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  dbconfig-common librelp0
The following NEW packages will be installed:
  dbconfig-common librelp0 rsyslog-mysql rsyslog-relp
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 677kB of archives.
After this operation, 2,335kB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

During the installation process, do the following:

1. Create the tables that are needed in MySQL when prompted.
2. Set the MySQL root password
3. Create a password that the rsyslog processes will use in its configuration files.

Enable accepting remote logs

To turn on accepting remote logs, edit the `/etc/rsyslog.conf` file by commenting out the following lines:

```
# provides TCP syslog reception
```

```
$ModLoad imtcp
$InputTCPServerRun 61514
```

Restart rsyslog service

Enter the following command:

```
root@linux:~$sudo service rsyslog restart
```

NOTE
It is recommended to reboot the Linux server after the setup.

Print log messages

Enter the following command to update the log-watcher window with logged messages as they arrive.

```
root@linux:~$tail  -f  /var/log/messages
```

You can also configure a web UI to display the syslog messages using the Reliable Event Logging Protocol (RELP). See http://www.linuxjournal.com/content/centralized-logging-web-interface for more information.

TLS encrypted syslog server configuration and validation

Certificates (both Server and Trusted) will need to meet the following criteria.

- Only RSA certificates is accepted.
- Public Key should be greater than or equal to 2048 bits.
- The device should have server certificate installed.
- Expired certificate is not accepted.
- A certificate with an empty Subject Alternative Name (SAN) field is rejected.
- When the server’s certificate signature is invalid, the client rejects a certificate based on the public key provided in the issuer's self-signed certificate.
- A certificate with a mismatching Subject Alternative Name (SAN) IP address field is rejected.
- Correct cipher suites.

In common criteria mode, when FastIron device acts as a TLS client while connecting to a remote server, the client needs to perform validation of the server certificate.

1. Create the TLS encrypted syslog server's private key using the **openssl genrsa** command.

```
    openssl genrsa -out rsakey2048.pem 2048
    Generating RSA private key, 2048 bit long modulus
    ..+++
    ..........................................................+++
e is 65537 (0x10001)
```

2. Create the TLS encrypted syslog server's self-signed certificate, also including the IP address of the server in the Subject Alternative Name (SAN) extension of the certificate.

a. Create a configuration file which looks like the following.

```
cat req_san.config.txt

[ req ]
default_bits                     = 2048                 # Size of keys
default_keyfile                 = key.pem             # name of generated keys
default_md                     = sha256                              # message
digest algorithm
string_mask                      = nombstr              # permitted characters
distinguished_name               = req_distinguished_name
req_extensions                   = v3_req

[ req_distinguished_name ]
# Variable name                  Prompt string
#-------------------------        ----------------------------------
0.organizationName               = Organization Name (company)
organizationalUnitName           = Organizational Unit Name (department,
division)
emailAddress                     = Email Address
emailAddress_max                 = 40
localityName                     = Locality Name (city, district)
stateOrProvinceName              = State or Province Name (full name)
countryName                      = Country Name (2 letter code)
countryName_min                  = 2
countryName_max                  = 2
commonName                       = Common Name (hostname, IP, or your name)
commonName_max                   = 64

[ v3_req ]
basicConstraints                 = CA:FALSE
subjectKeyIdentifier             = hash

[ extensions_section ]
subjectAltName=IP:192.168.10.201
```

b. Create the certificate giving the configuration file created in the previous step as parameter.

```
openssl req -new -x509 -key rsakey2048.pem -out
rsacert2048_days1095_sha256_SAN.pem -days 1095 -sha256 -config
./req_san.config.txt -extensions extensions_section

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Organization Name (company) []:Brocade
Organizational Unit Name (department, division) []:Engineering
Email Address []:
Locality Name (city, district) []:San Jose
State or Province Name (full name) []:California
Country Name (2 letter code) []:US
Common Name (hostname, IP, or your name) []:SP_EMIS TLS Encrypted SYSLOG
server
```

c. To view the TLS encrypted syslog server's self-signed certificate that is created:

```
openssl x509 -inform PEM -noout -text -in rsacert2048_days1095_sha256_SAN.pem

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            f9:aa:bd:da:1b:5a:3e:51
        Signature Algorithm: sha256WithRSAEncryption
       Issuer: O=XYZ, OU=ABC, L=San Jose, ST=California, C=US, CN=SP_EMIS TLS
Encrypted SYSLOG server
        Validity
            Not Before: Mar 31 22:20:47 2014 GMT
            Not After : Mar 30 22:20:47 2017 GMT
       Subject: O=XYZ, OU=ABC, L=San Jose, ST=California, C=US, CN=SP_EMIS TLS
Encrypted SYSLOG server
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ca:5f:78:de:07:b7:15:21:b4:9d:e9:66:b7:5e:
                    48:8b:96:ed:4b:f3:5d:dc:d7:95:27:ed:ca:1d:00:
                    9d:d6:06:5b:f5:df:d2:0c:54:69:53:4a:38:d1:52:
                    2d:bf:6c:a4:2b:7d:dd:ad:e7:2c:5a:4f:1c:0e:8b:
                    59:7a:04:f1:54:b8:00:99:51:21:f7:42:81:17:4c:
                    cc:94:86:00:8b:c6:c0:0d:3b:7a:19:66:3c:e5:33:
                    be:5f:b5:2c:d9:df:74:1c:07:f5:41:82:c0:b2:48:
                    9e:c3:7b:cc:2e:07:4e:d8:2a:17:69:48:ae:f2:97:
                    4a:fd:7e:4b:34:2d:36:49:bb:3a:79:c6:c4:9c:1e:
                    5f:1b:d7:59:a0:3e:27:02:2f:2b:eb:60:26:95:20:
                    bb:2a:e8:5b:9b:56:b6:2e:62:eb:a1:21:f4:95:1c:
                    e1:d6:ca:4e:74:0a:a1:6a:f6:b0:27:7f:f4:e2:d2:
                    92:f9:db:25:49:9f:c1:87:d3:ed:1f:d1:98:6c:da:
                    15:04:c1:bb:16:66:78:02:ab:81:a0:98:c2:62:75:
                    b1:4e:96:0a:fd:25:84:64:f3:e6:35:5e:06:05:79:
                    c6:83:73:d6:33:6b:57:64:ad:4d:b5:f4:3d:f6:e7:
                    e5:a3:71:d0:c9:e5:77:7a:4a:11:c0:89:ca:1a:35:
                    72:df
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                IP Address:192.168.10.201
    Signature Algorithm: sha256WithRSAEncryption
        88:a5:6c:d3:15:c2:10:20:c9:36:73:ba:c5:72:4c:e4:26:78:
        dc:ec:21:a2:2b:ec:4b:5a:42:85:be:fe:c4:1f:01:97:f0:5c:
        e2:51:1a:3b:84:15:c9:cb:63:35:b1:e6:b8:3e:2a:76:47:5f:
        ce:1b:59:80:43:81:95:b8:aa:1b:11:7f:80:6f:3f:97:d9:0c:
        43:7e:53:b0:04:80:be:52:da:4b:0b:b4:70:07:a8:b6:d8:09:
        55:9f:4e:08:7a:c1:df:7e:da:dd:c0:59:f3:9d:c6:f5:2b:ec:
        66:89:9e:c9:5f:6c:d1:e7:fe:1e:d3:b1:6e:9f:84:3c:fb:ed:
        e5:c9:2c:7f:8c:85:f4:97:bb:99:3c:cd:1e:3e:d2:a1:6e:09:
        3a:05:b6:c1:76:b9:54:ec:34:a8:a9:6f:ca:30:34:cb:ec:05:
        5d:17:a3:cb:21:3a:69:e3:7d:28:d2:15:c0:19:0e:34:00:8d:
        68:ce:cd:0a:65:db:e4:88:b6:d1:67:40:3a:3d:22:bf:dc:22:
        16:ec:4f:08:a7:54:7f:42:73:9b:f7:88:1a:70:73:8c:81:a8:
        5c:b4:55:5f:7e:94:75:ec:93:f0:48:08:18:4a:3c:ea:c6:6b:
        48:d6:b2:f4:ff:de:23:df:d5:fd:a0:bd:8a:cb:c7:69:f9:3a:
        d9:5f:c5:0f
```

3. Upload the self-signed certificate to the FastIron device. Verify the certificate after upload, using either the signature or the fingerprint of the certificate.

```
scp rsacert2048_256_days1095_SAN.pem lab1@192.168.105.82:ssltrustedcert

lab1@192.168.105.82's password:
rsacert2048_256_days1095_SAN.pem              100% 1448     1.4KB/s   00:00
Connection to 192.168.105.82 closed by remote host.
```

The SCP command can be executed from a remote system (like Linux or Windows). Use the **ssltrustedcert** option to upload a trusted certificate (certificate.pem) to the FastIron device specified by the IP Address as user.

The device can have up to three dynamic trusted certificates. Once three dynamic trusted certificates are uploaded, running the command again will return an error.

To display the list of dynamic trusted certificates on the device, use the **show ip ssl certificate** CLI described in the previous section.

To delete the dynamic trusted certificate list on the device, use an empty certificate file. Following is an example of deleting the dynamic trusted certificate list:

```
> ls -la empty.file
ls: empty.file: No such file or directory
> empty.file
> ls -la empty.file
-rw-r--r-- 1 lab engr 0 Mar 31 12:47 empty.file
> scp empty.file lab@192.168.10.82:ssltrustedcert
```

4. Verify the certificate after upload to the device, using either the signature or the fingerprint of the certificate.

   The **show ip ssl certificate** command displays the dynamic trusted certificate list. The dynamic trusted certificate list can be modified by the **scp ssltrustedcert** command.

```
Device# show ip ssl certificate

No SSL sessions in use.
Trusted Certificates:
 Dynamic:
  Signature Algorithm: sha256WithRSAEncryption
  Validity:
   Not Before: Mar 31 2014 13:22:47
   Not After : Mar 30 2017 13:22:47
  X509v3 extensions:
   X509v3 Subject Alternative Name:
    IP Address:192.168.10.201
  Signature:
    88:a5:6c:d3:15:c2:10:20:c9:36:73:ba:c5:72:4c:e4:26:78:
    dc:ec:21:a2:2b:ec:4b:5a:42:85:be:fe:c4:1f:01:97:f0:5c:
    e2:51:1a:3b:84:15:c9:cb:63:35:b1:e6:b8:3e:2a:76:47:5f:
    ce:1b:59:80:43:81:95:b8:aa:1b:11:7f:80:6f:3f:97:d9:0c:
    43:7e:53:b0:04:80:be:52:da:4b:0b:b4:70:07:a8:b6:d8:09:
    55:9f:4e:08:7a:c1:df:7e:da:dd:c0:59:f3:9d:c6:f5:2b:ec:
    66:89:9e:c9:5f:6c:d1:e7:fe:1e:d3:b1:6e:9f:84:3c:fb:ed:
    e5:c9:2c:7f:8c:85:f4:97:bb:99:3c:cd:1e:3e:d2:a1:6e:09:
    3a:05:b6:c1:76:b9:54:ec:34:a8:a9:6f:ca:30:34:cb:ec:05:
    5d:17:a3:cb:21:3a:69:e3:7d:28:d2:15:c0:19:0e:34:00:8d:
    68:ce:cd:0a:65:db:e4:88:b6:d1:67:40:3a:3d:22:bf:dc:22:
    16:ec:4f:08:a7:54:7f:42:73:9b:f7:88:1a:70:73:8c:81:a8:
    5c:b4:55:5f:7e:94:75:ec:93:f0:48:08:18:4a:3c:ea:c6:6b:
    48:d6:b2:f4:ff:de:23:df:d5:fd:a0:bd:8a:cb:c7:69:f9:3a:
    d9:5f:c5:0f
```

5. Configure the TLS encrypted syslog server with the server private key, and certificate. The following example shows the successful configuration of a Linux syslog server with the DHE-RSA-AES256-SHA cipher.

   ```
   openssl s_server -accept 60892 -cert rsacert2048_256_days1095_SAN.pem -key
   rsakey2048.pem -cipher DHE-RSA-AES256-SHA

   Using default temp DH parameters
   Using default temp ECDH parameters
   ACCEPT
   -----BEGIN SSL SESSION PARAMETERS-----
   MHUCAQECAgMBBAIAOQQgw8qyfvnc6W0z65juN+RuUeurjFO3qVuNXTMDQPdAGdwE
   MI6hWek1E/a69dWIJ6VImumyQTTuv90P+8AzwIpb2JHc3MWliE0qZJ6wsFg4jvDQ
   Y6EGAgRSXsY3ogQCAgEspAYEBAEAAAA=
   -----END SSL SESSION PARAMETERS-----
   Shared ciphers:AES128-SHA:AES256-SHA:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA
   CIPHER is DHE-RSA-AES256-SHA
   Secure Renegotiation IS NOT supported
   <14>Mar 31 2014 14:58:57 XM82 FIPS mode enabled by operator from console
   <14>Mar 31 2014 14:58:57 XM82 CLI CMD: "fips enable common-criteria" from
   console
   ```

6. Configure the FastIron device with the IP address of the TLS encrypted syslog server.

   ```
   logging host 192.158.105.82 ssl-port 60892
   ```

   NOTE
   The port number should be the same as used in the **openssl s_server** command in step 5.

Appendix

Syslog messages

B

The following table lists some of the syslog messages in FIPS mode.

TABLE 7 FIPS syslog messages

Message level	Message	Explanation
Alert	Time is updated by NTP server *ip-address* from NO_CLOCK to <*new time*> GMT+00 <*new date*>	Indicates time is updated by an NTP server.
Alert	Clock Changed from old time <*old time*> GMT+00 <*old date*> to new time <*new time*> GMT+00 <*new date*>	Indicates time is updated using the **clock set** command.
Informational	SSH login by *user* from src IP *ip-address*, src MAC *mac-address* to USER EXEC mode using RSA as Server Host Key.	Indicates entry into the "user exec" mode for all sessions for the mentioned user. Similar message is logged for “privileged exec” mode.
Informational	SSH logout by *user* from src IP *ip-address*, src MAC *mac-address* from USER EXEC mode using RSA as Server Host Key.	Indicates exit from "user exec" mode for all sessions for the mentioned user. Similar message is logged for “privileged exec” mode.
Informational	SSH session for *user* from src IP *ip-address*, MAC *mac-address* in PRIVILEGED EXEC mode has timed out.	Indicates SSH logout has occurred due to timeout. Similar message is logged for “user exec” mode.
Informational	SSH session closed by *user* from src IP *ip-address*, MAC *mac-address* in PRIVILEGED EXEC mode.	Indicates SSH logout has occurred due to termination. Similar message is logged for “user exec” mode.
Informational	SSH session killed for user src IP *ip-address*, MAC *mac-address* in PRIVILEGED EXEC mode.	Indicates SSH logout has occurred because the session was killed.
Informational	Super user login success in console session.	Indicates user has logged in with super user password.
Informational	Logging CLI_CMD operation enabled by *user* from console session. "logging cli-command" by *user* from console.	Indicates audit log command "logging cli-command" is enabled.
Informational	Logging CLI_CMD operation disabled by *user* from console session.	Indicates audit log command "logging cli-command" is disabled.
Informational	"reload" by un-authenticated user from console	Indicates initiation of device reload through console.
Informational	SSL Syslog server *ip-address:portnum* is now connected.	Indicates encrypted syslog server is connected in the server end.
Informational	SSL Syslog server *ip-address:portnum* is now disconnected.	Indicates encrypted syslog server is disconnected in the server end.

TABLE 7 FIPS syslog messages (Continued)

Message level	Message	Explanation
Informational	SSH login by *user* from src IP *ip-address* from src MAC *mac-address* to USER EXEC mode using RSA as Server Host Key. Brocade scp -t file: secondary.sig Brocade transfer to device completed SSH logout by *user* from src IP *ip-address* from src MAC *mac-address* from USER EXEC mode using RSA as Server Host Key.	Indicates SCP transfer.
Informational	*yyyy month dd hh:mm:ss*	The year is always displayed in the four digit yyyy format.
Informational	Error - Incorrect username or password in console session.	Indicates incorrect username or password.
Informational	Brocade(config)#wr m Message: "write memory" by *user* from console.	Audit log will display the commands in expanded form.
Informational	console login by *user* to USER EXEC mode.	Displays all "login" events including the user and session details. Similar message is logged for “logout” events and “privileged exec” mode.

Appendix

C

Running Tasks

The following tables list the running tasks for different FastIron devices in FIPS mode.

TABLE 8 List of ICX 6430 / ICX 6450 tasks

Task Name	Priority	Description
SigHdlrTsk	-20	Signal handler task
OsTsk	21	OS task
TimerTsk	-20	Timer task
FlashTsk	21	Flash task
MainTsk	21	Main task
MportPollTsk	-19	Management Poll Task
IntrTsk	-20	Interrupt task
stkKeepAliveTsk	-19	Keep Alive task for stack
keygen	32	Key generation task
itc	-18	ITC task
poeFwdfsm	-19	POE FW download task
scp	-18	SCP task
appl	21	Application task
snms	31	SNMS task
snmp	31	SNMP task
rmon	31	RMON task
web	31	Web task
acl	26	ACL task
ntp	31	NTP task
rconsole	21	RCONSOLE task
console	21	Console task
auxTsk	35	Auxiliary task
syscmd-handler	NA	syscommand handler

TABLE 9 List of FastIron SXL tasks

Task Name	Priority	Description
SigHdlrTsk	-20	Signal handler task
OsTsk	21	OS task

TABLE 9 List of FastIron SXL tasks (Continued)

Task Name	Priority	Description
TimerTsk	-20	Timer task
FlashTsk	21	Flash task
MainTsk	-18	Main task
HbtTsk	-18	Heart beat task
MportPollTsk	-19	Management Poll Task
IntrTsk	-20	Interrupt task
msgTask	21	Message receive Task
hSync	21	Hitless sync task
auxTsk	26	Auxiliary task
ipc_rx	-17	IPC receive task
ipc_tx	-17	IPC transmit task
keygen	32	Key generation task
itc	-18	ITC task
poeFwdfsm	35	POE FW download task
scp	-18	SCP task
appl	21	Application task
snms	31	SNMS task
rtm	26	RTM task
rtm6	26	RTM v6 task
rip	26	RIP task
bgp	26	BGP task
bgp_io	26	BGP IO Task
ospf	26	OSPF task
ospf_r_calc	26	OSPF Route calculation task
mcast_fwd	26	Multicast ITC application task
mcast	26	Multicast task
msdp	26	MSDP task
ripng	26	RIPNG task
ospf6	26	OSPFv6 task
ospf6_rt	26	OSPFv6 Route calculation task
mcast6	26	Multicast v6 task
ipsec	26	IPSec task
snmp	31	SNMP task
rmon	31	RMON task
web	31	Web task
acl	26	ACL task

TABLE 9 List of FastIron SXL tasks (Continued)

Task Name	Priority	Description
ntp	31	NTP task
console	21	Console task
ospf_msg_task	25	OSPF message task
hswap	21	Hot swap task
syscmd-handler	NA	syscommand handler

TABLE 10 List of FCX/ICX 6610 tasks

Task Name	Priority	Description
$(idle)	0	Idle task
$con	27	Console task
$mon	31	Monitor task
$flash	20	Flash task
$dbg	30	Debug task
$boot	29	Boot task
main	3	Main task
stkKeepAliveTsk	15	Keep Alive task for stack
keygen	4	Key generation task
itc	6	ITC task
poeFwdfsm	1	POE FW download task
tmr	8	Timer task
scp	6	SCP task
appl	7	Application task
snms	5	SNMS task
rtm	5	RTM task
rtm6	5	RTM v6 task
rip	5	RIP task
bgp	5	BGP task
bgp_io	5	BGP IO task

TABLE 11 List of ICX 6650 tasks

Task Name	Priority	Description
SigHdlrTsk	-20	Signal handler task
OsTsk	21	OS task

TABLE 11 List of ICX 6650 tasks (Continued)

Task Name	Priority	Description
TimerTsk	-20	Timer task
FlashTsk	21	Flash task
MainTsk	21	Main task
MportPollTsk	-19	Management Poll Task
IntrTsk	-20	Interrupt task
stkKeepAliveTsk	-19	Keep Alive task for stack
keygen	32	Key generation task
itc	-18	ITC task
poeFwdfsm	-19	POE FW download task
scp	-18	SCP task
appl	21	Application task
snms	31	SNMS task
snmp	*31*	SNMP task
rmon	31	RMON task
web	31	Web task
acl	26	ACL task
ntp	31	NTP task
rconsole	21	RCONSOLE task
console	21	Console task
auxTsk	35	Auxiliary task
syscmd-handler	NA	syscommand handler
rtm	26	RTM task
rtm6	26	RTM v6 task
rip	26	RIP task
bgp	26	BGP task
bgp_io	26	BGP IO task
ospf	26	OSPF task
ospf_r_calc	26	OSPF Route calculation task
mcast_fwd	26	Multicast ITC application task
mcast	26	Multicast task
msdp	26	MSDP task
ripng	26	RIPNG task
ospf6	26	OSPF v6 task
ospf6_rt	26	OSPF v6 Route calculation task
mcast6	26	Multicast v6 task
ipsec	26	IPSec task

TABLE 11 List of ICX 6650 tasks (Continued)

Task Name	Priority	Description
ospf_msg_task	25	OSPF message task
ssl	31	SSL task