Brocade® FCX L2/L3 Switch and Brocade FastIron® SX Series L2/L3 Switch

FIPS 140-2 Non-Proprietary Security Policy

Level 2 with Design Assurance Level 3 Validation

Document Version 1.8

April 10, 2014

Revision History

Revision Date	Revision	Summary of Changes
10/15/2012	0.1	Initial draft version
10/25/2012	0.2	Updated Table 17 Access Control Policy and CSP access. Updated the title. Changed protocols to methods in the statement under Table 18. Updated the naming convention for the firmware release. Removed the reference to SSL RSA key
12/12/2012	1.0	Updated the DRBG Entropy and DRBG V and C zeroization method and how the DSA Public Key is over written in section 5.3.1. Restructured the SX and FCX part number tables
3/21/2013	1.1	Added the FCX648S-HPOE SKU to Table 5 FCX Part Numbers, Table 13 FastIron FCX Series Physical Ports and Appendix A. Updated DRBG zeroization statement in section 5.3.1.
3/5/14	1.6	Changed RSA/DSA/DH to be noncompliant per 800-131a
3/20/14	1.7	Updated note under table 24 to clarify details on RSA and DSA non-compliancy. Moved SSH, HTTPS, SCP in sections 4.1, 4.2, and 4.3 as unsupported service as listed in section 4.4 Non-FIPS mode services
4/10/14	1.8	Added entries for NIST in table 20 and section 5.1.1

© 2014 Brocade Communications Systems, Inc. All Rights Reserved.

This Brocade Communications Systems Security Policy for Brocade FCX and FastIron SX L2/L3 switches embodies Brocade Communications Systems' confidential and proprietary intellectual property. Brocade Systems retains all title and ownership in the Specification, including any revisions.

This Specification is supplied AS IS and may be reproduced only in its original entirety [without revision]. Brocade Communications Systems makes no warranty, either express or implied, as to the use, operation, condition, or performance of the specification, and any unintended consequence it may on the user environment.

Table of Contents

Table of Tables

Table of Figures

1. Introduction

The Brocade FastIron SX and Brocade FCX switches are part of Brocade's FastIron L2/L3 switch family. They are designed for medium to large enterprise backbones. The FastIron SX series chassis devices are modular switches that provide the enterprise network with a complete end-to-end Enterprise LAN solution, ranging from the wiring closet to the LAN backbone. The FCX series is an access layer Gigabit Ethernet switch designed from the ground up for the enterprise data center environment. When these switches are stacked, they appear as one switch, reducing management up to 8 times.

2. Overview

Each Brocade FastIron device is a switch, which is a multi-chip standalone cryptographic module. Each device has an opaque enclosure with tamper detection tape for detecting any unauthorized physical access to the device. The power supplies and fan tray assemblies are part of the cryptographic boundary and can be replaced in the field. Unpopulated power supplies and fan trays are covered by opaque bezels, which are part of the cryptographic boundary when the secondary redundant power supplies and/or fans trays are not used. Within the FastIron family, the FastIron SX series is chassis based while FCX series are fixed-port devices.

2.1 FastIron SX series

Table 1 Firmware Version

Firmware
IronWare Release R07.3.00c

Each FI-SX800-S, FI-SX1600-AC and FI-SX1600-DC device validated within this implementation includes the following SX modules: SX-FISF and SX-FIZMR or SX-FI2XGMR6

Table 2 FastIron SX Part Numbers

SKU	MFG Part Number	Brief Description
FI-SX800-S	80-1003050-03	FastIron SX800 CHASSIS
FI-SX1600-AC	80-1002764-02	FastIron SX1600, 16 slot, 2 SX-FISF, 2 AC Power Supplies
FI-SX1600-DC	80-1003005-02	FastIron SX1600, 16 slot, 2 SX-FISF, 2 DC Power Supplies

Table 3 Components of the SX 800 and SX 1600

SKU	MFG Part Number	Brief Description
SX-FISF	80-1002957-03	Switch Fabric module for the FI SX800 & FI SX1600
SX-FIZMR	80-1002955-05	M3 management module for the FI SX800 & FI SX1600
SX-FI2XGMR6	80-1002961-06	M4 (IPv6) 2-Port 10 GbE for the FI SX800 & FI SX1600

Figure 1 illustrates the FI-SX800 cryptographic module.

Figure 1 FI-SX800 cryptographic module

Figure 2 illustrates the FI-SX1600 cryptographic module.

Figure 2 FI-SX1600 cryptographic module

2.2 Brocade FCX series

Brocade FCX series devices are fixed-port devices. FCX supports stacking and multiple FCX devices can be stacked into a single logical switch using stacking ports. The cryptographic boundary of a FCX series device is the entire unit. Each FCX 624 and FCX 648 device validated within this implementation includes an FCX-2XG module.

Table 4 Firmware Version

Firmware
IronWare Release R07.3.00c

Table 5 FCX Part Numbers

SKU	MFG Part Number	Brief Description
FCX624S	80-1002388-07	24-Port 1GbE, 2X16G stackable switch
FCX624S-HPOE-ADV	80-1002715-07	24-Port 1GbE, HPOE, 2X16G stackable, ADV L3 switch
FCX624S-F-ADV	80-1002727-05	24-Port, FE/GE SFP, 2X16G stackable, ADV L3 switch
FCX648S	80-1002392-07	48-Port 1GbE, 2X16 stackable switch
FCX648S-HPOE	80-1002391-09	48-Port 1GbE, HPOE, 2x16G stackable switch
FCX648S-HPOE-ADV	80-1002716-09	48-Port 1GbE, HPOE, 2x16G stackable, ADV L3 switch

Table 6 FCX 624 and FCX 628 Optional Component Part Numbers

SKU	MFG Part Number	Brief Description
FCX-2XG	80-1002399-01	XFP Module,Uplink,2X10G,FCX

Figure 3 illustrates the FCX624S cryptographic module.

Figure 3 FCX624S cryptographic module

Figure 4 illustrates the FCX624S-HPOE-ADV cryptographic module.

Figure 4 FCX624S-HPOE-ADV cryptographic module

Figure 5 illustrates the FCX648S cryptographic module.

Figure 5 FCX648S cryptographic module

Figure 6 illustrates the FCX648S-HPOE and FCX648S-HPOE-ADV cryptographic module.

Figure 6 FCX648S-HPOE and FCX648-HPOE-ADV cryptographic module

Figure 7 illustrates the FCX624S-F-ADV cryptographic module.

Figure 7 FCX624S-F-ADV cryptographic module

2.3 Ports and Interfaces

Each FastIron device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces they provide for Data Input, Data Output, Control Input, and Control Output.

Though not part of this validation, the Brocade FastIron devices provide a range of physical network ports. The family supports both copper and fiber connectors with some models supporting combination ports. Some models support uplink ports for stacking devices. Most models have an out-of-band management port and a console management port (Gigabit Ethernet RJ-45 connector and serial connector, respectively).

2.3.1 SX Management Cards

The SX 800 and SX 1600, SX-FIZMR, management module provides the physical ports listed below

- EIA/TIA-232 Serial port for a console terminal
- 10/100/1000 Mbps Ethernet port for out-of-band management.

The SX 800 and SX 1600, SX-FI2XGMR6, management module provides the physical ports and status indicators listed below

- EIA/TIA-232 Serial port for a console terminal,
- 10/100/1000 Mbps Ethernet port for out-of-band management.
- Two 10-Gbe ports

See the Management Modules section within the FastIron hardware installation guide [53-1002219-02] for detailed descriptions of management card ports and status indicators.

2.3.2 Brocade FastIron FCX 624 and FCX 648 Series

Models in the Brocade FastIron FCX 624 and FCX 648 series provide either 24 or 48 Gigabit Ethernet ports. The series supports both copper and fiber connecters with some models supporting combination ports. Some models support 10 Gigabit Ethernet uplink ports. All models have an out-of-band Ethernet management port and a console management port (Gigabit Ethernet RJ-45 connector and serial connector, respectively).

See [53-1002220-01] section *Hardware features* for detailed descriptions of network ports (including combination ports), management ports, and status indicators provided by each model.

2.3.3 Interfaces

Table 7 shows the correspondence between the physical interfaces of FCX and SX devices and logical interfaces defined in FIPS 140-2.

Table 7 Physical/Logical Interface Correspondence

Physical Interface	Logical Interface
Networking ports	Data input
Console	
Networking ports	Data output
Console	
Networking ports	Control input
Console	
Networking ports	Status output
Console	
LED	
Power plugs	Power

2.3.4 Status LEDs

Table 8 Port status LEDs for the FCX 624 and FCX 648 models

Port Status LEDS		
LED	**State**	**Meaning**
Ethernet Link or Activity or Speed	On/Flashing Green	The port has established a valid link at 1000 Mbps. Flashing indicates the port is transmitting and receiving user packets.
	On/Flashing Amber	The port has established a valid link at 10 or 100 Mbps. Flashing indicates the port is transmitting and receiving user packets.
	Off	A link is not established with a remote port.
HPOE	On	The port is providing HPOE power to a connected device
	Off	The port is not providing HPOE power.
SFP	On Green	The SFP port is operating at 1000 Mbps.
	On Amber	The SFP port is operating at 100 Mbps.
	Off	A link is not established with a remote port.
PS1 & PS2 (Power Supply)	Green	Power supply is operating normally.
	Amber	Power supply fault

Port Status LEDS		
LED	**State**	**Meaning**
	Off	Power off or fault
Diag (Diagnostic)	Flashing Green	System self-diagnostic test in progress
	Green	System self-diagnostic test successfully completed
	Amber	System self-diagnostic test has detected a fault. (Blower, thermal or any interface fault.)
A or S	Green	The device is the Active controller. If this LED is flashing green, the system is initializing.
	Amber	Indicates the device is the Standby controller.
	Off	Device is operating as a stack member, or is in standalone mode.
Up Link	Green	Uplink is operating normally
	Off	Uplink has failed or there is no link
Stack ID (1-8)	Green	Indicates the device stack ID

Table 9 Power status LEDs for the FCX 624 and FCX 648 models

LED	State	Meaning
DC OK	Green	DC output OK
	Red	DC output failure
AC OK	Green	AC input OK
	Red	AC input failure

Table 10 Status LEDs for the SX 800 and SX 1600 Management Modules

LED	Position	State	Meaning
Pwr	Left of the console port	On (Green)	The module is receiving power
		Off	The module is not receiving power
Active	Left of the console port	On (Green)	The module is the active management module
		Off	The module is not the active management module
10/100/1000 Ethernet Port			
Link	Left-most LED	On	The port is connected

LED	Position	State	Meaning
	within the RJ-45 Ethernet port connector	Off	No port connection
Act	Right-most LED within the RJ-45 Ethernet port connector	On or Blinking	The port is transmitting and receiving traffic
		Off	The port is not transmitting or receiving traffic
10-GbE Port			
Link	Top-most LED to the left of the port	On	Fiber port is connected
		Off	No fiber port connection exists
Act	Bottom-most LED to the left of the port	On or Blinking	The port is transmitting and receiving traffic
		Off	The port is not transmitting or receiving traffic

Table 11 Status LEDs for the SX 800 and SX 1600 Switch Fabric Modules

LED	Position	State	Meaning
Pwr	Top	On (Green)	The module is receiving power
		Off	The module is not receiving power
Active	Bottom	On (Green)	The module is functioning properly
		Off	The module is not functioning properly

Tables 12 and 13 summarize the network ports provided by each FastIron model.

Table 12 FastIron SX Series Physical Ports

SX series	Model ID	Class 3 PoE	Poe+ (802.3at compliant)	10 GbE
FastIron SX 800	SX 800	Up to 192	Up to 140	
FastIron SX 1600	SX 1600	Up to 384	Up to 280	Up to 36

See the Brocade FastIron SX Series Chassis Hardware Installation Guide [53-1002219-02] Chapter 1 for detailed descriptions of network ports (including combination ports), management ports, and status indicators provided by each model.

Table 13 FastIron FCX Series Physical Ports

FCX series	10/100/1000 Mbps RJ-45	100/1000 Mbps SFP	10/100/1000 Mbps PoE+	16 GbE stacking
FCX624S	24			2
FCX624S-F-ADV		24		2
FCX624S-HPOE-ADV			24	2
FCX648S	48			2

FCX series	10/100/1000 Mbps RJ-45	100/1000 Mbps SFP	10/100/1000 Mbps PoE+	16 GbE stacking
FCX648S-HPOE			48	2
FCX648S-HPOE-ADV			48	2

See the Brocade FCX Series Hardware Installation Guide [53-1002220-01] section *Hardware Feature*s for detailed descriptions of network ports (including combination ports), management ports, and status indicators provided by each model.

2.4 Modes of Operation

The FastIron cryptographic module has two modes of operation: FIPS Approved mode and non-FIPS Approved mode. Section 4 describes services and cryptographic algorithms available in FIPS-Approved mode. In non-FIPS Approved mode, the module runs without these FIPS policy rules applied. Section 6.1.1 FIPS Approved Mode describes how to invoke FIPS-Approved mode.

2.5 Module Validation Level

The module meets an overall FIPS 140-2 compliance of security level 2 with Design Assurance level 3.

Table 14 FastIron Security Levels

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Cryptographic Key Management	2
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A
Operational Environment	N/A

3. Roles

In FIPS Approved mode, FastIron supports four roles: Crypto Officer, Port Configuration Administrator, User, and Unauthenticated Role:

1. Crypto Officer Role: The Crypto Officer role on the device in FIPS Approved mode is equivalent to the administrator or super-user in non-FIPS mode. Hence, the Crypto Officer role has complete access to the system.
2. Port Configuration Administrator Role: The Port Configuration Administrator role on the device in FIPS Approved mode is equivalent to the port-config, a port configuration user in non-FIPS Approved mode. Hence, the Port Configuration Administrator role has read-and-write access for specific ports but not for global (system-wide) parameters.
3. User Role: The User role on the device in FIPS Approved mode has read-only privileges and no configuration mode access (user).
4. Unauthenticated Role: The unauthenticated role on the device in FIPS mode is possible while using serial console to access the device. Console is considered as a trusted channel. The scope of the role

is same as the User Role without authentication. The enable command allows user to authenticate using a different role. Based on the authentication method mentioned in section 5.2, the role would change to one of Crypto Officer, Port Configuration Administrator or User role.

The User role has read-only access to the cryptographic module while the Crypto Officer role has access to all device commands. FastIron modules do not have a maintenance interface.

See section 4 Services, the section titled Setting passwords for management privilege levels in [53-1002240-04] for details of role capabilities. Within this document, Section 5.2 Authentication describes the authentication policy for the user roles.

4. Services

The services available to an operator depend on the operator's role. Unauthenticated operators may view externally visible status LED. LED signals indicate status that allows operators determine if the network connections are functioning properly. Unauthenticated operators can also perform self-test via power-cycle. They can also view the module status via "fips show".

For all other services, an operator must authenticate to the device as described in section 5.2 Authentication.

FastIron devices provide services for remote communication (SSH, HTTPS, SNMPv3 and Console) for management and configuration of cryptographic functions.

The following subsections describe services available to operators based on role. Each description includes lists of cryptographic functions and critical security parameter (CSP) associated with the service. Table 15 summarizes the available FIPS-Approved cryptographic functions.

Table 16 FIPS Non-Approved Cryptographic Functions Allowed in FIPS Approved Mode lists cryptographic functions that while not FIPS-Approved are allowed in FIPS Approved mode of operation.

Table 15 FIPS Approved Cryptographic Functions

Label	Cryptographic Function
AES	Advanced Encryption Algorithm
Triple-DES	Triple Data Encryption Algorithm
SHA	Secure Hash Algorithm
HMAC	Keyed-Hash Message Authentication code
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
RSA	Rivest Shamir Adleman Signature Algorithm

Table 16 FIPS Non-Approved Cryptographic Functions Allowed in FIPS Approved Mode

Label	Cryptographic Functions
KW	RSA Key Wrapping
DH	Diffie-Hellman key agreement
SNMP	SNMPv3
MD5	Message-Digest algorithm 5
KDF	SSHv2 Key Derivation Function

Table 17 FIPS Non-Approved Cryptographic Functions and Protocols available in non-FIPS Approved Mode

Label/Protocol	Cryptographic Functions
HTTPS Cipher Suites	RSA_WithDES_CBC_SHA RSA_With3DES_EDE_CBC_SHA DHE_DSSWithDES_CBC_SHA DHE_DSSWith3DES_EDE_CBC_SHA DHE_RSAWithDES_CBC_SHA DHE_RSAWith3DES_EDE_CBC_SHA RSA_Export1024WithDES_CBC_SHA RSA_WithAES_128_CBC_SHA RSA_WithAES_256_CBC_SHA DHE_DSS_WITH_AES_128_CBC_SHA DHE_RSA_WITH_AES_128_CBC_SHA DHE_DSS_WITH_AES_256_CBC_SHE_RSA_WITH_AES_256_CBC_SHA
HTTP	None
SNMP (Simple Network Management Protocol v1 and v2)	None
Telnet	None
TFTP (Trivial File Transfer Protocol)	None

Table 18 Services that do not use any Cryptographic Functions available in both Approved and Non Approved FIPS mode

VSRP	None
VRRP/VRRP-E	None
MPLS RSVP	None
MPLS-LDP	None
SNTP	None
NTP	None
BGP	None

4.1 User Role Services

4.1.1 SNMP

The SNMP service within the FastIron device uses SNMPv1, v2c or v3 versions. SNMPv1 and SNMPv2c do not use any cryptographic functions. SNMPv3 uses non-approved cryptographic functions. The device does not provide SNMP access to CSPs when operating in FIPS Approved mode. These CSP MIB objects are a small subset of MIB that represent the security parameters like passwords, secrets and keys. All other MIB objects are available for use in approved and non- approved FIPS mode. These other MIB objects provide capability to monitor and manage the various functional entities in the module.

The SNMP service within user role allows read-only access to the SNMP MIB.

4.1.2 Console

Console connection occurs via a directly connected RS-232 serial cable. Once authenticated as the User, the module provides console commands to display information about a FastIron device and perform basic tasks (such as pings). The User role has read-only privileges and no configuration mode access. The list of commands available are same as the list mentioned in the SSH service.

4.2 Port Configuration Administrator Role Services

4.2.1 SNMP

Section 4.1.3, above, describes this service.

The SNMP service is not available for a port configuration under the administrator role.

4.2.2 Console

Section 4.1.4, above, describes this service.

Console access as the Port Configuration Administrator provides an operator with the same capabilities as User Console commands plus configuration commands associated with a network port on the device. EXEC commands. The list of commands available are same as those mentioned in the SSH service. This service is described in Section 4.1.4 above.

4.3 Crypto Officer Role Services

4.3.1 SNMP

Section 4.1.3, above, describes this service. The SNMP service within crypto-officer role allows read-write access to the SNMP MIB within the FastIron device.

4.3.2 Console

Section 4.1.4, above, describes this service

Console commands provide an authenticated Crypto Officer complete access to all the commands within the FastIron device. This operator can enable, disable and perform status checks. This operator can also enable any service by configuring the corresponding command. For example, to turn on SSH service, the operator would create a pair of DSA host keys, configure the authentication scheme for SSH access. To enable the Web Management service, the operator would create a pair of RSA host keys and a digital certificate using corresponding commands, and enable the HTTPS server.

4.4 Non-FIPS Mode Services

Certain services are available within non-FIPS mode of operation, which are otherwise not available in FIPS mode of operation. They are:

1. TFTP
   - Trivial File Transfer Protocol (TFTP) is a file transfer protocol notable for its simplicity. It is generally used for automated transfer of configuration or boot files between machines in a local environment. Compared to FTP, TFTP is extremely limited, providing no authentication, and is rarely used interactively by a user.
2. Telnet
   - Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

3. SNMP
   - SNMP is a network management protocol to manage the device. When a device is put in non-FIPS mode all the Critical Security Parameters (CSP) will be zeroized. Any configurations of CSP after that will be accessible through SNMP.
4. HTTP
   - This service provides a graphical user interface for managing FastIron SX and FCX series devices over an unsecure communication channel.
5. SSH
   - This service is no longer allowed in FIPS mode of operation.
6. SCP
   - This service is no longer allowed in FIPS mode of operation.
7. HTTPS
   - This service is no longer allowed in FIPS mode of operation.

5. Policies

5.1 Security Rules

The cryptographic modules' design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS140-2 Level 2 module.

1) The cryptographic module provides role-based authentication.
2) Until the module is initialized, the operator cannot access any cryptographic services.
3) The cryptographic module performs the following tests:
   a) Power on Self-Tests:
      i) Cryptographic algorithm tests:
         (1) TripleDES 56bit encrypt KAT
         (2) TripleDES 56bit decrypt KAT
         (3) AES 128, 192,256 bit encrypt KAT
         (4) AES 128, 192,256 bit decrypt KAT
         (5) SHA-1 KAT
         (6) SHA-256 KAT
         (7) SHA-512 KAT
         (8) HMAC-SHA1 KAT
         (9) HMAC-SHA256 KAT
         (10) HMAC-SHA512 KAT
         (11) DRBG KAT
         (12) DSA sign KAT
         (13) DSA verify KAT
         (14) RSA sign KAT
         (15) RSA verify KAT
      ii) Firmware integrity test (DSA signature verification)
      iii) If the module does not detect an error during the Power on Self Test (POST), at the conclusion of the test, the console displays the message shown below.

Crypto module initialization and Known Answer Test (KAT) Passed.

iv) If the module detects an error during the POST, at the conclusion of the test, the console displays the message shown below. After displaying the failure message, the module reboots.

Crypto Module Failed <Reason String>

b) The module also supports the following conditional tests:

i) CRNGT for DRBG

ii) CRNGT for Hardware RNG

iii) Pair-wise consistency tests on generation of DSA and RSA keys

iv) Firmware load test (DSA signature verification)

4) At any time the cryptographic module is in a Common Services state, the operator can command the module to perform a power-up self-test.

5) Data output is inhibited during key generation, self-tests, zeroization, and error states.

6) Status information does not contain CSPs or sensitive data that if used could compromise of the module.

5.1.1 Cryptographic Module Operational Rules

In order to operate an FCX 624, FCX 648, SX 800 and SX 1600 series device securely, an operator should be aware of the following rules for FIPS Approved mode of operation.

External communication channels / ports are not be available before initialization of an FCX 624, FCX 648, SX 800 and SX 1600 series device.

FCX 624, FCX 648, SX 800 and SX 1600 series devices uses a FIPS Approved random number generator implementing Algorithm Hash DRBG based on hash functions.

FCX 624, FCX 648, SX 800 and SX 1600 series devices test the prime numbers generated for both DSA and RSA keys using multiple Miller-Rabin test. See [RSA PKCS #1] Appendix 2.1 A Probabilistic Primality Test.

FCX 624, FCX 648, SX 800 and SX 1600 series devices use NIST non-Approved and non-compliant key establishment techniques:

- Diffie-Hellman [non-compliant]
- RSA Key Wrapping [non-compliant]

FCX 624, FCX 648, SX 800 and SX 1600 series devices restrict key entry and key generation to authenticated roles.

FCX 624, FCX 648, SX 800 and SX 1600 series devices do not display plaintext secret or private keys. The device displays "…" in place of plaintext keys.

FCX 624, FCX 648, SX 800 and SX 1600 series devices use the standard RFC 4253 method for generating session keys for SSHv2 and HTTPS.

FCX 624, FCX 648, SX 800 and SX 1600 series perform only "get" operations using SNMP.

5.2 Authentication

FastIron devices support role-based authentication. A device can perform authentication and authorization (that is, role selection) using TACACS/TACACS+, RADIUS and local configuration database. Moreover, FastIron supports multiple authentication methods for each service.

To implement one or more authentication methods for securing access to the device, an operator in the Crypto Officer role configures authentication-method lists that set the order in which a device consults authentication methods. In an authentication-method list, an operator specifies an access method (SSH, Web, SNMP, and so on) and the order in which the device tries one or more of the following authentication methods:

a. Line password authentication,

b. Enable password authentication,

c. Local user authentication,

d. RADIUS authentication with exec authorization and command authorization, and

e. TACACS/TACACS+ authentication with exec authorization and command authorization

When a list is configured, the device attempts the first method listed to provide authentication. If that method is not available, (for example, the device cannot reach a TACACS+ server) the device tries the next method until a method in the list is available or all methods have been tried.

FastIron devices allow multiple concurrent operators through SSH and the console. One operator's configuration changes can overwrite the changes of another operator. See [53-1002240-04] *Single user in CONFIG mode*.

5.2.1 Line Authentication Method

The line method uses the Telnet password to authenticate an operator.

To use line authentication, a Crypto Officer must set the Telnet password. See *Setting a Telnet password* in [53-1002240-04]. Please note that when operating in FIPS mode, Telnet is disabled and Line Authentication is not available.

5.2.2 Enable Authentication Method

The enable method uses a password corresponding to each role to authenticate an operator. An operator must enter the read-only password to select the User role. An operator enters the port-configuration password to the Port Configuration Administrator role. An operator enters the super-user password to select the Crypto Officer Role.

To use enable authentication, a Crypto Officer must set the password for each privilege level. See *Setting passwords for management privilege levels* in [53-1002240-04]

5.2.3 Local Authentication Method

The local method uses a password associated with a user name to authenticate an operator. An operator enters a user name and corresponding password. The FastIron device assigns the role associated with the user name to the operator when authentication is successful.

To use local authentication, a Crypto Officer must define user accounts. The definition includes a user name, password, and privilege level (which determines role). See *Setting up local user accounts* in [53-1002240-04]

5.2.4 RADIUS Authentication Method

The RADIUS method uses one or more RADIUS servers to verify user names and passwords. The FastIron device prompts an operator for user name and password. The device sends the user name and password to the RADIUS server. Upon successful authentication, the RADIUS server returns the operator's privilege level, which determines the operator's role. If a RADIUS server does not respond, the FastIron device will send the user name and password information to the next configured RADIUS server.

FastIron series devices support additional command authorization with RADIUS authentication. The following events occur when RADIUS command authorization takes place.

a. A user previously authenticated by a RADIUS server enters a command on the FastIron device.

b. The FastIron device looks at its configuration to see if the command is at a privilege level that requires RADIUS command authorization.

c. If the command belongs to a privilege level that requires authorization, the FastIron device looks at the list of commands returned to it when RADIUS server authenticated the user.

NOTE: After RADIUS authentication takes place, the command list resides on the FastIron device. The device does not consult the RADIUS server again once the operator has been authenticated. This means that any changes made to the operator's command list on the RADIUS server are not reflected until the next time the RADIUS server authenticates the operator, and the server sends a new command list to the FastIron device.

To use RADIUS authentication, a Crypto Officer must configure RADIUS server settings along with authentication and authorization settings. See *RADIUS configuration procedure* in [53-1002240-04]

5.2.5 TACACS/TACACS+ Authentication Method

The TACACS/TACACS+ method uses one or more TACACS/TACACS+ servers to verify user names and passwords. For TACACS, the FastIron device prompts an operator for user name and password. The device sends the user name and password to the TACACS server. Upon successful authentication, the FastIron device selects the operator's role implicitly based on the action requested (for example, User role for a login request or Crypto Officer role for a configure terminal command). For TACACS+ authentication, the FastIron device prompts an operator for a user name, which the device uses to get a password prompt from the TACACS+ server. The operator enters a password, which the device relays to the server for validation. Upon successful authentication, the TACACS+ server supports both exec and command authorization similar to RADIUS authorization described above.

To use TACACS/TACACS+ authentication, a Crypto Officer must configure TACACS/TACACS+ server settings along with authentication and authorization settings. See Configuring TACACS/TACACS+ security in [53-1002240-04].

5.2.6 Strength of Authentication

FastIron devices minimize the likelihood that a random authentication attempt will succeed. The User and Crypto Officer passwords must each be at least 8 alphanumeric characters in length. Moreover, the RADIUS/TACACS+ shared secrets must each be at least 8 alphanumeric characters in length.

The character-set that is used for the User , Port Configuration Adminstrator, or Crypto Officer passwords or RADIUS/TACACS+ shared consists of 94 characters. Therefore, an adversary should try 94^8 = 6.09568939*10^15 ('^' indicates the exponentiation operation) attempts randomly to guess the correct sequence. Therefore, for each authentication method, the associated random access rate is 1/6.09568939*10^15, which is much less than one in 1,000,000.

As shown above, one should try 6.09568939*10^15 (94^8) attempts randomly to guess the passwords.

Assuming 100,000 attempts per minute are tried, the probability of success in a one minute period is less than 1 in 6.09568939 * 10^10 which is less than 1 in 100,000 and the requirement is easily met.

5.3 Access Control and Critical Security Parameter (CSP)

Table 17 summarizes the access operators in each role have to critical security parameters. Grayed out table cells indicate that the intersection of the role the CSP have not security relevance. The table entries have the following meanings:

- r – operator can read the value of the item,
- w – operator can write a new value for the item,
- x – operator can use the value of the item (for example encrypt with an encryption key), and
- d – operator can delete the value of the item (zeroize).

Table 19 Access Control Policy and CSP access

	User				Port Administrator			Crypto Officer				
Service / CSP	SSH	HTTPS	SNMP	Console	SSH	HTTPS	Console	SSH	SCP	HTTPS	SNMP	Console

	User				Port Administrator			Crypto Officer				
Service / CSP	SSH	HTTPS	SNMP	Console	SSH	HTTPS	Console	SSH	SCP	HTTPS	SNMP	Console
SSH host RSA or DSA private key	x				x			xwd	x			wd
SSH host RSA or DSA public key	x				x			xrwd	xrw			rwd
SSH client RSA or DSA public key	x				x			xrwd	xrwd			xrwd
SSH session key	x				x			x	x			
TLS host RSA private key		x				x		wd		x		wd
TLS host RSA digital certificate		x				x		rwd		x		rwd
TLS pre-master secret		x				x				x		
TLS session key		x				x				x		
DH Private Exponent	x				x			x	x			
DH Public Key	x				x			x	x			
User Password	x	x	x	x	x			xrwd	xrwd	xrwd	x	xrwd
Port Administrator Password					x	x	x	xrwd	xrwd	xrwd		xrwd
Crypto Officer Password								xrwd	xrwd	xrwd		xrwd
RADIUS Secret	x	x		x	x	x	x	xrwd	xrwd	xrwd		xrwd
TACACS+ Secret	x	x		x	x	x	x	xrwd	xrwd	xrwd		xrwd
Firmware Integrity / Firmware Load DSA public key								x		x		X
DRBG Seed	x	x			x	x		x	x	x		
DRBG Value V	x	x	x	x	x	x	x	x	x	x	x	x
DRBG Constant C	x	x	x	x	x	X	x	x	x	x	x	x
Hash DRBG Entropy	x	x	x	x	x	x	x	x	x	x	x	x

5.3.1 CSP Zeroizaton

- The SSH session key is transient. It is zeroized at the end of a session and recreated at the beginning of a new session.
- The TLS pre-master secret is generated during the TLS handshake. It is destroyed after it is used.

- The TLS session key is generated for every HTTPS session. The TLS session key is deleted after the session is closed.
- The DRBG entropy and seed (8 bits) is recomputed periodically on 100 millisecond intervals to add 6.7 bits of entropy. Each time this occurs, four bytes of the seed are written into an 8K buffer. When the buffer is full the DRBG V and C values are reseeded and the buffer is zeroized.
- The DH private exponent is generated at the beginning of DH KEX. A new random number overwrites the memory location used to store the value each time a new session is initiated.
- The DSA public key cannot be written, read or deleted. The key pair is prebuilt within the code binary. The key pair is destroyed and recreated each time new firmware is installed.
- For SSH, the RSA private key is stored in a locally generated file on flash during the key generation process. The file is removed during zeroization. The *crypto key zeroize* command removes the keys.
- Executing the *no fips enable* command zeroizes all CSPs.

5.4 Physical Security

FastIron devices require the Crypto Officer to install tamper evident labels (TELs) in order to meet FIPS 140-2 Level 2 Physical Security requirements. The TELs are available from Brocade under part number XBR-000195. The Crypto Officer shall follow the Brocade FIPS Security Seal application procedures prior to operating the module in FIPS mode. The FIPS seal application procedure is available in Appendix A of this document and defined within Brocade document 53-1002119-02. The procedure can be download at http://my.brocade.com (See “Documentation>Technical Documentation>Federal Information Process Standard (FIPS).

6. Crypto Officer Guidance

For each module to operate in a FIPS approved mode of operation, the tamper evident seals supplied in Brocade XBR-000195 must be installed, as defined in Appendix A. The FIPS Security Seal Procedures for Brocade FCX Series and Brocade FastIron SX Series document [53-1002119-02] provides instructions on the proper installation of the tamper evident seals.

The security officer is responsible for storing and controlling the inventory of any unused seals. The unused seals shall be stored in plastic bags in a cool, dry environment between 60° and 70° F (15° to 20° C) and less than 50% relative humidity. Rolls should be stored flat on a slit edge or suspended by the core.

The security officer shall maintain a serial number inventory of all used and unused tamper evident seals. The security officer shall periodically monitor the state of all applied seals for evidence of tampering. A seal serial number mismatch, a seal placement change, a checkerboard destruct pattern that appears in peeled film and adhesive residue on the substrate are evidence of tampering. The security officer shall periodically view each applied seal under a UV light to verify the presence of a UV wallpaper pattern. The lack of a wallpaper pattern is evidence of tampering. The security officer is responsible for returning a module to a FIPS approved state after any intentional or unintentional reconfiguration of the physical security measures.

The Brocade FastIron Configuration Guide [53-1002240-04] and FastIron FIPS Configuration Guide [53-1002618-01] addresses device configuration. In particular, the FastIron FIPS Configuration Guide provides configuration instructions specific to operating a FastIron devices in FIPS Approved mode.

6.1 Mode Status

FastIron devices provide the fips show command to display status information about the device’s FIPS mode. This information includes the status of administrative commands for security policy, the status of security policy enforcement, and security policy settings. The fips enable command changes the status of administrative commands; see also section 6.1.1 FIPS Approved Mode.

The following example shows the output of the fips show command before an operator enters a fips enable command. Administrative commands for security policy are unavailable (administrative status is off) and the device is not enforcing a secure operation (operational status is off).

```
FIPS mode: Administrative Status: OFF, Operational Status: OFF
```

The following example shows the output of the fips show command after an operator enters the fips enable command. Administrative commands for security policy are available (administrative status is on) but the device is not enforcing secure operation yet (operational status is off). Once powered on, the fips show command displays the security policy settings.

1. FIPS mode: Administrative Status: ON, Operational Status: OFF
    a. Once all CSPs are zeroized, the system needs to be reloaded to operationally enter FIPS mode.
2. System Specific:
    a. OS monitor mode access: Disabled
3. Management Protocol Specific:
    a. Telnet server: Disabled
    b. TFTP Client: Disabled
    c. HTTPS SSL 3.0: Disabled
    d. SNMP Access to security objects: Disabled
4. Critical Security Parameter Updates across FIPS Boundary:
    a. Protocol shared secret and host passwords: Clear
    b. SSH DSA Host Keys: Clear

HTTPS RSA Host Keys and Signature: Clear

The following example shows the output of the fips show command after the device reloads successfully in the default strict FIPS mode. Administrative commands for security policy are available (administrative status is on) and the device is enforcing secure operation (operational status is on): The fips show command displays the policy settings.

1. FIPS mode: Administrative Status: ON, Operational Status: ON
2. System Specific:
    a. OS monitor mode access: Disabled
3. Management Protocol Specific:
    a. Telnet server: Disabled
    b. TFTP Client: Disabled
    c. HTTPS SSL 3.0: Disabled
    d. SNMP Access to security objects: Disabled
4. Critical Security Parameter Updates across FIPS Boundary:
    a. Protocol shared secret and host passwords: Clear
    b. SSH DSA Host Keys: Clear
    c. HTTPS RSA Host Keys and Signature: Clear

6.1.1 FIPS Approved Mode

This section describes FIPS Approved mode of operation and the sequence of actions that put a FastIron device in FIPS Approved mode. FIPS Approved mode disables the following:

1. Telnet access including the *telnet server* command
2. AAA authentication for the console including the *enable aaa console* command
3. Command *ip ssh scp disable*
4. TFTP access
5. SNMP access to CSP MIB objects
6. Access to all commands within the monitor mode
7. HTTP access including the web-management http command
8. HTTPS SSL 3.0 access and RC4 cipher

9. Command web-management allow-no-password

Entering FIPS Approved mode also clears:

1. Protocol shared secret and host passwords
2. SSH DSA host keys
3. HTTPS RSA host keys and certificate

FIPS Approved mode enables:

1. SCP
2. HTTPS TLS version 1.0 and greater

In FIPS Approved mode, FastIron devices provide FIPS-Approved cryptographic algorithms as well as non-Approved security functions.

Table 20 Algorithm Certificates

Algorithm	Supports	Certificate
Advanced Encryption Algorithm (AES)	128-, 192, and 256-bit keys, ECB and CBC mode	#2150
Triple Data Encryption Algorithm (Triple-DES)	KO 1,2 ECB and CBC mode	#1363
Secure Hash Algorithm	SHA-1, SHA-256, SHA-384, and SHA-512	#1871
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	#1317
Deterministic Random Bit Generator (DRBG)	SHA-256 Based SP 800-90 DRBG	#239
Digital Signature Algorithm (DSA)	1024-bit keys SigVer only	#668*
Rivest Shamir Adleman Signature Algorithm (RSA)	1024-bit keys SigVer only, 2048-bit keys SigVer and SigGen	#1106*

*Note: RSA(Cert. #1106; non-compliant with the functions from the CAVP Historical RSA list)

FIPS186-2:
ALG[RSASSA-PKCS1_V1_5]: SIG(gen): 1024 , 1536 , SHS: SHA-1, SHA-256, SHA-384, SHA-512, 2048 , 3072 , 4096 , SHS: SHA-1

DSA(Cert. #668; non-compliant with the functions from the CAVP Historical DSA list)

FIPS186-2:
PQG(gen) MOD(1024);
KEYGEN(Y) MOD(1024);
SIG(gen) MOD(1024);

The following non-Approved but allowed cryptographic methods are allowed within limited scope in the FIPS Approved mode of operation:

1. SNMPv3 (Cryptographic function does not meet FIPS requirements and is considered plaintext)
2. MD5 – may be used in the TLS pseudo-random function (PRF) in FIPS mode
3. MD5 – may be used with TACACS+ packets. MD5 is used for TACACS+ authentication.
4. HMAC-MD5 – used to support RADIUS authentication
5. SSHv2 Key Derivation Function (KDF). This is a legacy implementation.

The following are non-compliant and cannot be used in FIPS mode:

1. RSA Key Wrapping [Non Compliant]
2. Diffie-Hellman (DH) [Non Compliant]

6.1.1.1 Invoking FIPS Approved Mode for Brocade FCX 624, FCX 648, SX 800 and SX 1600 Devices

To invoke the FIPS Approved mode of operation, perform the following steps from the console terminal.

1) Assume Crypto Officer role
2) Enter command: *fips enable*

   The device enables FIPS administrative commands. The device is not in FIPS Approved Mode of operation yet. Do *not* change the default strict FIPS security policy, which is required for FIPS Approved mode.
3) Enter command: *fips zeroize all*

   The device zeros out the shared secrets use by various networking protocols including host access passwords, SSH host keys, and HTTPS host keys with the digital signature.
4) Save the running configuration: *write memory*
5) The device saves the running configuration as the startup configuration
6) Reload the device

   The device resets and begins operation in FIPS Approved mode.
7) Enter command: *fips show*

   The device displays the FIPS-related status, which should confirm the security policy is the default security policy.
8) Inspect the physical security of the module, including placement of tamper evident labels according to Section 6.

6.1.1.2 Negating FIPS Approved Mode for Brocade FCX 624, FCX 648, SX 800 and SX 1600 Devices

To exit the FIPS Approved mode of operation, perform the following steps from the console terminal.

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 all 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.

7. Glossary

Term/Acronym	Description
AES	Advanced Encryption Standard
ADV L3	Advanced Layer 3 License
CBC	Cipher-Block Chaining
CLI	Command Line Interface
CSP	Critical Security Parameter
DES	Data Encryption Standard

Term/Acronym	Description
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook mode
FI	FastIron platform
GbE	Gigabit Ethernet
HMAC	Keyed-Hash Message Authentication Code
HPOE	High Power over Ethernet
HTTPS	Hypertext T4ansfer Protocol Secure
KDF	Key Derivation Function
LED	Light-Emitting Diode
LP	Line Processor
L2	Layer 2, Data link layer
L3	Layer 3, Network layer
Mbps	Megabits per second
MP	Management Processor
NDRNG	Non-Deterministic Random Number Generator
FI	FastIron platform
OC	Optical Carrier
PRF	pseudo-random function
RADIUS	Remote Authentication Dial in User Service
RSA	Rivest Shamir Adleman
SCP	Secure Copy
SFM	Switch Fabric Module
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Networking
SRDI	Security Relevant Data Items
SSH	Secure Shell
TACACS	Terminal Access Control Access-Control System
TACACS+	Terminal Access Control Access-Control System Plus
TDEA	Triple-DES Encryption Algorithm
TEL	Tamper Evident Label
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
XFP	10 Gigabit Small Form Factor Pluggable

8. References

[53-1002240-04] Brocade FastIron Configuration Guide, Brocade Communications Systems, Inc., Publication number 53-1002240-04, 30 April 2012

[53-1002618-01] FastIron FIPS Configuration Guide, Brocade Communications Systems, Inc., Publication number 53-1002618-01, 30 May 2012

[53-1002219-02] Brocade FastIron SX Series Chassis Hardware Installation Guide, Brocade Communications Systems, Inc., Publication number 53-1002219-02, 9 December 2011

[53-1002220-01] Brocade FCX Series Hardware Installation Guide, Brocade Communications Systems, Inc., Publication Number 53-1002220-01, 14 October 2011

[53-1002119-02] FIPS Security Seal Procedures for Brocade FCX Series and Brocade FastIron SX Series, Brocade Communications Systems, Inc., Publication Number 53-1002119-02, 28 August 2012

[FIPS 186-2+] Federal Information Processing Standards Publication 186-2 (+Change Notice), *Digital Signature Standard (DSS),* 27 January 2000

[RSA PKCS #1] PKCS #1: RSA Cryptography Specifications Version 2.1**,** http://tools.ietf.org/html/rfc3447

[SP800-90] National Institute of Standards and Technology Special Publication 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised),* March 2007

Appendix A: Tamper Label Application

The FIPS Kit (SKU XBR-000195) contains the following items:

- Tamper Evident Security Seals
  - Count 120
  - Checkerboard destruct pattern with ultraviolet visible “Secure” image
- 53-1002458-02 : FIPS Pointer Document Guideline

This document provides instructions on how to access the [53-1002119-02] FIPS Security Seal Procedures for Brocade FCX Series and Brocade FastIron SX Series, document on the MyBrocade website.

Use 99% isopropyl alcohols to clean the surface area at each tamper evident seal placement location. Isopropyl alcohol is not provided in the kit. However, 99% isopropyl alcohol is readily available for purchase from a chemical supply company. Prior to applying a new seal to an area, that shows seal residue, use consumer strength adhesive remove to remove the seal residue. Then use additional alcohol to clean off any residual adhesive remover before applying a new seal.

Applying seals to Brocade FCX 624S-F-ADV, Brocade FCX 624S and Brocade FCX 624S-HPOE-ADV devices

Use the figures in this section as a guide for security seal placement on the following Brocade FastIron devices:

- Brocade FCX 624S-F-ADV
- Brocade FCX 624S
- Brocade FCX 624S-HPOE-ADV

The connectors on the faceplates of your particular device might vary from the connectors shown on the figures, but the placement of the seals will be the same. Figure 8 and Figure 9 display a Brocade FCX 624S with seals as a model for the seal placement on the Brocade FCX 624S-F-ADV, FCX 624S and FCX 624S-HPOE-ADV. Each of these devices requires the placement of 13 seals:

- Top: Affix 4 total seals to the top panel of the device. Affix two seals so that they cover the left and right front most screws on the top panel of the device. Affix two seals so that they cover the two screws adjacent to the front most screws on the top panel. See Figure 8 for correct seal orientation and positioning.
- Right and left sides: Affix 4 total seals to the left and right sides of the device--two seals on the right side and two seals on the left side. Each seal should cover two holes on either side of the first vent section. See Figure 8 for correct seal orientation and positioning on the right side of the device. The orientation and placement of seals on the left side mirrors the orientation and placement of seals on the right side of the device (visible in Figure 8).
- Front: Affix one seal horizontally aligned with half affixed to the front panel and half affixed to the bottom panel. You must bend this seal to place it correctly. See Figure 8 for correct seal orientation and positioning.
- Rear: Affix 4 total seals to the rear panel of the device. Affix one seal from the rear panel to the bottom panel and three seals from the rear panel to the top panel. You must bend these seals to place them correctly. See Figure 9 on page 6 for correct seal orientation and positioning.

Figure 8 Front, top, and right side views of a Brocade FCX624S-F-ADV, FCX 624S and FCX 624S-HPOE-ADV device with security seals

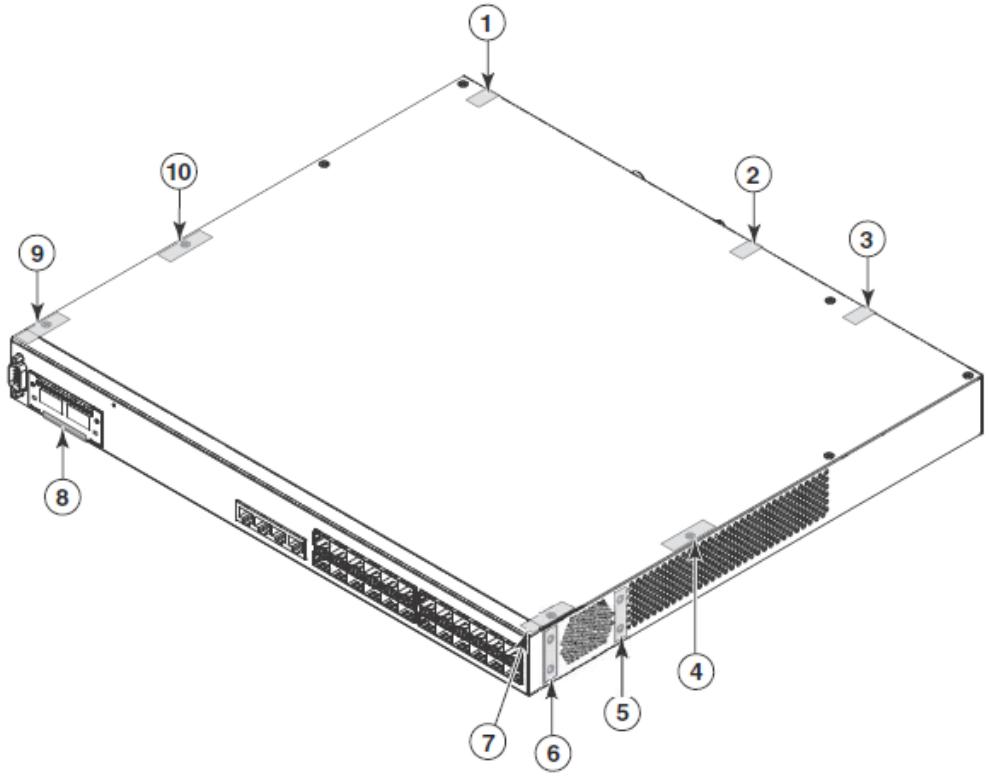
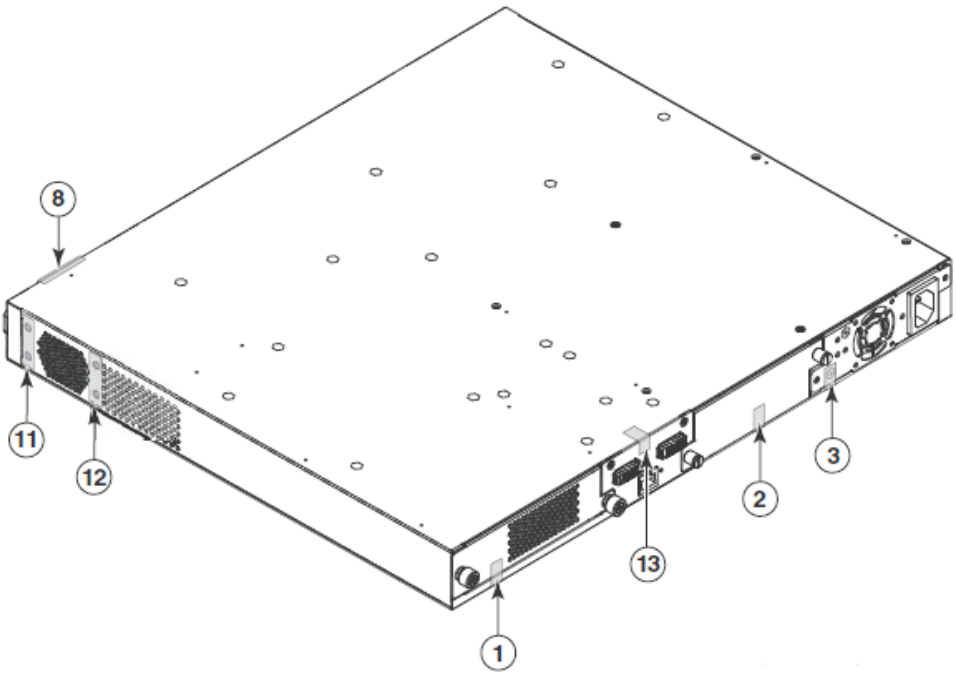


Figure 9 Rear, bottom, and left side views of a Brocade FCX624S-F-ADV, FCX 624S and FCX 624S-HPOE-ADV device with security seals



Applying seals to Brocade FCX 648S, FCX 648S-HPOE and FCX 648S-HPOE-ADV devices

Use the figures in this section as a guide for security seal placement on the following Brocade FastIron devices:

- Brocade FCX 648S
- Brocade FCX 648S-HPOE
- Brocade FCX 648S-HPOE-ADV

Figure 10 and Figure 11 display a Brocade FCX 648S with seals as a model for the seal placement on the Brocade FCX 648S, FCX 648S-HPOE and FCX 648S-HPOE-ADV. Each of these devices requires the placement of 13 seals:

- **Top**: Affix 4 total seals to the top panel of the device. Affix two seals so that they cover the left and right front most screws on the top panel of the device. Affix two seals so that they cover the two screws adjacent to the front most screws on the top panel. See Figure 10 for correct seal orientation and positioning.
- **Right and left sides**: Affix 4 total seals to the left and right sides of the device--two seals on the right side and two seals on the left side. Each seal should cover two holes on either side of the first vent section. See Figure 10 for correct seal orientation and positioning on the right side of the device. The orientation and placement of seals on the left side mirrors the orientation and placement of seals on the right side of the device (visible in Figure 10).
- **Front**: Affix one seal horizontally aligned with half affixed to the front panel and half affixed to the bottom panel. You must bend this seal to place it correctly. See Figure 10 for correct seal orientation and positioning.

  Rear: Affix 4 total seals to the rear panel of the device. Affix one seal from the rear panel to the bottom panel and three seals from the rear panel to the top panel. You must bend these seals to place them correctly. See Figure 11 for correct seal orientation and positioning.

Figure 10 Front, top and right side views of a Brocade FCX 648S, FCX 648S-HPOE and FCX 648S-HPOE-ADV device with security seals

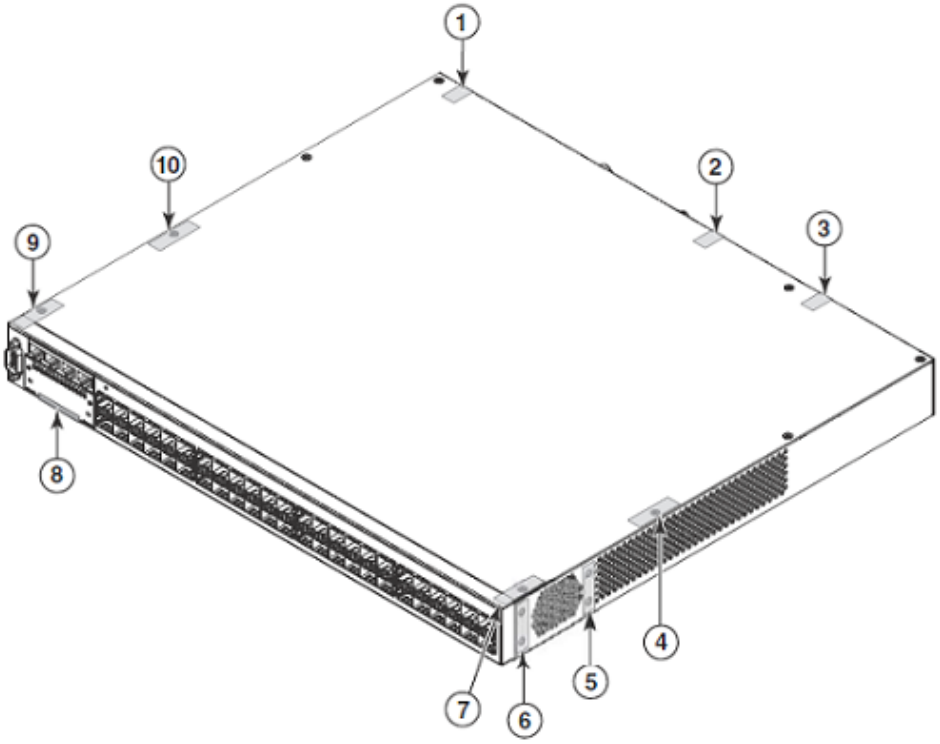
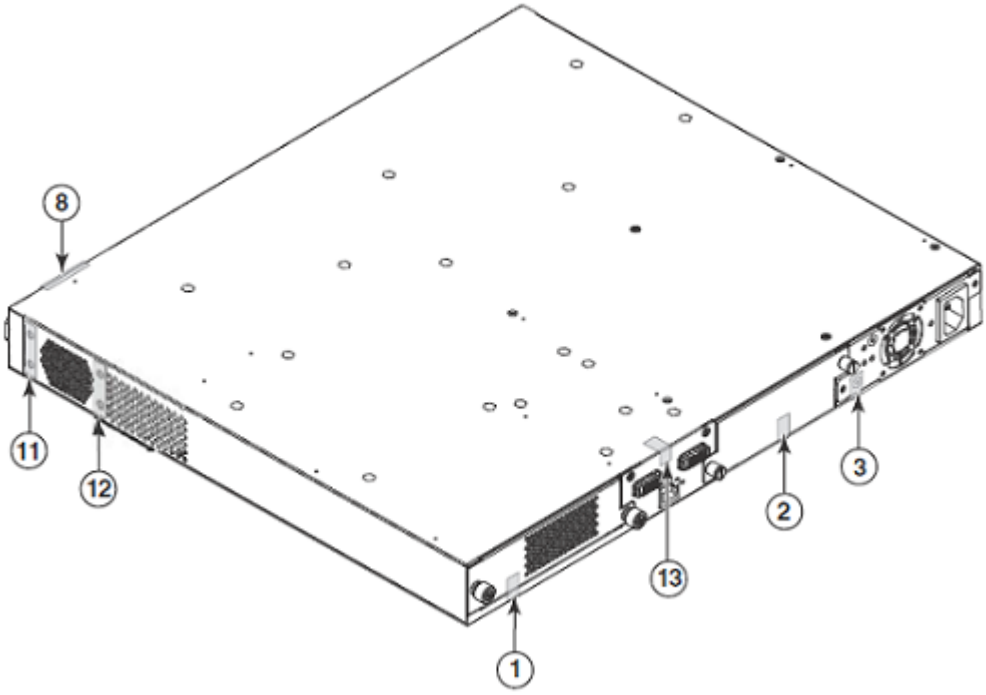


Figure 11 Rear, bottom, and left side views of a Brocade FCX 648S, FCX 648S-HPOE and FCX 648S-HPOE-ADV device with security seals



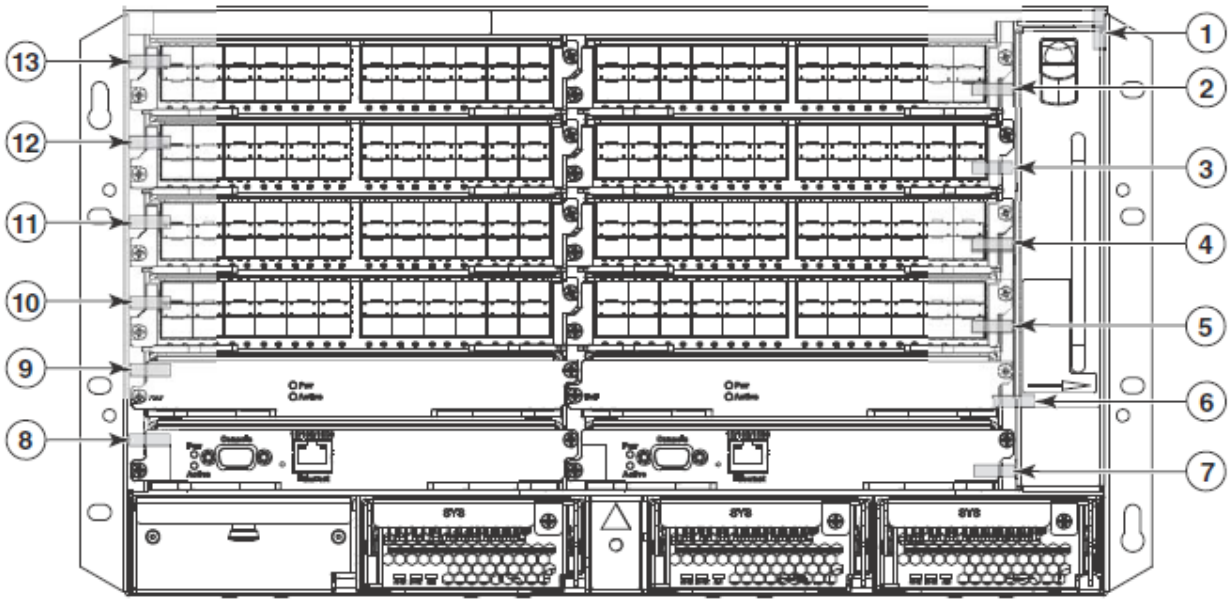
Applying seals to Brocade FastIron SX 800 devices

Use the figures in this section as a guide for security seal placement on a Brocade FastIron SX 800 device.

The connectors on the faceplates of a particular module might vary from the connectors shown on the figures, but the placement of the seals will be the same. There is no seal placement required on the side panels or solely on the top and bottom panels of Brocade FastIron SX 800 devices. Each Brocade FastIron SX 800 device requires the placement of 16 seals:

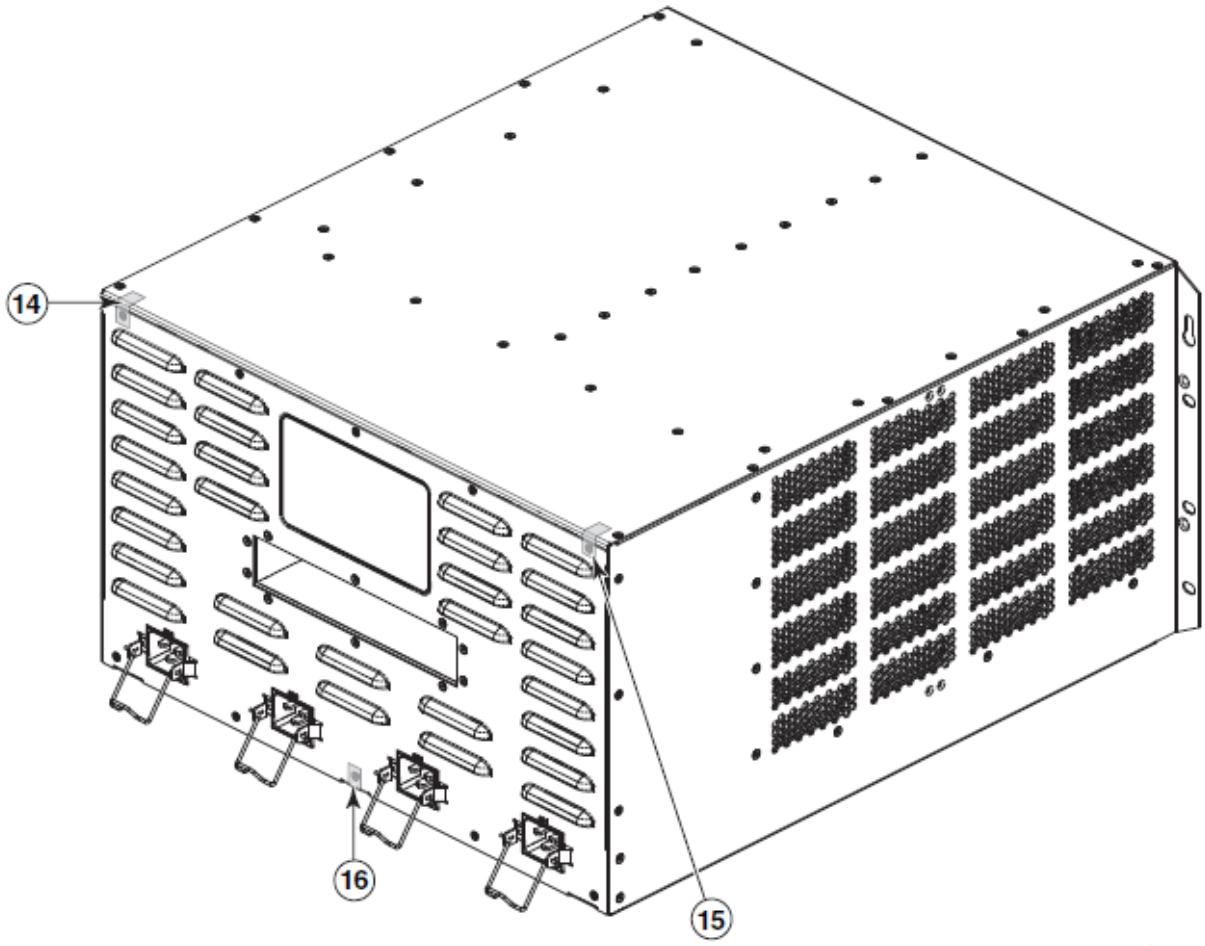
- Front: Affix 13 total seals to the front panel of the device. Affix one vertically oriented seal to the left ear of each module installed in the left side of the chassis. As much as possible of the seal should be affixed to the module directly above the left screw for the left side modules. Affix one vertically oriented seal to each of the modules installed in the right side of the chassis by affixing the seals directly under the screw to the right ear of each module and to the chassis. Affix one seal from the upper right corner of the fan tray to the chassis. All 13 of these seals should lie flat against the front of the device. See Figure 12 for correct seal orientation and positioning.

Figure 12 Front view of a Brocade FastIron SX 800 device with security seals



- Rear: Affix 3 total seals to the rear panel of the device. Affix two vertically-aligned seals at the upper right and left sides of the rear panel so that one half of the seal is affixed to the top panel of the device and the other half is affixed to the rear panel and covering the rightmost and leftmost screws. You must bend these seals to place them correctly. Affix one seal vertically aligned at the lower center of the rear panel so that one-half of the seal is affixed to the bottom panel of the device and the other half of the seal is affixed to the rear panel of the device, covering the middle screw. See Figure 13 for seal orientation and positioning.

Figure 13 Rear, top, and left side panel views of a Brocade FastIron SX 800 device with security seals



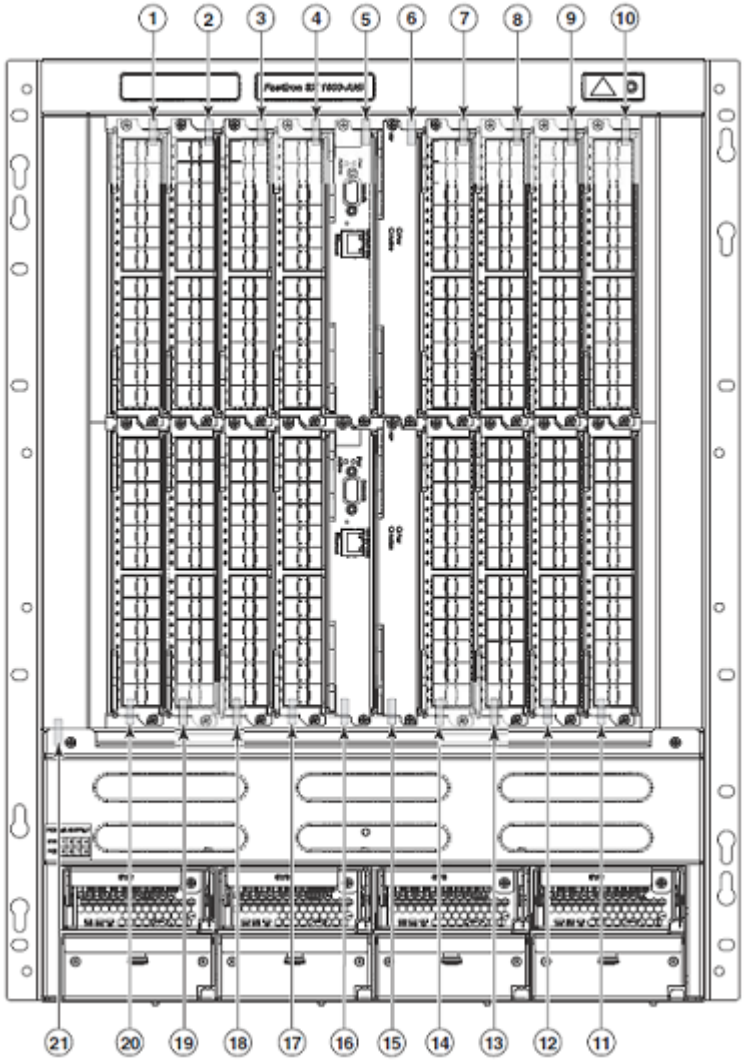
Applying seals to Brocade FastIron SX 1600 devices

Use the figures in this section as a guide for security seal placement on a Brocade FastIron SX 1600 device.

The connectors on the faceplates of a particular module might vary from the connectors shown on the figures, but the placement of the seals will be the same. There is no seal placement required on the top panel, bottom panel, or side panels of Brocade FastIron SX 1600 devices. Each Brocade FastIron SX 1600 device requires the placement of 24 seals:

- **Front**: Affix 21 total seals to the front panel of the device. Affix one horizontally oriented seal to the upper ear of each module installed in the top row of the chassis as shown in Figure 14. As much as possible of the seal should be affixed to the module to the right of the screw that secures each module to the chassis. Affix one horizontally oriented seal to the lower ear of each module installed in the bottom row of the chassis as shown in Figure 14. As much as possible of the seal should be affixed to the module to the left of the screw that secures each module to the chassis. Affix one seal from the upper left corner of the fan tray to the chassis, as shown in Figure 14. All 21 of the seals should lie flat against the front panel of the device.

Figure 14 Front view of a Brocade FastIron SX 1600 device with security seals



- **Rear**: Affix 3 total seals to the rear panel of the device. Affix two vertically aligned seals to the right and left top edges of the chassis so that half of the seal is affixed to the top panel and half to the rear panel or, in the case of an ANR, to the bracket that attaches the ANR bracket to the rear panel of the chassis. Affix one seal vertically to the center bottom edge of the rear panel so that one-half of the seal is affixed to the rear panel of the device and one-half of the seal is affixed to the bottom panel. You must bend this seal to place it correctly. See Figure 15 for correct seal orientation and positioning.

Figure 15 Rear view of the FastIron SX 1600 device with security seals