Brocade® FCX 624/648, ICX 6450, ICX 7750, ICX 7250 and SX 800/1600 Series

FIPS 140-2 Non-Proprietary Security Policy Level 2
with Design Assurance Level 3 Validation

Document Version 1.0

June 24, 2016

Revision History

Revision Date	Revision	Summary of Changes
6/24/2016	1.0	Initial Release

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

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.

Brocade ICX 6450 switches provide enterprise-class stackable LAN switching solutions to meet the growing demands of campus networks. Designed for small to medium-size enterprises, branch offices, and distributed campuses, these intelligent, scalable edge switches deliver enterprise-class functionality without compromising performance and reliability.

The Brocade ICX7250 Switch delivers the performance, flexibility, and scalability required for enterprise Gigabit Ethernet (GbE) access deployment. It raises the bar with up to 8×10 GbE ports for uplinks or stacking and market-leading stacking density with up to 12 switches (576×1 GbE) per stack. In addition, the Brocade ICX 7250 combines enterprise-class features, manageability, performance, and reliability with the flexibility, cost-effectiveness, and "pay as you grow" scalability of a stackable solution.

The Brocade ICX 7750 is a 10/40 GbE Ethernet switch delivering a chassis experience for campus LAN aggregation and core. It offers unprecedented port density and chassis-level performance, availability, and scalability. The ICX 7750 distributed chassis technology enables scale-out networking and its true hybrid-port mode OpenFlow provides a migration path to SDN.

2 Overview

The FIPS 140-2 validation includes hardware devices running the firmware version presented in Table 1. The module meets an overall FIPS 140-2 compliance of Security Level 2 with Design Assurance Level 3.

Table 2, Table 6, Table 7, Table 9 and Table 11 list the devices included in this evaluation.

Table 2 lists the six (6) Brocade FCX 624 series and FCX 648 series devices, referred collectively for the remainder of this document as FCX 624/648 device (cryptographic module, or simply the module). Each FCX 624/648 device is a fixed-port switch, which is a multi-chip standalone cryptographic module. The power supplies, fan tray assemblies and 2X10G Ethernet uplink module (FCX-2XG) are part of the cryptographic boundary and can be replaced in the field. An unpopulated FCX-2XG slot is covered by an opaque bezel which is part of the cryptographic boundary. For each module to operate in a FIPS Approved mode of operation, the tamper evident label security seals, supplied in FIPS Kit (Part Number: XBR-000195) must be installed, as defined in Appendix A.

Table 6 lists the five (5) Brocade ICX 6450 series devices, referred collectively for the remainder of this document as ICX 6450 device (cryptographic module, or simply the module). Each ICX 6450 device is a fixed-port switch, which is a multi-chip standalone cryptographic module. The power supplies and fan tray assemblies are part of the cryptographic boundary and cannot be replaced in the field. The cryptographic boundary for each ICX 6450 device is represented by the opaque enclosure (including the power supply, fan tray and bezels) with removable cover. For each module to operate in a FIPS

Approved mode of operation, the tamper evident label security seals, supplied in FIPS Kit (Part Number: XBR-000195) must be installed, as defined in Appendix A.

Table 7 lists the five (5) Brocade ICX 7250 series devices, referred collectively for the remainder of this document as ICX 7250 device (cryptographic module, or simply the module). Each ICX 7250 device is a fixed-port switch. This environment is a multi-chip standalone cryptographic module. ICX 7250 is available in PoE and non-PoE configuration. The cryptographic boundary for each ICX 7250 device is represented by the opaque enclosure (including the power supply, fan tray and bezels). For each module to operate in a FIPS approved mode of operation, the tamper evident label security seals, supplied in FIPS Kit (Part Number: XBR-000195) must be installed, as defined in Appendix A.

Table 9 lists the three (3) Brocade ICX 7750 series devices, referred collectively for the remainder of this document as ICX 7750 device (cryptographic module, or simply the module). Each ICX 7750 device is a fixed-port switch, which is a multi-chip standalone cryptographic module. The installed fans either use a push or pull configuration to move the air between the back and front of the device. Each model is orderable with either fan trays or power supply side intake (-I) or power supply side exhaust (-E) airflow. 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. The cryptographic boundary for each ICX 7750 device is represented by the opaque enclosure (including the power supply, fan tray and bezels) with removable cover. For each module to operate in a FIPS approved mode of operation, the tamper evident label security seals, supplied in FIPS Kit (Part Number: XBR-000195) must be installed, as defined in Appendix A.

Table 11 lists the two (2) FastIron SX 800 and SX 1600 series devices, referred collectively for the remainder of this document as SX 800/1600 device (cryptographic module, or simply the module). Each SX 800/1600 device is a chassis based switch, which is a multi-chip standalone cryptographic module. The power supplies are part of the cryptographic boundary. The fan tray assemblies are part of the cryptographic boundary and can be replaced in the field. Unpopulated management module, switch fabric module and port blade modules slots are covered by opaque bezels. The cryptographic boundary for each SX 800/1600 device is represented by the opaque enclosure (including the management modules, switch fabric modules, fan trays and bezels) with removable cover. For each module to operate in a FIPS approved mode of operation, the tamper evident label security seals, supplied in FIPS Kit (Part Number: XBR-000195) must be installed, as defined in section 16, Appendix A: Tamper Evident Label application.

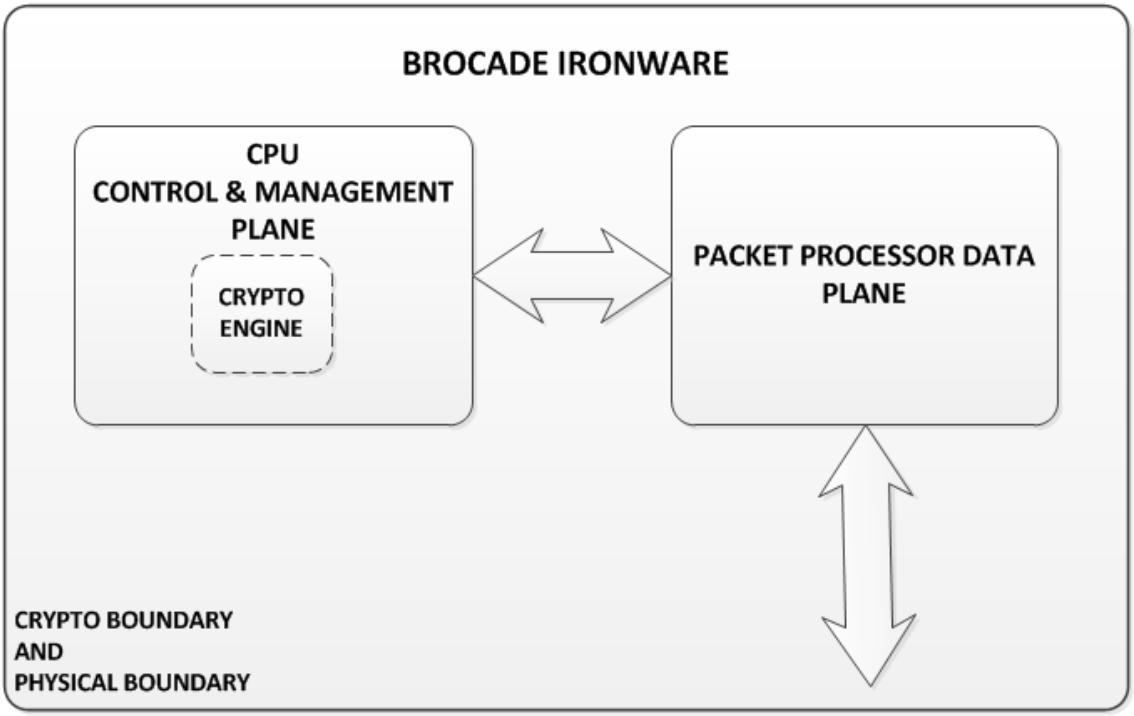

Figure 1 - Block diagram

3 FastIron Firmware

Each of the ICX, FCX and SX series run a different firmware image which is built from the same source code. This firmware image includes the cryptographic functionality described under section 10.

Firmware Version
IronWare R08.0.30b

Table 1 - Firmware Version

Next page →

4 FCX 624 and FCX 648 Series

SKU	MFG Part Number	Brief Description
FCX624S	80-1002388-08	24-Port 1GbE, 2X16G stackable switch
FCX624S-HPOE-ADV	80-1002715-08	24-Port 1GbE, HPOE, 2X16G stackable, ADV L3 switch
FCX624S-F-ADV	80-1002727-07	24-Port, FE/GE SFP, 2X16G stackable, ADV L3 switch
FCX648S	80-1002392-08	48-Port 1GbE, 2X16 stackable switch
FCX648S-HPOE	80-1002391-10	48-Port 1GbE, HPOE, 2x16G stackable switch
FCX648S-HPOE-ADV	80-1002716-10	48-Port 1GbE, HPOE, 2x16G stackable, ADV L3 switch
XBR-000195	80-1002006-02	FIPS Kit containing tamper evident labels to be affixed to the module per Appendix A: Tamper Evident Label application in this document. All SKUs listed above utilize this kit to satisfy the physical security requirements

Table 2 - FCX Part Numbers Product Family Part Numbers of Validated Cryptographic Modules

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

Table 3 - FCX 624 and FCX 628 Optional Component Part Numbers

Module	Configuration 1, SKUs (Count)
FCX 624S (see note A)	Base: FCX624S Interface module: FCX-2XG (1) (see note B) License: None
FCX 624S-HPOE-ADV (see note A)	Base: FCX624S-HPOE-ADV Interface module: None License: Advanced L3 license
FCX 624S-F-ADV (see note A)	Base: FCX624S-F-ADV Interface module: FCX-2XG (1) (see note B) License: Advanced L3 license

Table 4 - Validated FCX 624 Series Configurations

NOTES:

A - See Table 2 for MFG Part number.

B - See Table 3 for MFG Part number.

Module	Configuration 1, SKUs (Count)
FCX 648S (see note A)	Base: FCX648S Interface module: None License: None
FCX 648S-HPOE (see note A)	Base: FCX648S-HPOE Interface module: FCX-2XG (1) (see note B) License: None
FCX 648S-HPOE-ADV (see note A)	Base: FCX648S-HPOE-ADV Interface module: FCX-2XG (1) (see note B) License: Advanced L3 license

Table 5 - Validated FCX 648 Series Configurations

NOTES:

A - See Table 2 for MFG Part number.

B - See Table 3 for MFG Part number.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

FCX 624 models

Figure, below, illustrates the FCX 624S cryptographic module.

Figure 2 - FCX 624S with FCX-2XG module

Figure, below, illustrates the FCX 624S-HPOE-ADV cryptographic module.

Figure 3 - FCX 624S-HPOE-ADV with FCX-2XG module

Figure, below, illustrates the FCX 624S-F-ADV cryptographic module.

Figure 4 - FCX 624S-F-ADV with FCX-2XG module

NOTES:

The following SKUs are physically equivalent:

- FCX624S
- FCX624S-HPOE-ADV
- FCX624S-F-ADV

Next page →

FCX 648 models

Figure, below, illustrates the FCX 648S cryptographic module.

Figure 5 - FCX 648S with FCX-2XG module

Figure, below, illustrates the FCX 648S-HPOE and FCX 648S-HPOE-ADV cryptographic modules.

Figure 6 - FCX 648S-HPOE and FCX 648-HPOE-ADV with FCX-2XG module

NOTES:

The following SKUs are physically equivalent:

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

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

5 ICX 6450 Series

SKU	MFG Part Number	Brief Description
ICX6450-24	80-1005997-03	24-port 1G Switch, 2x1G SFP+ & 2x1G/10G SFP+ Uplink/Stacking Ports
ICX6450-24P	80-1005996-04	24-port 1G Switch PoE+ 390W, 2x1G SFP+ & 2x1G/10G SFP+ Uplink/Stacking Ports
ICX6450-48	80-1005999-04	48-port 1G Switch, 2x1G SFP+ & 2x1G/10G SFP+ Uplink/Stacking Ports
ICX6450-48P	80-1005998-04	48-port 1G Switch PoE+ 780W, 2x1G SFP+ & 2x1G/10G SFP+ Uplink/Stacking Ports
ICX6450-C12-PD	80-1007578-01	12-port 1G Compact Switch (4 PoE+), 2X100M/1G SFP, 2X100M/1G Copper Uplinks, Fanless, Layer 3
XBR-000195	80-1002006-02	FIPS Kit containing tamper evident labels to be affixed to the module per Appendix A: Tamper Evident Label application in this document. All SKUs listed above utilize this kit to satisfy the physical security requirements

Table 6 - ICX 6450 Switch Family Part Numbers of Validated Cryptographic Modules

Figure 7 through Figure 11 illustrates the ICX 6450-24 and ICX 6450-24P cryptographic module (See Table 6 - ICX 6450 Switch Family Part Numbers of Validated Cryptographic Modules)

Figure 7 - Front/top side of the ICX 6450-24P (equivalent to the ICX 6450-24 configuration)

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Figure 8 - Back side of the ICX 6450-24P (equivalent to the ICX 6450-24 configuration)

Figure 9 - Left side of the ICX 6450-24P (equivalent to the ICX 6450-24 configuration)

Figure 10 - Right side of the ICX 6450-24P (equivalent to the ICX 6450-24 configuration)

Figure 11 - Bottom side of the ICX 6450-24P (equivalent to the ICX 6450-24 configuration)

Figure 12 through Figure 17 illustrates the ICX 6450-48 and ICX 6450-48P cryptographic modules (See Table 6 - ICX 6450 Switch Family Part Numbers of Validated Cryptographic Modules).

Figure 12 - Front/top side of the ICX 6450-48P (equivalent to the ICX 6450-48 configuration)

Figure 13 - Back side of the ICX 6450-48P

Figure 14 - Back side of the ICX 6450-48

Next page →

Figure 15 - Left side of the ICX 6450-48P (equivalent to the ICX 6450-48 configuration)

Figure 16 - Right side of the ICX 6450-48P (equivalent to the ICX 6450-48 configuration)

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Figure 17 - Bottom side of the ICX 6450-48P (equivalent to the ICX 6450-48 configuration)

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Figure 18 through Figure 22 illustrates the ICX 6450-C12-PD cryptographic module (See Table 6 - ICX 6450 Switch Family Part Numbers of Validated Cryptographic Modules).

Figure 18 - Front and top side of the module

Figure 19 - Left side with vents

Figure 20 - Back side with power supply

Figure 21 - Right side with vents

Figure 22 - Bottom side of module

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

6 ICX 7250 Series

Each ICX7250 device validated within this implementation includes the following:

SKU	MFG Part Number	Brief Description
ICX7250-24P	80-1008381-02	24 Ports POE+ 8X1G SFP+
ICX7250-24G	80-1008379-02	24 Ports 4X1G SFP
ICX7250-24	80-1008380-02	24 Ports 8X1G SFP+
ICX7250-48P	80-1008386-02	48 Ports POE+ 8X1G SFP+
ICX7250-48	80-1008384-02	48 Ports 8X1G SFP+

Table 7 - ICX7250 Switch Family Part Numbers of Validated Cryptographic Modules

Figure 23 through Figure 28 illustrates a Brocade ICX7250-24P cryptographic module:

Figure 23 - Front/top side of the module ICX7250-24P

Figure 24 - Back side of the module ICX7250-24P

Figure 25 - Right side of the module ICX7250-24P

Figure 26 - Left side of the module ICX7250-24P

Figure 27 - Top side of the module ICX7250-24P

Figure 28 - Bottom side of the module ICX7250-24P

Figure 29 through Figure 34 illustrates a Brocade ICX7250-24G cryptographic module:

Figure 29 - Front/top side of the module ICX7250-24G

Figure 30 - Back side of the module ICX7250-24G

Figure 31 - Right side of the module ICX7250-24G

Figure 32 - Left side of the module ICX7250-24G

Figure 33 - Top side of the module ICX7250-24G

Figure 34 - Bottom side of the module ICX7250-24G

Figure 35 through Figure 40 illustrate a Brocade ICX7250-24 cryptographic module:

Figure 35 - Front/top side of the module ICX7250-24

Figure 36 - Back side of the module ICX7250-24

Figure 37 - Right side of the module ICX7250-24

Figure 38 - Left side of the module ICX7250-24

Figure 39 - Top side of the module ICX7250-24

Figure 40 - Bottom side of the module ICX7250-24

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Figure 41 through Figure 46 illustrate a Brocade ICX7250-48P cryptographic module:

Figure 41 - Front/top side of the module ICX7250-48P

Figure 42 - Back side of the module ICX7250-48P

Figure 43 - Right side of the module ICX7250-48P

Figure 44 - Left side of the module ICX7250-48P

Figure 45 - Top side of the module ICX7250-48P

Figure 46 - Bottom side of the module ICX7250-48P

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Figure 47 through Figure 52 illustrate a Brocade ICX7250-48 cryptographic module:

Figure 47 - Front/top side of the module ICX7250-48

Figure 48 - Back side of the module ICX7250-48

Figure 49 - Right side of the module ICX7250-48

Figure 50 - Left side of the module ICX7250-48

Figure 51 - Top side of the module ICX7250-48

Figure 52 - Bottom side of the module ICX7250-48

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

7 ICX 7750 Series

Each ICX 7750 Series device validated within this implementation includes the following ICX modules:

SKU	MFG Part Number	Brief Description
RPS9+I	80-1007871-01	500 W AC power supply; power-supply-side intake (port-side exhaust) airflow
RPS9+E	80-1007870-01	500 W AC power supply; power-supply-side exhaust (port-side intake) airflow
ICX7750-FAN-I	80-1007738-01	Fan kit of 4; fan-side intake (port-side exhaust) airflow
ICX7750-FAN-E	80-1007737-01	Fan kit of 4; fan-side exhaust (port-side intake) airflow
ICX7750-FAN-I- SINGLE	80-1007761-01	Fan single unit; fan-side intake (port-side exhaust) airflow
ICX7750-FAN-E- SINGLE	80-1007760-01	Fan single unit; fan-side exhaust (port-side intake) airflow
ICX7750-6Q	80-1007632-01	Brocade ICX 7750 with 6 40 GbE QSFP module for use in Brocade ICX 7750- 48F, 7750-48C, or 7750-26Q

Table 8 - Components of the ICX 7750 Series

SKU	MFG Part Number	Brief Description
ICX7750-48F	80-1007607-01	Brocade ICX 7750 with 48 1/10 GbE SFP+ ports, 6 40 GbE QSFP ports and modular interface slot. No power supplies or fan units (need to be ordered separately)
ICX7750-48C	80-1007608-01	Brocade ICX 7750 with 48 1/10 GbE RJ-45 10GBASE-T ports, 6 40 GbE QSFP ports and modular interface slot. No power supplies or fan units (need to be ordered separately).
ICX7750-26Q	80-1007609-01	Brocade ICX 7750 with 26 40 GbE QSFP ports and modular interface slot. No power supplies or fan units (need to be ordered separately).
XBR-000195	80-1002006-02	FIPS Kit containing tamper evident labels to be affixed to the module per Appendix A: Tamper Evident Label application in this document. All SKUs listed above utilize this kit to satisfy the physical security requirements

Table 9 – Base units for ICX 7750 Series

Next page →

Configuration	SKU	MFG Part Number	Quantity	Brief Description
ICX 7750 Configuration 1	ICX7750-48F	80-1007607-01	1	Brocade ICX 7750 with 48 1/10 GbE SFP+ ports, 6 40 GbE QSFP ports and modular interface slot. No power supplies or fan units (need to be ordered separately).
	RPS9+E	80-1007870-01	2	500 W AC power supply; power-supply-side exhaust (port-side intake) airflow
	ICX7750-FAN-E	80-1007737-01	1	Fan kit of 4; fan-side exhaust (port-side intake) airflow
	ICX7750-6Q	80-1007632-01	1	Brocade ICX 7750 with 6 40 GbE QSFP module
ICX 7750 Configuration 2	ICX7750-48C	80-1007608-01	1	Brocade ICX 7750 with 48 1/10 GbE RJ-45 10GBASE-T ports, 6 40 GbE QSFP ports and modular interface slot. No power supplies or fan units (need to be ordered separately).
	RPS9+E	80-1007870-01	2	500 W AC power supply; power-supply-side exhaust (port-side intake) airflow
	ICX7750-FAN-E	80-1007737-01	1	Fan kit of 4; fan-side exhaust (port-side intake) airflow
	ICX7750-6Q	80-1007632-01	1	Brocade ICX 7750 with 6 40 GbE QSFP module
ICX 7750 Configuration 3	ICX7750-26Q	80-1007609-01	1	Brocade ICX 7750 with 26 40 GbE QSFP ports and modular interface slot. No power supplies or fan units (need to be ordered separately).
	RPS9+E	80-1007870-01	2	500 W AC power supply; power-supply-side exhaust (port-side intake) airflow
	ICX7750-FAN-E	80-1007737-01	1	Fan kit of 4; fan-side exhaust (port-side intake) airflow
	ICX7750-6Q	80-1007632-01	1	Brocade ICX 7750 with 6 40 GbE QSFP module
	XBR-000195	80-1002006-02		FIPS Kit containing tamper evident labels to be affixed to the module per Appendix A: Tamper Evident Label application in this document. All SKUs listed above utilize this kit to satisfy the physical security requirements

Table 10 - ICX 7750 Switch Family Part Numbers of Validated Cryptographic Modules

Figure 53 through Figure 57 illustrates an ICX 7750-48F cryptographic module

Figure 53 - Front/top side of the ICX 7750-48F

Figure 54 - Back side of the ICX 7750-48F with optional ICX7750-6Q module

Figure 55 - Left side of the ICX 7750-48F

Figure 56 - Right side of the ICX 7750-48F

Next page →

Figure 57 - Bottom side of the ICX 7750-48F

Figure 58 through Figure 62 illustrates an ICX 7750-48C cryptographic module

Figure 58 - Front/top side of the ICX 7750-48C

Figure 59 - Back side of the ICX 7750-48C with optional ICX7750-6Q module

Figure 60 - Left side of the ICX 7750-48C

Figure 61 - Right side of the Brocade ICX 7750-48C

Figure 62 - Bottom side of the Brocade ICX 7750-48C

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Figure 63 through Figure 67 illustrates an ICX 7750-26Q cryptographic module

Figure 63 - Front/top side of the ICX 7750-26Q

Figure 64 - Back side of the ICX 7750-26Q with optional ICX7750-6Q module

Figure 65 - Left side of the ICX 7750-26Q

Figure 66 - Right side of the ICX 7750-26Q

Next page →

Figure 67 - Bottom side of the ICX 7750-26Q

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

8 SX 800 and SX 1600 Series

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

SKU	MFG Part Number		Brief Description
FI-SX800-S	80-1003050-03	80-1007143-03	FastIron SX 800 CHASSIS
FI-SX1600-AC	80-1002764-02	80-1007137-02	FastIron SX 1600, 16 slot, 2 SX-FISF, 2 AC Power Supplies (bundled SKU)

Table 11 - FastIron SX Part Numbers

SKU	MFG Part Number	Brief Description
SX-FISF	80-1002957-03	Switch Fabric module for the FI SX 800 & FI SX 1600
SX-FI-2XGMR-XL	80-1006607-01	FI SX 2PRT G3 10GE XL MGMT MOD
SX-FI-ZMR-XL	80-1006486-02	FastIron SX XL management module, No 10G ports
SX-ACPWR-SYS	80-1003883-02	FSX AC 90-240 VAC SYSTEM POWER SUPPLY
N/A	11456-005	Filler panel – sheet metal, FAB, line card slot blank
N/A	11457-006	Filler panel – sheet metal, FAB, management blank, SDX, RoHS
N/A	18072-004	Filler panel – sheet metal assembly, PU BLANK, SX/SDX

Table 12 - Components of the SX 800 and SX 1600

Module	Configuration 1, SKUs (Count)
SX 800 (with AC power; see note C)	Base: FI-SX800-S chassis (see note A) Management module: SX-FI-ZMR-XL (2), (see note B) Switch Fabric: SX-FISF (2) (see note B) License: None Power Supply: SX-ACPWR-SYS (1) (see note B)

Table 13 - Validated SX 800 Series Configurations

Notes:

A - See Table 11 for MFG Part numbers.

B - See Table 12 for MFG Part numbers.

C - Any unused and open slots must be covered using filler panels, located in Table 12 (Part Numbers 11456-005, 11457-006 or 18072-004)

Model	Configuration 1, SKUs (Count)
SX 1600 (with AC power; see note C)	Base: FI-SX1600-AC chassis (see note A) Management module: SX-FI-2XGMR-XL (2) (see note B) Switch Fabric: SX-FISF (2) (see note B) License: None Power Supply: SX-ACPWR-SYS (2) (see note B)

Table 14 - Validated SX 1600 Series Configurations

Notes:

A - *See Table 11 for MFG Part numbers.

B - **See Table 12 for MFG Part numbers.

C - Any unused and open slots must be covered using filler panels, located in Table 12 (Part Numbers 11456-005, 11457-006 or 18072-004)

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Figure 68 through Figure 73 illustrate Brocade SX800 with SX-FI-ZMR-XL and Brocade SX800 with SX-FI-2XGMR-XL

Figure 68 - Front side view of the Brocade SX800 with SX-FI-ZMR-XL

Figure 69 - Front side view of the Brocade SX800 with SX-FI-2XGMR-XL

Next page →

Figure 70 - Bottom view of the Brocade SX800

Figure 71 - Back side view of the Brocade SX800

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Figure 72 - Left side view of the Brocade SX800

Figure 73 - Right side view of the Brocade SX800

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Figure 74 through Figure 79 illustrate Brocade SX1600 with SX-FI-ZMR-XL and Brocade SX1600 with SX-FX-2XGMR-XL

Figure 74 - Front side view of the Brocade SX1600 with SX-FI-ZMR-XL

Figure 75 - Front side view of the Brocade SX1600 with SX-FX-2XGMR-XL

Figure 76 - Right side view of the Brocade SX1600

Figure 77 - Back side view of the Brocade SX1600 with fans and power supply

Next page →

Figure 78 - Left side view of the Brocade SX1600

Figure 79 - Bottom view of the Brocade SX1600

Next page →

9 Ports and Interfaces

9.1 FCX 624 and FCX 648 Series

Each FCX 624/648 device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces that provide for Data Input, Data Output, Control Input, and Status Output.

While not part of this validation, the FCX 624/648 devices provide a range of physical network ports. The series supports both copper and fiber connectors with some models supporting combination ports. All models within the scope of this evaluation support 10G uplink ports for stacking devices. All models have a management port (also known as out-of-band management port; a Gigabit Ethernet RJ-45 connector) and a console port (RJ-45 serial connector).

See left column of Table 15 which summarizes the physical ports provided by FCX 624/648 devices. Also, see right column of Table 15 which shows the correspondence between the physical interfaces of a FCX 624/648 device and the logical interfaces defined in FIPS 140-2.

FCX 624/648 Port mapping to logical interface

Physical Port	Logical Interface
SFP ports (FCX-2XG Ethernet Uplink Module)	Data input/Data output, Status output
SFP ports	Data input/Data output, Status output
10/100/1000 Mbps RJ-45 ports	Data input/Data output, Status output
AC socket	Power
Management port	Control input, Status output
Console port	Control input, Status output
Reset	Control input
LED	Status output
16 Gbps CX4 stacking ports	Not Applicable; Latent Interface disabled in the FIPS Approved Mode.

Table 15 – FCX 624/648 Port mapping to logical interface

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

FCX 624/648 Series Physical Port LED Status

LED	Condition	Status
Ethernet Ports 24-port and 48-port models	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 24-port and 48- port models	On (Green)	The port is providing HPOE power to a connected device.
	Off	The port is not providing HPOE power.
SFP (Link LED)	On (Flashing Green)	The SFP port has established a valid link. Flashing indicates that the port is transmitting and receiving user packets.
	Off	A link is not established with a remote port.
SFP (Speed LED)	On (Green)	The SFP port is operating at 1000 Mbps.
	On (Amber)	The SFP port is operating at 100 Mbps.
		A link is not established with a remote port.

Table 16 – FCX 624/648 Series Physical Port LED Status

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

FCX 624/648 Series System LED Status

LED	Condition	Status
PS1	On (Green)	Power supply is operating normally.
	On (Amber)	Power supply fault detected.
	Off	Power supply is off or experience a system failure.
PS2	On (Green)	Power supply is operating normally.
	On (Amber)	Power supply fault detected.
	Off	Power supply is off or experience a system failure.
Diag (Diagnostic)	On (Flashing Green)	System self-diagnostic test is in progress.
	On (Green)	System self-diagnostic test successfully completed.
	On (Amber)	System self-diagnostic test detected a fault.
A (Active)	On (Green)	The device is the active controller.
	On (Amber)	The device is the standby controller.
	Off	The device is operating as a stack member or is in standalone mode.
S (Standby)	On (Green)	The device is the active controller.
	On (Amber)	The device is the standby controller.
	Off	The device is operating as a stack member or is in standalone mode.
Up link	On (Green)	Up link is operating properly.
	Off	Up link has failed or there is no link.
Down Link	On (Green)	Down link is operating properly.
	Off	Down link has failed or there is no link.
Stack ID (1-8)	On (Green)	Indicates the device stack ID.

Table 17 – FCX 624/648 Series System LED Status

FCX 624/648 Series Power Module LED Status

LED	Condition	Status
DC OK	On (Green)	DC output OK.
DC OK	On (Red)	DC output failure.
AC OK	On (Green)	AC input OK.
AC OK	On (Red)	AC input failure.

Table 18 – FCX 624/648 Series Power Module LED Status

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

9.2 ICX 6450 Series

Each ICX 6450 device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces that provide for Data Input, Data Output, Control Input, and Status Output.

The ICX 6450 devices provide a range of physical network ports. The series supports both copper and fiber connectors with some models supporting combination ports. Some models support uplink ports for stacking devices. Most models have a management port (also known as out-of-band management port; Gigabit Ethernet RJ-45 connector) and a console port (RJ-45 serial connector).

Table 19 shows the correspondence between the physical interfaces of an ICX 6450 device and the logical interfaces defined in FIPS 140-2.

Mapping ICX 6450 physical ports to logical interfaces

Physical Port	Logical Interface
SFP/SFP+ ports	Data input/Data output, Status output
10/100/1000 Mbps RJ-45 ports	Data input/Data output, Status output
AC socket	Power
External power supply connector (EPS) (The ICX6450-24, ICX6450-24P and ICX6450-48 have one EPS connector. The ICX 6450-48P has two EPS connectors)	Power
Management port	Control input, Status output
Console port	Control input, Status output
Reset	Control input
LED	Status output

Table 19 - ICX 6450 Port mapping to logical interface

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Physical ports' LED Status on ICX 6450 Series

LED	Condition	Status
Ethernet Ports 24-port and 48-port models	On/Flashing Green	The port has established a valid link at 10, 100 or 1000 Mbps. Flashing indicates the port is transmitting and receiving user packets.
	Off	A link is not established with a remote port.
PoE/PoE+ 24-port and 48-port models	On/Green	The port is providing PoE or PoE+ power to a connected device.
	Off	The port is not providing PoE or PoE+ power.
SFP/SFP+ (X1 – X4) for ICX 6450 devices	On/Flashing Green	The SFP port is operating at 10 Gbps. Flashing indicates the port is transmitting and receiving user packets at 10 Gbps.
	On/Flashing Yellow	The SFP port is operating at 1 Gbps. Flashing indicates the port is transmitting and receiving user packets at 1 Gbps.
	Off	A link is not established with a remote port.

Table 20 - ICX 6450 Series Physical Port LED Status

Management port (also known as out-of-band management port) LED Status ICX 6450 Series

LED	Condition	Status
Management port (2 LEDs)	Off (both LEDs)	Offline.
	On/Flashing (left side)	Link-up. Flashing indicates the port is transmitting and receiving user packets.
	On/Green (right side)	1 Gbps Link-up.
	Right LED off, left LED on or flashing	10/100 Mbps Link-up. Flashing indicates the port is transmitting and receiving user packets.

Table 21 - ICX 6450 Series Management port LED Status

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

LED Status on ICX 6450 Series devices

LED	Condition	Status
EPS1 and EPS2 (External Power Supply status for ICX 6450-48P devices only)	Green	EPS1 and EPS2 power supplies are operating normally.
	Yellow	EPS1 and EPS2 power supply fault.
	Off	EPS1 and EPS2 off or not present.
PWR (Power)	Green	Power supply is operating normally.
	Yellow	Power supply fault.
	Off	Power supply off.
Diag (Diagnostic)	Flashing Green	System self-diagnostic test in progress. System reloads automatically.
	Steady Yellow	System self-diagnostic test has detected a fault (fan, thermal, or any interface fault). The user must reload the system.
MS (Stacking configuration)	Green	The device is the Active controller. Flashing indicates the system is initializing.
	Yellow	Indicates the device is the Standby controller. Flashing indicates the system is in Master arbitration or selection state.
	Off	Device is operating as a stack member, or is in standalone mode.
Uplink (X1 and X2 stacking port status)	Green	Uplink port is operating normally.
	Off	Uplink failed or there is not link.
Downlink (X3 and X4, stacking port status)	Green	Downlink port is operating normally.
	Off	Downlink failed or there is not link.
1-8 (Switch ID in the stack)	Green	Indicates the switch ID in the stack. For ICX 6450 devices, 1 – 8 indicates the switch ID in the stack.

Table 22 - ICX 6450 System LED Status

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

9.3 ICX 7250 Series

An ICX 7250 device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces that provide for Data Input, Data Output, Control Input, and Status Output.

The ICX 7250 devices provide a range of physical network ports. The series supports both copper and fiber connectors. The ICX 7250 device has one RJ-45 network management port, one mini USB serial console port, and one USB storage port on the front panel.

Table, below, shows the correspondence between the physical interfaces of an ICX 7250 device and the logical interfaces defined in FIPS 140-2.

Physical Port	Logical Interface
SFP+ ports	Data input/Data output, Status output
10/100/1000 Mbps RJ-45 ports	Data input/Data output, Status output
AC socket	Power
Console port (mini USB)	Control input, Status output
Management port	Control input, Status output
Reset	Control input
LED	Status output
USB type-A port	This port is permanently disabled

Table 23 - ICX 7250 Port mapping to logical interface

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Tables, below summarize the physical port LED status provided by ICX 7250 devices.

LED state	Status of hardware
On/Flashing green	The port has established a valid link at 10, 100 or 1000 Mbps. Flashing means the port is transmitting and receiving user packets.
Off	A link is not established with a remote port.

Table 24 ICX 7250 - RJ-45 port LEDs

LED state	Status of hardware
On/Steady green	Port is providing POE power to a connected device.
Off	Port is not providing PoE power

Table 25 - ICX 7250 - 100/1000 Mbps RJ-45 PoE LEDs

LED state	Status of hardware
Off (no light)	The SFP port operates at 1 Gbps. Flashing indicates the port is transmitting and receiving user packets at 1 Gbps.
Off	A link is not established with a remote port.

Table 26 - ICX 7250 24G - SFP port LEDs

LED state	Status of hardware
On/Flashing Green	The SFP+ port is operating at 10 Gbps. Flashing indicates the port is transmitting and receiving user packets at 10 Gbps.
On/Flashing Yellow	The SFP+ port is operating at 1 Gbps. Flashing indicates the port is transmitting and receiving user packets at 1 Gbps.
Off	A link is not established with a remote host

Table 27 - ICX 7250 (except 24G) - 1/10 GbE SFP+ module port LEDs

LED state	Status of hardware
Green	Power supply is operating.
Yellow	Power supply fault.
Off	Power supply off

Table 28 - ICX 7250 – Power LEDs

LED state	Status of hardware
Green	EPS1 and EPS2 power supplies are operating normally.
Yellow	EPS1 and EPS2 power supply fault
Off	EPS1 and EPS2 off or not present

Table 29 - ICX 7250 – EPS1 and EPS2 port LEDs

LED state	Status of hardware
Flashing Green	System self-diagnostic test in progress. System reloads automatically
Steady Yellow	System self-diagnostic test has detected a fault. (Fan, thermal, or any interface fault.) The user must reload the system.

Table 30 - ICX 7250 - DIAG LED

LED state	Status of hardware
Green	The device is the Active controller. Flashing indicates the system is initializing
Yellow	Indicates the device is the Standby controller. Flashing indicates the system is in Master arbitration or selection state
Off	Device is operating as a stack member, or is in standalone mode

Table 31 - ICX 7250 - MS LED

LED state	Status of hardware
Green	Uplink port is operating normally
Off	Uplink has failed or there is no link

Table 32 - ICX 7250 - UPLINK LED

LED state	Status of hardware
Green	Downlink port is operating normally
Off	Downlink has failed or not present

Table 33 - ICX 7250 - DOWNLINK LED

LED state	Status of hardware
Green	Indicates stack unit identifier.

Table 34 - ICX 7250 - Stack ID LEDs

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

9.4 ICX 7750 Series

Each ICX 7750 device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces that provide for Data Input, Data Output, Control Input, and Status Output.

The ICX 7750 devices provide a range of physical network ports. The series supports both copper and fiber connectors with some models supporting combination ports. Some models support uplink ports for stacking devices. Most models have a management port (also known as out-of-band management port; Gigabit Ethernet RJ-45 connector) and a console port (mini USB serial connector).

Table 35 and Table 36 show the correspondence between the physical interfaces of an ICX 7750 device and the logical interfaces defined in FIPS 140-2.

Physical Port	Logical Interface
SFP ports	Data input/Data output, Status output
QSFP ports	Data input/Data output, Status output
10/100/1000 Mbps RJ-45 ports (see note 1)	Data input/Data output, Status output
AC socket	Power
External power supply connector	Power
Console port (mini USB)	Control input, Status output
Management port	Control input, Status output
Reset	Control input
LED	Status output
USB type-A port	This port is permanently disabled

Table 35 - ICX 7750 Port mapping to logical interface

Note:

1. ICX 7750-26Q and ICX 7750-48F do not support 10/100/1000 Mbps RJ-45 ports

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

LED	Condition	Status
Management Port (Left or Right)	Flashing	There is traffic and packets are being transmitted and received.
Management Port (Left or Right)	Steady	No traffic is being transmitted, but the link is active.
	Off	External cable is not present.
1/10 GbE Port (RJ45 and SFP+)	Steady Green	Link is up in 10 GbE mode.
	Flashing Green	There is 10 GbE activity (traffic) and packets are being transmitted or received.
	Steady Amber	Link is up in 1 GbE mode.
	Flashing Amber	There is 1 GbE activity (traffic) and packets are being transmitted or received.
40 GbE (rear port) front port LED	Off	Disabled.
	Steady Green	Link is up in 40 GbE mode.
	Flashing Green	Active traffic. Packets are being transmitted or received.
4x10 GbE (rear port) front port LED	Off	Disabled.
	Steady Amber	Link is up in 10 GbE mode.
	Flashing Amber	Active traffic. Packets are being transmitted or received.
10/100/1000 Mbps HA Ethernet port LEDs	Off	Not Cabled.
	Steady green	Link is up in 1 GbE mode.
	Blinking Green	There is 1 GbE traffic and packets are being transmitted or received.
	Steady Amber	Link is up in 10/100 Mbps mode.
	Blinking Amber	There is 10/100 Mbps traffic and packets are being transmitted or received.

Table 36 - ICX 7750 Series Physical Port LED Status

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

LED	Condition	Status
PSU1 and PSU2	Steady Green	PSU is on and operating normally.
	Steady Amber	PSU power supply fault.
	Off	PSU is off or not present.
Diag (Diagnostic)	Flashing Green	System self-diagnostic test in progress. System reloads automatically.
	Steady Amber	System self-diagnostic test has detected a fault.
	Steady Green	System self-diagnostic test completed successfully. Device reboots and turns the LED off.
	Off	Diagnostic is off.
MS LED	Off	Stacking mode is enabled and the switch is a stack member, or the switch is operating in stand-alone mode.

Table 37 - ICX 7750 System LED Status

LED	Condition	Status
MS LED	Steady Green	Stacking mode is enabled and the switch is the stack master.
	Steady Amber	Stacking mode is enabled and the switch is in slave mode.
HA LED	Off	System high-availability mode is disabled.
	Steady Green	System is operating in high-availability mode.
	Steady Amber	System is preparing to operate in high- availability mode.
RDNT LED	Off	System does not have redundant fans or PSUs installed.
	Steady Green	System is operating in redundant mode.
	Steady Amber	System has redundant fans and PSUs, but software has disabled redundant mode.

Table 38 - ICX 7750 Other LED Status

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

9.5 SX800 and SX1600 Series

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

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 a management port (also known as out-of-band management port; Gigabit Ethernet RJ-45 connector) and a console port (RJ-45 serial connector).

Table 39 summarizes the physical ports provided by the SX-FI-ZMR-X and SX-FI-2XGMR-XL management modules, and shows the correspondence between the physical interfaces of the management modules and the logical interfaces defined in FIPS 140-2.

Physical Port	Logical Interface
Management port (10/100/1000 Mbps Ethernet port)	Data input/Data output, Status output
Console port	Control input, Status output
10Ge G3 port (see note 1)	Data input/Data output, Status output
USB port	Permanently disabled
Reset	Control input
LED	Status output

Table 39 - SX-FI-ZMR-XL and SX-FI-2XGMR-XL Port mapping to logical interface

Note:

1. SX-FI-ZMR-XL management module does not support 10Ge G3 port.

LED	Condition	Status
PWR (Power)	On (Green)	Module is receiving power.
	Off	Module is not receiving power.

Table 40 - SX-FI-ZMR-XL and SX-FI-2XGMR-XL LED Status

Next page →

LED	Condition	Status
Active	On (Green)	The module is the active management module.
	Off	The module is not the active management module.
GMT-Link (Right-most Ethernet port LED)	On (Green)	10/100/1000.
	Blinking	The port is transmitting and receiving traffic.
	Off	No port connection exists.
Sync-Link (Left-most Ethernet port LED)	On (Green)	Two management modules are present.
	Blinking	Active and Standby modules are syncing.
	Off	No port connection exists.

Table 41 - SX-FI-ZMR-XL and SX-FI-2XGMR-XL LED Link Status

LED	Condition	Status
PWR	On (Green)	Module is receiving power.
	Off	Module is not receiving power.
Active	On (Green)	The module is functioning properly.
	Off	The module is not functioning properly.

Table 42 - SX-FISF Switch Fabric LED Status

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

10 Modes of Operation

FCX 624/648 devices, ICX 6610 devices, ICX 6450 devices, ICX 7450 devices, ICX 7250 devices, ICX 7750 devices, and SX800/1600 devices (aka Brocade cryptographic modules) have two modes of operation: FIPS Approved mode and non-Approved mode. Section 10.3 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 13.2 FIPS Approved Mode describes how to invoke FIPS Approved mode.

10.1 Module Validation Level

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

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
Operational Environment	N/A
Cryptographic Key Management	2
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 43 - Security Requirements and Levels

NOTE: Please see section 17, Appendix B: Critical Security Parameters, for more details on CSPs and Keys.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

10.2 Roles

In FIPS Approved mode, Brocade cryptographic modules support three roles: Crypto Officer, Port Configuration Administrator and User:

1. Crypto Officer Role (Super User): The Crypto Officer Role on the device in FIPS Approved mode is equivalent to the administrator role super-user in non-FIPS mode the Crypto Officer Role has complete access to the system. The Crypto Officer is the only role that can perform firmware loading.

2. Port Configuration Administrator Role (Port Configuration): 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 (Read Only): The User Role on the device in FIPS Approved mode has read-only privileges and no configuration mode access (user).

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

Section 11.2 describes the authentication policy for user roles.

10.3 Services

NOTE: Please see section 17, Appendix B: Critical Security Parameters, for more details on CSPs and Keys.

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 to determine if the network connections are functioning properly. Unauthenticated operators can also perform self-tests via a 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 11.2 Authentication. Brocade cryptographic modules provide services for remote communication (SSHv2, Secure Web Management over TLS v1.0, TLS v1.1, TLS v1.2, 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 parameters (CSP) associated with the service. Table 44 summarizes the available FIPS Approved cryptographic functions. Table 45 lists cryptographic functions that while not FIPS Approved are allowed in FIPS Approved mode of operation.

NOTE: Table 48 to Table 52 list the FIPS Approved algorithms with their full modes and key sizes along with their associated CAVP certificate number.

Table, below, lists FIPS Approved cryptographic algorithms allowed in FIPS Approved mode:

Label	Cryptographic Algorithm
AES	Advanced Encryption Algorithm (CBC and CFB)
SHA	Secure Hash Algorithm
HMAC	Keyed-Hash Message Authentication code
DRBG	Deterministic Random Bit Generator
RSA	Rivest Shamir Adleman Signature Algorithm
CVL	SSHv2, TLS and SNMPv3 Key Derivation Function

Table 44 – FIPS Approved Cryptographic Algorithms allowed in FIPS Approved mode

Table, below, lists FIPS non-Approved cryptographic algorithms available in FIPS Approved Mode:

Label	Cryptographic Algorithm
DH KA	Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
HMAC-MD5	Used to support RADIUS for operator authentication only (HMAC-MD5 is not exposed to the operator)
KW	RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
MD5	Used in the TLS v1.0 KDF in FIPS mode as per SP800-135 (MD5 is not exposed to the operator)
MD5	Message-Digest algorithm - Used in TACACS+ for operator authentication only (MD5 is not exposed to the operator)
NDRNG	Generation of seeds for DRBG

Table 45 - FIPS non-Approved Cryptographic Algorithms available in FIPS Approved Mode

Next page →

Table, below, lists FIPS non-Approved cryptographic algorithms and protocols only available in non-FIPS Approved Mode:

Service / Algorithm	Role	Description
AES (non-compliant)	This is not a user accessible service	AES (non-compliant) encryption/decryption. Modes: AES-ECB (non-compliant), AES-CTR (non-compliant) Key sizes: 128, 192 and 256-bit
BGP	Crypto Officer Role, User Role	Border Gateway Protocol (BGP) is a standardized exterior gateway protocol. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
DSA	This is not a user accessible service	DSA digital signature generation/verification only available in non-FIPS mode. Modes: PQG(ver), PQG(gen), SIG(Ver), SIG(gen), KEYGEN(Y) Key sizes: 1024-bit
HTTP	Crypto Officer Role, User Role	Hyper Text Transport Protocol. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
HTTPS	Crypto Officer Role, User Role	Hyper Text Transport Protocol Secure. Cipher Suites: AES-128-GCM (non-compliant); AES-256-GCM (non-compliant); AES-128-CBC (non-compliant); AES-256-CBC (non-compliant); SHA-1 (non-compliant); SHA-256 (non-compliant); SHA-384 (non-compliant); RSA (non-compliant); DSA (non-compliant); Diffie-Hellman; MD5; RC4
MD5	This is not a user accessible service	Message Digest 5 algorithm is used as cryptographic hash function to check for verification of data integrity and wide variety of cryptographic applications. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)

Service / Algorithm	Role	Description
MSTP	Crypto Officer Role, User Role	Multiple Spanning Tree Protocol. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
NTP (Authentication using MD5)	Crypto Officer Role, User Role	Network Time Protocol. Modes: MD5 for authentication Key sizes: 20 bytes
SNMP (SNMPv1, SNMPv2c and SNMPv3)	Crypto Officer Role, User Role	Simple Network Management Protocol. SNMPv1, SNMPv2c and SNMPv3 in noAuthNoPriv, authNoPriv mode SNMPv3 in authPriv mode using DES MD5 Modes: Not Applicable Key sizes: Not Applicable DES Modes: CBC Key sizes: 56-bit AES (non-compliant) Modes: AES-CFB (non-compliant) Key sizes: 128-bit SHA-1 (non-compliant) Modes: SHA-1 (non-compliant) Key sizes: Not Applicable SP800-135 SNMPv3 KDF (non-compliant) Modes: Not Applicable Key sizes: Not Applicable
SSHv2	Crypto Officer Role, User Role	Secure Shell Protocol. Triple-DES (non-compliant) Modes: Triple-DES-ECB (non-compliant), Triple-DES-CBC (non-compliant) Key Size: KO 1 (3-key) AES (non-compliant) Modes: AES-CTR (non-compliant) Key Size: 128, 192 and 256-bit

Service / Algorithm	Role	Description
Syslog	Crypto Officer Role, User Role	Syslog is a standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
TACACS	Crypto Officer Role, User Role	TACACS (Terminal Access Controller Access Control System) is an authentication protocol which allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. Mode: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
TELNET	Crypto-officer Role, Port Configuration Administrator Role, User Role	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). Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)
TFTP (Trivial File Transfer Protocol)	Crypto Officer Role	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. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)

Service / Algorithm	Role	Description
“Two way encryption”	This is not a user accessible service	Base64 Modes: Not Applicable Key sizes: Not Applicable
VRRP/VRRP-E	Crypto Officer Role, User Role	Virtual Router Redundancy Protocol (VRRP) and Virtual Router Redundancy Protocol (VRRP-E) Enhancement. Modes: Layer 3 mode Key sizes: Not Applicable (plaintext; no cryptography)
VSRP	Crypto Officer Role, User Role	Virtual Switch Redundancy Protocol. Modes: Layer 2 mode Key sizes: Not Applicable (plaintext; no cryptography)

Table 46 - FIPS non-Approved Cryptographic Algorithms and Protocols only available in non-FIPS Approved Mode

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

10.4 User Role Services

10.4.1 SSHv2

This service provides a secure session between a Brocade cryptographic module and an SSHv2 client using SSHv2 protocol. Brocade cryptographic modules authenticate an SSHv2 client and provides an encrypted communication channel. An operator may use an SSHv2 session for managing the device via the command line interface.

Brocade cryptographic modules support three kinds of SSHv2 client authentication: password, client public key and keyboard interactive. For password authentication, an operator attempting to establish an SSHv2 session provides a password through the SSHv2 client. The Brocade cryptographic module authenticates operator with passwords stored on the device, on a TACACS+ server, or on a RADIUS server. Section 11.2 Authentication provides authentication details.

The keyboard interactive (KI) authentication goes one step ahead. It allows multiple challenges to be issued by the Brocade cryptographic module, using the backend RADIUS or TACACS+ server, to the SSHv2 client. Only after the SSHv2 client responds correctly to the challenges, will the SSHv2 client get authenticated and proper access is given to the Brocade cryptographic module.

SSHv2 supports Diffie-Hellman (DH) to configure the modulus size on the SSHv2 server for the purpose of key- exchange.

Maximum number of concurrent SSHv2 user sessions supported is 5.

The following encryption algorithms are available for negotiation during the key exchange with an SSHv2 client:

- AES-CBC with a 128-bit key (aes128-cbc),
- AES-CBC with a 256-bit key (aes256-cbc),

All secure hashing is done with SHA 256.

The following MAC algorithms are available for negotiation during the key exchange with an SSHv2 client: (hmac- sha1) HMAC-SHA1 (digest length = key length = 20 bytes)

In User role access, the client is given access to three commands: `enable`, `exit` and `terminal`. The `enable` command allows user to re-authenticate using a different role. If the role is the same, based on the credentials given during the `enable` command, the user has access to a small subset of commands that can perform `ping  traceroute` in addition to `show` commands.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

10.4.2 HTTPS

This service provides a graphical user interface for managing a Brocade cryptographic module over a secure communication channel. Using a web browser, an operator connects to a designated management port on a Brocade cryptographic module. The device negotiates a TLS v1.0/1.1 and v1.2 connection with the browser and authenticates the operator. The device uses HTTP over TLS v1.0/1.1 and v1.2 with cipher suites 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, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, and TLS_DHE_RSA_WITH_AES_256_CBC_SHA256. Brocade switches have the ability to generate RSA 2048 certificates signed with SHA 256.

Maximum number of concurrent HTTPS user sessions supported is 8.

In User role, after successful login, the default HTML page is the same for any role. The user can surf to any page after clicking on any URL. However, this user will not be allowed to make any modifications. If the user presses the 'Modify' button within any page, he will be challenged to re-enter his credentials. The challenge dialog box will not be closed without proper access credentials of the Crypto Officer. After default three attempts, the page 'Protected Object' is displayed, in effect disallowing any changes from the web.

10.4.3 SNMP

SNMPv1 and SNMPv2 services are disabled in FIPS mode and the SNMPv3 service with authentication as MD5 and privacy as DES are also disabled. The SNMPv3 service within User role allows read-only access to the SNMP MIB within the FastIron device. The device does not provide SNMP MIB access to CSPs when operating in FIPS Approved mode. All other MIB objects are made available for use in approved FIPS mode. These other MIB objects provide capability to monitor the various functional entities in the module which are non-security relevant.

10.4.4 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 Brocade cryptographic module 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 the same as the list mentioned in the SSHv2 service.

10.4.5 NTP

The NTP [same as NTPv4] Network Time Protocol configuration and time statistics details can be viewed but not configured.

Next page →

10.5 Port Configuration Administrator Role Services

10.5.1 SSHv2

This service is described in section 10.4.1 above.

The Port Configuration Administrator will have seven commands, which allows this user to run show commands, run ping or trace route. The enable command allows the user to re-authenticate as described in section 10.4.1. Within the configuration mode, this role provides access to all the port configuration commands, e.g. all sub-commands within “interface eth 1/1” command.

10.5.2 HTTPS

This service is described in section 10.4.2 above.

Like the User role, this user will get to view all the web pages. In addition, this operator will be allowed to modify any configuration that is related to an interface. For example, the Configuration->Port page will allow this operator to make changes to individual port properties within the page.

10.5.3 SNMP

The SNMP service is not available for a Port Configuration Administrator Role Service.

10.5.4 Console

This service is described in section 10.4.4 above. 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 the same as those mentioned in the SSHv2 service.

10.5.5 NTP

The NTP [same as NTPv4] Network Time Protocol configuration and time statistics details can be viewed but not configured.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

10.6 Crypto Officer Role Services

10.6.1 SSHv2

In addition to the two methods of authentication, password and keyboard interactive, described in section 10.4.1, SSHv2 service in this role supports RSA public key authentication, in which the device stores a collection of client public keys. Only clients with a private key that corresponds to one of the stored public keys can gain access to the device using SSHv2. After a client's public key is found to match one of the stored public keys, the device will give Crypto Officer access to the entire module.

The Crypto Officer can perform configuration changes to the module (including enabling and disabling MACsec on a per-port basis). This role has full read and write access to the Brocade cryptographic module.

When firmware download is desired, the Crypto Officer shall download firmware download in the primary image and secondary image.

The Crypto Officer can perform zeroization by invoking the firmware command "fips zeroize all" or session termination.

10.6.2 SCP

This is a secure copy service. The service supports both outbound and inbound copies of configuration, binary images, or files. Binary files can be copied and installed similar to TFTP operation (that is, upload from device to host and download from host to device, respectively). SCP automatically uses the authentication methods, encryption algorithm, and MAC algorithm configured for SSHv2. For example, if password authentication is enabled for SSHv2, the user is prompted for a user name and password before SCP allows a file to be transferred. One use of SCP on Brocade cryptographic modules is to copy user digital certificates and host public-private key pairs to the device in support of HTTPS. Other use could be to copy configuration to/from the cryptographic module.

10.6.3 HTTPS

This service is described in section 10.4.2 HTTPS.

In addition to Port Configuration Administrator-role capabilities, the Crypto Officer has complete access to all the web pages and is allowed to make configuration updates through the web pages that support configuration changes.

10.6.4 SNMP

Section 10.4.3, above, describes this service. The SNMP service within Crypto Officer role allows read-write access to only Non-Security Relevant elements of the SNMP MIB within the FastIron device.

10.6.5 Console

Logging in through the CLI service is described in section 10.4.4 above. Console commands provide an authenticated Crypto Officer complete access to all the commands within the Brocade cryptographic module. 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 SSHv2 service, the operator creates a pair of RSA host keys, to configure the authentication scheme for SSHv2 access;

afterwards the operator may securely import additional pairs of RSA host keys as needed over a secured SSHv2 connection. To enable the Web Management service, the operator would securely import a pair of RSA host keys and a digital certificate using corresponding commands (over a secured SSHv2 connection), and enable the HTTPS server.

NOTE: The cryptographic module “does not” support DSA key generation in FIPS mode.

10.6.6 NTP

The NTP [same as NTPv4] Network Time Protocol can be configured to provide cryptographic authentication of messages with the clients/peers, and with its upstream time server. Symmetric key scheme is supported for authentication.

NTPv4 specification (RFC-5905), allows any one of possibly 65,534 message digest keys (excluding zero), each distinguished by a 32-bit key ID, to authenticate an association. The servers and clients involved must agree on the key ID, key type and key to authenticate NTP packets.

NTP service with MD5 key authentication is disabled in FIPS mode.

NTPv4 service with SHA1 key authentication is available upon configuration in FIPS mode.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

11 Policies

NOTE: Please see section 17, Appendix B: Critical Security Parameters, for more details on CSPs and Keys.

11.1 Security Rules

NOTE: If the module has been configured for FIPS Approved mode as described in Section 13.2 below, the Crypto Officer, Port Configuration Administrator and User are required to abide by the restrictions documented in this Section. In the event that the Crypto Officer, Port Configuration Administrator or User violates or attempts to violate such restrictions, the module is in strict violation of this Security Policy and is deemed fully non-compliant and unfit for service to protect sensitive unclassified data with cryptography.

The Brocade cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the FIPS 140-2 Level 2 security requirements. After configuring a FastIron device to operate in FIPS Approved mode, the Crypto Officer must execute the "fips self-tests" command to validate the integrity of the firmware installed on the device. If an error is detected during the self-test, the error must be corrected prior to rebooting the device.

1) The cryptographic module provides role-based authentication.

2) Until the module is placed in a valid role, the operator does not have access to any Critical Security Parameters (CSP).

3) The cryptographic module fully implements DRBG Health Tests performed as part of self-tests, and therefore meets the requirements of SP800-90A Section 11.3.

4) The cryptographic module performs the following tests:

    a) Power up Self-Tests:

        i) Cryptographic Known Answer Tests (KAT):

            (1) Triple-DES KAT (encrypt)

            (2) Triple-DES KAT (decrypt)

            (3) AES-128,192,256-bit key sizes KAT (encrypt) in CBC, ECB, CTR and CFB modes

            (4) AES-128,192,256-bit key sizes KAT (decrypt) in CBC, ECB, CTR and CFB modes

            (5) SHA-1,256,384,512 KAT (Hashing)

            (6) HMAC-SHA-1,256 KAT (Hashing)

            (7) RSA 2048 bit key size KAT (encrypt)

(8) RSA 2048 bit key size KAT (decrypt)

(9) RSA 2048 bit key size, SHA-256,384,512 Hash KAT (signature generation)

(10)RSA 2048 bit key size, SHA-256,384,512 Hash KAT (signature verification)

(11)DRBG KAT

(12)SP800-135 TLS v1.0 KDF KAT

(13)SP800-135 SSHv2 KDF KAT

(14)SP800-135 TLS v1.2 KDF KAT

(15)SP800-135 SNMPv3 KDF KAT

ii) Firmware Integrity Test (CRC 32)

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) Conditional Self-Tests:

i) Continuous Random Number Generator (RNG) test – performed on NDRNG

ii) Continuous Random Number Generator test – performed on DRBG

iii) RSA 2048 SHA-256 Pairwise Consistency Test (Sign/Verify)

iv) RSA 2048 SHA-256 Pairwise Consistency Test (Encrypt/Decrypt)

v) Firmware Load Test: RSA 2048 bit, SHA-256 Signature Verification

vi) Bypass Test: N/A

vii) Manual Key Entry Test: N/A

5) At any time the cryptographic module is in an idle state, the operator can command the module to perform the power-up self-test by executing the "`fips self-tests`" command.

6) Data output to services defined in section 10.3 Services is inhibited during key generation, self-tests, zeroization, and error states.

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

8) Stacking feature shall not be enabled. Usage of the CLI commands, *`stack enable`*, and/or, *`stack secure-setup`*, violates the restrictions set forth in this Security Policy.

9) The following protocols have not been reviewed or tested by the CAVP nor CMVP:
   a) TLS v1.0/1.1
   b) SSHv2
   c) TLS v1.2
   d) SNMPv3

11.1.1 FIPS Fatal Cryptographic Module Failure

When POST is successful, the following messages will be displayed on the console:

```
FIPS Power On Self Tests and KAT tests successful.
Running continuous DRBG check.
Running continuous DRBG check successful.
Pairwise consistency check successful.
fips crypto drbg health check tests ran successful.
Crypto module initialization and Known Answer Test (KAT) Passed.
```

In order to operate a Brocade cryptographic module securely, an operator should be aware of the following rules for FIPS Approved mode of operation:

External communication channels / ports shall not be available before initialization of a Brocade cryptographic module.

Brocade cryptographic modules shall use a FIPS Approved random number generator implementing Algorithm CTR_DRBG. NOTE: Hash_Based DRBG "IS NOT" available within any service used in any mode of operation in this module.

Brocade cryptographic modules shall ensure the random number seed and seed key input do not have the same value. The devices shall generate seed keys and shall not accept a seed key entered manually.

Brocade cryptographic modules shall use FIPS Approved key generation methods:

1) RSA public and private keys in accordance with [ANSI X9.31]

Brocade cryptographic modules shall test prime numbers generated for RSA keys using Miller-Rabin test. See [ANSI X9.31]

Brocade cryptographic modules shall use Approved key establishment techniques:

1) Diffie-Hellman
2) RSA Key Wrapping

Brocade cryptographic modules shall restrict key entry and key generation to authenticated roles.

Brocade cryptographic modules shall not display plaintext secret or private keys. The device shall display "…" in place of plaintext keys.

Brocade cryptographic modules shall use automated methods to realize session keys for SSHv2 and HTTPS. Brocade cryptographic modules shall only perform "get" operations using SNMP.

11.2 Authentication

Brocade cryptographic modules support role-based authentication. A device can perform authentication and authorization (that is, role selection) using TACACS+, RADIUS and local configuration database. Moreover, Brocade cryptographic modules support 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 (Console, SSHv2, Web, SNMP) and the order in which the device tries one or more of the following authentication methods:

1) Line Password Authentication,
2) Enable Password Authentication,
3) Local User Authentication,
4) RADIUS Authentication with exec authorization and command authorization, and
5) 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.

Brocade cryptographic modules allow multiple concurrent operators through SSHv2 and the console, only limited by the system resources.

11.2.1 Line Password Authentication Method

The Line Password Authentication method uses the Telnet password to authenticate an operator.

To use Line Password Authentication, a Crypto Officer must set the Telnet password. Please note that when operating in FIPS mode, Telnet is disabled and Line Password Authentication is not available.

11.2.2 Enable Password Authentication Method

The Enable Password Authentication 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-config password to select the Port Configuration Administrator role. An operator enters the super-user password to select the Crypto Officer Role.

To use Enable Password Authentication, a Crypto Officer must set the password for each privilege level.

11.2.3 Local Password Authentication Method

The Local Password Authentication Method uses a password associated with a user name to authenticate an operator. An operator enters a user name and corresponding password. Brocade cryptographic modules assign the role associated with the user name to the operator when authentication is successful.

To use Local Password Authentication, a Crypto Officer must define user accounts. The definition includes a user name, password, and privilege level (which determines role).

11.2.4 RADIUS Authentication Method

The RADIUS Authentication method uses one or more RADIUS servers to verify user names and passwords. Brocade cryptographic modules prompt 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, a Brocade cryptographic module will send the user name and password information to the next configured RADIUS server.

Brocade cryptographic modules support additional command authorization with RADIUS Authentication. The following events occur when RADIUS command authorization takes place.

1) A user previously authenticated by a RADIUS server enters a command on a Brocade cryptographic module.
2) A Brocade cryptographic module looks at its configuration to see if the command is at a privilege level that requires RADIUS command authorization.
3) If the command belongs to a privilege level that requires authorization, the Brocade cryptographic modules 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 Brocade cryptographic module. 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 Brocade cryptographic module.

To use RADIUS authentication, a Crypto Officer must configure RADIUS server settings along with authentication and authorization settings.

This is a protocol that relies on the strength of TLSv1.2, which is utilizing RSA 2048 with SHA-256 and FIPS Approved cipher suites (please, see list of ciphers in section 10.4.2).

11.2.5 TACACS+ Authentication Method

The TACACS+ Authentication Method uses one or more TACACS+ servers to verify user names and passwords. For TACACS+ Authentication, Brocade cryptographic modules prompt 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+ authentication, a Crypto Officer must configure TACACS+ server settings along with authentication and authorization settings.

11.2.6 Strength of Authentication

Brocade cryptographic modules minimize the likelihood that a random authentication attempt will succeed. The module supports minimum 8 character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore the probability of a random attempt is 1/ 80^8 which is less than 1/1,000,000.

The module enforces a one second delay for each attempted password verification, therefore maximum of 60 attempts per minute, thus the probability of multiple consecutive attempts within a one minute period is 60/80^8 which is less than 1/100,000.

The probability of a successful random guess of a RADIUS or TACACS+ password during a one-minute period is less than 3 in 1,000,000 which is less than 1/100,000 as the authentication message needs to go to the server from the switch and then the response needs to come back to the switch.

For the SNMPv3 secret used for authentication, the module supports minimum 8 character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore the probability of a random attempt is 1/ 80^8 which is less than 1/1,000,000.

The module can process 1 authentication packet per 10 msec. Therefore, the probability of multiple consecutive attempts within a one minute period is 6000/80^8 which is less than 1/100,000.

For the SNMPv3 secret used for privacy, the module supports minimum 12 character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore the probability of a random attempt is 1/ 80^12 which is less than 1/1,000,000.

The module can process 1 authentication packet per 10 msec. Therefore, the probability of multiple consecutive attempts within a one minute period is 6000/80^12 which is less than 1/100,000.

For the NTP secret, the module supports minimum 8 character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18) in passwords. Therefore the probability of a random attempt is 1/ 80^8 which is less than 1/1,000,000.

The module can process 1 authentication packet per 10 msec. Therefore, the probability of multiple consecutive attempts within a one minute period is 6000/80^8 which is less than 1/100,000.

11.2.7 User Roles Access to CSPs and Services

NOTE: Please see section 17, Appendix B: Critical Security Parameters, for more details on CSPs and Keys.

Table, below, summarizes the access operators in each role have to critical security parameters. The table entries have the following meanings:

1) r – Operator can read the value of the item,
2) w - Operator can write a new value for the item,
3) x - Operator can use the value of the item without direct access (for example encrypt with an encryption key)
4) d - Operator can delete the value of the item (zeroize).

Roles →		User					Port Configuration Administrator				Crypto Officer					
Services → / CSP & Keys		SSHv2	HTTPS	SNMP	Console	NTP	SSHv2	HTTPS	Console	NTP	SSHv2	SCP	HTTPS	SNMP	Console	NTP
1	SSHv2 Host RSA Private Key (2048 bit)	x					x				xwd	x			wd	
2	SSHv2 DH Private Key (2048 bit)	x					x				xwd	x			wd	
3	SSHv2 DH Shared Secret Key (2048 bit)	x					x				xd	x			xd	
4	SSHv2/SCP Session Keys (128 and 256 bit AES CBC)	x					x				xd	x			xd	
5	SSHv2/SCP Authentication Key (HMAC-SHA-1)	x					x				xd	x			xd	
6	SSHv2 KDF Internal State	x					x				xd	x			xd	
7	TLS Host RSA Private Key (RSA 2048 bit)		x					x			rwd		x		rwd	
8	TLS Pre-Master Secret		x					x					x		xd	
9	TLS Master Secret		x					x					x		xd	
10	TLS KDF Internal State		x					x			xd		x		xd	
11	TLS Session Key		x					x					x		xd	

Roles →		User					Port Configuration Administrator				Crypto Officer					
Services → / CSP & Keys		SSHv2	HTTPS	SNMP	Console	NTP	SSHv2	HTTPS	Console	NTP	SSHv2	SCP	HTTPS	SNMP	Console	NTP
12	TLS Authentication Key		x					x					xd		xd	
13	DRBG Seed	x	x				x	x			xd	x	x		xd	
14	DRBG Value V	x	x				x	x			xd	x	x		xd	
15	DRBG Key	x	x				x	x			xd	x	x		xd	
16	DRBG Internal State	x	x				x	x			xd	x	x		xd	
17	User Password	x	x	x	x						xrwd	xrwd	xrwd	x	xrwd	
18	Port Administrator Password						x	x	x		xrwd	xrwd	rwd		xrwd	
19	Crypto Officer Password										xrwd	xrwd	xrwd		xrwd	
20	RADIUS Secret	x	x		x		x	x	x		xrwd	xrwd	xrwd		xrwd	
21	TACACS+ Secret	x	x		x		x	x	x		xrwd	xrwd	xrwd		xrwd	
22	Firmware Integrity / Firmware Load RSA Public Key										xd		x		xd	
23	SSHv2 Host RSA Public key	x					x				xrwd	xrw			rwd	
24	SSHv2 Client RSA Public Key	x					x				xrwd	xrwd			xrwd	
25	SSHv2 DH Public Key	x					x				xd	x			xd	
26	SSHv2 DH Peer Public Key	x					x				xd	x			xd	
27	TLS Host Public Key (RSA 2048 bit)		X					x			rwd		x		rwd	
28	TLS Peer Public Key (RSA 2048)		X					x			rwd		x		rwd	
29	SNMPv3 secret	r		r	r		r		r		rwd	rwd		r	rwd	
30	NTP secret	r			r	r	r		r	r	rwd	rwd		r	rw	rwd

Table 47 Access Control Policy and CSP & Public Key access

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

12 Physical Security

In order for a FCX 624/648 device, ICX 6450 device, ICX 7250 devices, ICX 7750 device or SX 800/1600 device to meet FIPS 140-2 Level 2 Physical Security requirements the Crypto Officer must install tamper evident label security seals. Tamper evident label security seals are available for order from Brocade under FIPS Kit (Part Number: XBR-000195). The Crypto Officer shall follow the Brocade FIPS Security Seal application procedures defined in Appendix A of this document prior to operating the module in FIPS mode.

The Crypto 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 Crypto Officer shall maintain a serial number inventory of all used and unused tamper evident label security seals. The Crypto 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 Crypto 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 Crypto Officer is responsible for returning a module to a FIPS approved state after any intentional or unintentional reconfiguration of the physical security measures.

Please refer to Appendix A of this Security Policy document for specific tamper evident seal application instructions.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

13 Mode Status

Brocade cryptographic modules 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 13.1 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 security policy (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 a security policy yet (operational status is off). The command displays the security policy settings.

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

Some shared secrets inherited from non-Approved mode may not be fips compliant and has
to be zeroized. The system needs to be reloaded to operate in FIPS mode.

System Specific:

OS monitor mode access: Disabled

Management Protocol Specific:

Telnet server: 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

SSHv2 RSA Host Keys: Clear

HTTPS RSA Host Keys and Signature: Clear
```

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

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 a security policy (operational status is on). The command displays the policy settings.

```
FIPS mode: Administrative Status: ON, Operational Status: ON
System Specific:
OS monitor mode access: Disabled
Management Protocol Specific:
Telnet server: 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
SSHv2 RSA Host Keys:       Clear
HTTPS RSA Host Keys and Signature:      Clear
```

13.1 FIPS Approved Mode

This section describes FIPS Approved mode of operation and the sequence of actions that place a Brocade cryptographic module in FIPS Approved mode. The first action is to apply tamper evident label security seals to the chassis at the locations specified in the Appendix A of this document.

FIPS Approved mode disables the following:

1) Telnet access including the telnet server command
2) Command *ip ssh scp disable*
3) TFTP access
4) SNMP access to CSP MIB objects
5) Access to all commands within the monitor mode
6) HTTP access including the web-management http command
7) Port 280

Entering FIPS Approved mode also clears:

1) Protocol shared secret and host passwords
2) SSHv2 RSA host keys
3) HTTPS RSA host keys and certificate

FIPS Approved mode enables:

1) SCP
2) HTTPS TLS v1.0/1.1 and v1.2

13.1.1 FCX624/648 Devices algorithm certificates

Table, below, lists all algorithm certificates for the FCX624/648 Devices. Each of the listed algorithms is implemented in the IronWare R08.0.30b (FastIron 8.0.30) firmware:

Algorithm	Supports	Certificate
Advanced Encryption Algorithm (AES) NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.	ECB (128, 192, 256 bits); CBC (128, 192, 256 bits); CTR (int only; 128, 192, 256 bits); CFB (128 bits) NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.	#2697, #3139 NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.
Triple Data Encryption Algorithm (Triple-DES) NOTE: KO 1 (or 3-key Triple-DES) is latent functionality and is not available within any service in Approved mode of operation.	KO 1, ECB and CBC mode NOTE: KO 1 (or 3-key Triple-DES) is latent functionality and is not available within any service in Approved mode of operation.	#1617 NOTE: KO 1 (or 3-key Triple-DES) is latent functionality and is not available within any service in Approved mode of operation.

Algorithm	Supports	Certificate
Secure Hash Algorithm (SHA) NOTE: SHA-384 and SHA-512 support are latent functionalities. They "ARE NOT" available within any service used in any mode of operation in this module.	SHA-1, SHA-256, SHA-384, and SHA-512 NOTE: SHA-384 and SHA-512 support are latent functionalities. They "ARE NOT" available within any service used in any mode of operation in this module	#2265 NOTE: SHA-384 and SHA-512 support are latent functionalities. They "ARE NOT" available within any service used in any mode of operation in this module
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1 and HMAC SHA-256	#1679
Deterministic Random Bit Generator (DRBG) NOTE: Hash_Based DRBG support is a latent functionality. It "IS NOT" available within any service in any mode of operation.	SP800-90A CTR_DRBG; Hash_Based DRBG NOTE: Hash_Based DRBG support is a latent functionality. It "IS NOT" available within any service in any mode of operation.	#442 NOTE: Hash_Based DRBG support is a latent functionality. It "IS NOT" available within any service in any mode of operation.
Digital Signature Algorithm (DSA) NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.	1024-bit keys NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.	#819 NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.
Rivest Shamir Adleman Signature Algorithm (RSA) NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and "IS NOT" available within any service in the Approved mode of operation.	1024-bit and 2048-bit keys NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and "IS NOT" available within any service in the Approved mode of operation.	#1396 NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and "IS NOT" available within any service in the Approved mode of operation.
Component Test Key Derivation Function (CVL)	TLS v1.0/1.1 and v1.2, SSHv2 and SNMPv3	#161, 386, 388

Table 48 - Algorithm Certificates for the FCX624/648 Devices

13.1.2 SX800/SX1600 Devices algorithm certificates

Table, below, lists all algorithm certificates for the SX800/1600 Devices. Each of the listed algorithms is implemented in the IronWare R08.0.30b (FastIron 8.0.30) firmware:

Algorithm	Supports	Certificate
Advanced Encryption Algorithm (AES) NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.	ECB (128, 192, 256 bits); CBC (128, 192, 256 bits); CTR (int only; 128, 192, 256 bits); CFB (128 bits) NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.	#2688, #3141 NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.
Triple Data Encryption Algorithm (Triple-DES) NOTE: KO 1 (or 3-key Triple-DES) is latent functionality and is not available within any service in Approved mode of operation.	KO 1 ECB and CBC mode NOTE: KO 1 (or 3-key Triple-DES) is latent functionality and is not available within any service in Approved mode of operation.	#1614 NOTE: KO 1 (or 3-key Triple-DES) is latent functionality and is not available within any service in Approved mode of operation.
Secure Hash Algorithm (SHA) NOTE: SHA-224, SHA-384 and SHA-512 support are latent functionalities. They "ARE NOT" available within any service used in any mode of operation in this module.	SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 NOTE: SHA-224, SHA-384 and SHA-512 support are latent functionalities. They "ARE NOT" available within any service used in any mode of operation in this module.	#2259 NOTE: SHA-224, SHA-384 and SHA-512 support are latent functionalities. They "ARE NOT" available within any service used in any mode of operation in this module.

Algorithm	Supports	Certificate
Keyed-Hash Message Authentication Code (HMAC)	HMAC SHA-1 and HMAC SHA-256	#1675
Deterministic Random Bit Generator (DRBG) NOTE: Hash_Based DRBG support is a latent functionality. It "IS NOT" available within any service in any mode of operation.	SP800-90A CTR_DRBG; Hash_Based DRBG NOTE: Hash_Based DRBG support is a latent functionality. It "IS NOT" available within any service in any mode of operation.	#438 NOTE: Hash_Based DRBG support is a latent functionality. It "IS NOT" available within any service in any mode of operation.
Digital Signature Algorithm (DSA) NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.	1024-bit keys NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.	#817 NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.
Rivest Shamir Adleman Signature Algorithm (RSA) NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and "IS NOT" available within any service in the Approved mode of operation.	1024-bit and 2048-bit keys NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and "IS NOT" available within any service in the Approved mode of operation.	#1388 NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and "IS NOT" available within any service in the Approved mode of operation.
Component Test Key Derivation Function (CVL)	TLS v1.0/1.1 and v1.2, SSHv2 and SNMPv3	#156, #392, #398

Table 49 - Algorithm Certificates for the SX800/1600 Devices

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

13.1.3 ICX6450 Devices algorithm certificates

Table, below, lists all algorithm certificates for ICX 6450 Devices. Each of the listed algorithms is implemented in the IronWare R08.0.30b (FastIron 8.0.30) firmware:

Algorithm	Supports	Certificate
Advanced Encryption Algorithm (AES) NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.	ECB (128, 192, 256 bits); CBC (128, 192, 256 bits); CTR (int only; 128, 192, 256 bits); CFB (128 bits) NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.	#2690, #3133 NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.
Triple Data Encryption Algorithm (Triple-DES) NOTE: KO 1 (or 3-key Triple-DES) is latent functionality and is not available within any service in Approved mode of operation.	KO 1 ECB and CBC mode NOTE: KO 1 (or 3-key Triple-DES) is latent functionality and is not available within any service in Approved mode of operation.	#1615 NOTE: KO 1 (or 3-key Triple-DES) is latent functionality and is not available within any service in Approved mode of operation.
Secure Hash Algorithm (SHA) NOTE: SHA-384 and SHA-512 support are latent functionalities. They "ARE NOT" available within any service used in any mode of operation in this module.	SHA-1, SHA-256, SHA-384, and SHA-512 NOTE: SHA-384 and SHA-512 support are latent functionalities. They "ARE NOT" available within any service used in any mode of operation in this module.	#2260 NOTE: SHA-384 and SHA-512 support are latent functionalities. They "ARE NOT" available within any service used in any mode of operation in this module.
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1 and HMAC SHA-256	#1676

Algorithm	Supports	Certificate
Deterministic Random Bit Generator (DRBG) NOTE: Hash_Based DRBG support is a latent functionality. It "IS NOT" available within any service in any mode of operation.	SP800-90A CTR_DRBG; Hash_Based DRBG NOTE: Hash_Based DRBG support is a latent functionality. It "IS NOT" available within any service in any mode of operation.	#439 NOTE: Hash_Based DRBG support is a latent functionality. It "IS NOT" available within any service in any mode of operation.
Digital Signature Algorithm (DSA) NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.	1024-bit keys NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.	#818 NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation
Rivest Shamir Adleman Signature Algorithm (RSA) NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and "IS NOT" available within any service in the Approved mode of operation.	1024 and 2048-bit Keys NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and "IS NOT" available within any service in the Approved mode of operation.	#1391 NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and "IS NOT" available within any service in the Approved mode of operation.
Component Test Key Derivation Function (CVL)	TLS v1.0/1.1 and v1.2, SSHv2 and SNMPv3	#159, #387, #389

Table 50 - Algorithm Certificates for ICX 6450 Devices

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

13.1.4 ICX7250 Devices algorithm certificates

Table, below, lists all algorithm Certificates for the ICX 7250 Devices. Each of the listed algorithms is implemented in the IronWare R08.0.30b (FastIron 8.0.30) firmware:

Algorithm	Supports	Certificate
Advanced Encryption Algorithm (AES) NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.	ECB (128, 192, 256 bits); CBC (128, 192, 256 bits); CTR (int only; 128, 192, 256 bits); CFB (128 bits); NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.	#2981, #3142 NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.
Triple Data Encryption Algorithm (Triple-DES) NOTE: KO 1 (or 3-key Triple-DES) is latent functionality and is not available within any service in Approved mode of operation.	KO 1 ECB and CBC mode NOTE: KO 1 (or 3-key Triple-DES) is latent functionality and is not available within any service in Approved mode of operation.	#1764 NOTE: KO 1 (or 3-key Triple-DES) is latent functionality and is not available within any service in Approved mode of operation.
Secure Hash Algorithm (SHA) NOTE: SHA-384 and SHA-512 support are latent functionalities. They "ARE NOT" available within any service used in any mode of operation in this module.	SHA-1, SHA-256, SHA-384, and SHA- 512 NOTE: SHA-384 and SHA-512 support are latent functionalities. They "ARE NOT" available within any service used in any mode of operation in this module.	#2505 NOTE: SHA-384 and SHA-512 support are latent functionalities. They "ARE NOT" available within any service used in any mode of operation in this module.
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1 and HMAC SHA-256	#1890

Algorithm	Supports	Certificate
Deterministic Random Bit Generator (DRBG) NOTE: Hash_Based DRBG support is a latent functionality. It "IS NOT" available within any service in any mode of operation.	SP800-90A CTR_DRBG; Hash_Based DRBG NOTE: Hash_Based DRBG support is a latent functionality. It "IS NOT" available within any service in any mode of operation.	#569 NOTE: Hash_Based DRBG support is a latent functionality. It "IS NOT" available within any service in any mode of operation.
Digital Signature Algorithm (DSA) NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.	1024-bit keys NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.	#887 NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation
Rivest Shamir Adleman Signature (RSA) NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and "IS NOT" available within any service in the Approve mode of operation.	1024 and 2048-bit keys NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and "IS NOT" available within any service in the Approve mode of operation.	#1565 NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and "IS NOT" available within any service in the Approve mode of operation.
Component Test Key Derivation Function (CVL)	TLS v1.0/1.1 and v1.2, SSHv2 and SNMPv3	#362, #390, #400

Table 51 - Algorithm Certificates for the ICX 7250 Devices

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

13.1.5 ICX7750 Devices algorithm certificates

Table, below, lists all algorithm certificates for the ICX 7750 devices. Each of the listed algorithms is implemented in the IronWare R08.0.30b (FastIron 8.0.30) firmware:

Algorithm	Supports	Certificate
Advanced Encryption Algorithm (AES) NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.	ECB (128, 192, 256 bits); CBC (128, 192, 256 bits); CTR (int only; 128, 192, 256 bits); CFB (128 bits) NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.	#2687, #3140 NOTE: AES 192 is latent functionality that "IS NOT" available within any service in the Approved mode of operation. NOTE: AES-CTR and AES-ECB are latent functionalities that "ARE NOT" available within any service in the Approved mode of operation.
Triple Data Encryption Algorithm (Triple-DES) NOTE: KO 1 (or 3-key Triple-DES) is latent functionality and is not available within any service in Approved mode of operation.	KO 1 ECB and CBC mode NOTE: KO 1 (or 3-key Triple-DES) is latent functionality and is not available within any service in Approved mode of operation.	#1613 NOTE: KO 1 (or 3-key Triple-DES) is latent functionality and is not available within any service in Approved mode of operation.
Secure Hash Algorithm (SHA) NOTE: SHA-384 and SHA-512 support are latent functionalities. They "ARE NOT" available within any service used in any mode of operation in this module.	SHA-1, SHA-256, SHA-384, and SHA-512 NOTE: SHA-384 and SHA-512 support are latent functionalities. They "ARE NOT" available within any service used in any mode of operation in this module.	#2258 NOTE: SHA-384 and SHA-512 support are latent functionalities. They "ARE NOT" available within any service used in any mode of operation in this module.

Algorithm	Supports	Certificate
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1 and HMAC SHA-256	#1674
Deterministic Random Bit Generator (DRBG) NOTE: Hash_Based DRBG support is a latent functionality. It "IS NOT" available within any service in any mode of operation.	SP800-90A CTR_DRBG; Hash_Based DRBG NOTE: Hash_Based DRBG support is a latent functionality. It "IS NOT" available within any service in any mode of operation.	#437 NOTE: Hash_Based DRBG support is a latent functionality. It "IS NOT" available within any service in any mode of operation.
Digital Signature Algorithm (DSA) NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.	1024-bit keys NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.	#816 NOTE: Latent functionality "IS NOT" available within any service in the Approved mode of operation.
Rivest Shamir Adleman Signature Algorithm (RSA) NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and "IS NOT" available within any service in the Approved mode of operation.	1024-bit and 2048-bit keys NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and "IS NOT" available within any service in the Approved mode of operation.	#1387 NOTE: RSA 1024 and any signature using SHA-1 is latent functionality and "IS NOT" available within any service in the Approved mode of operation.
Component Test Key Derivation Function (CVL)	TLS v1.0/1.1 and v1.2, SSHv2 and SNMPv3	#155, #391, #399

Table 52 - Algorithm Certificates for the ICX 7750 Devices

Users should reference the transition tables that will be available at the CMVP Web site http://csrc.nist.gov/groups/STM/cmvp/ . The data in the tables will inform users of the risks associated with using a particular algorithm and a given key length.

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

1. RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
2. Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
3. MD5 - Used in TACACS+ for operator authentication only (MD5 is not exposed to the operator)
4. NDRNG - Generation of seeds for DRBG

5. HMAC-MD5 - Used to support RADIUS for operator authentication only (HMAC-MD5 is not exposed to the operator)
6. MD5 - Used in the TLS v1.0 KDF in FIPS mode as per SP800-135 (MD5 is not exposed to the operator)

13.2 Invoke FIPS Approved Mode

Crypto Officer may use “FastIron FIPS and Common Criteria Configuration Guide” documentation on myBrocade.com for configuration of these devices.

To invoke the FIPS Approved mode of operation, perform the following steps:

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 used by various networking protocols including host access passwords, SSHv2 host keys, and HTTPS host keys with the digital signature.
4) Enter command: *no web-management hp-top-tools*

   The device will turn off access by HP ProCurve Manager via port 280.
5) Generate the SSHv2 Host RSA Private Key (2048 bit) and SSHv2 Host RSA Public Key.
   a) Use CLI command: *crypto key generate*
6) Generate the TLS Host RSA Private Key (RSA 2048 bit) and TLS Host Public Key (RSA 2048 bit).
   a) Use CLI command: *crypto-ssl certificate generate*

   NOTE: The command syntax above includes the nomenclature "ssl" from a legacy command line API; for the avoidance of doubt it is hereby stated that such syntax is a misnomer as SSL "IS NOT" supported in FIPS mode (i.e. the cryptographic module enforces the use of TLS in FIPS mode; SSL "IS NOT" supported in FIPS mode)

7) Copy signature files of all the affected images to the flash memory.
   a) Use CLI command: *scp <syntax>*

8) Enter command: *write memory*.

   The device saves the running configuration as the startup configuration.

9) Enter command: *reload*

   The device resets and begins operation in FIPS Approved mode. (Note: Do not press B as the module is reloading).

10) Enter command: *fips show* (This command displays the FIPS-related status, which should confirm the security policy is the default security policy.)

11) Inspect the physical security of the module, including placement of tamper evident labels according to Appendix A.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

14 Glossary

Term/Acronym	Description
AES	Advanced Encryption Standard
CBC	Cipher-Block Chaining
CLI	Command Line Interface
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook mode
FI	FastIron
GbE	Gigabit Ethernet
GMAC	Galois Message Authentication Code (GMAC): an authentication-only variant of the GCM
HMAC	Keyed-Hash Message Authentication Code
KDF	Key Derivation Function
LED	Light-Emitting Diode
Mbps	Megabits per second
MFG	Manufacturing operation (i.e. MFG Part Number)
Management port	Out-of-band management port
NDRNG	Non-Deterministic Random Number Generator
OC	Optical Carrier
POE	Power over Ethernet
POE+	High Power over Ethernet
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
SSHv2	Secure Shell
TACACS	Terminal Access Control Access-Control System
TACACS+	Terminal Access Control Access-Control System Plus
TDEA	Triple-DES Encryption Algorithm
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security

Table 53 - Glossary

15 References

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

[FIPS 186-4] Digital Signature Standard (DSS), July 2013

[SP800-90A Rev.1] National Institute of Standards and Technology Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), March 2007

[ANSI X9.31] ANSI X9.31:1998 Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

16 Appendix A: Tamper Evident Label application

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

1) Tamper evident label security seals
    a) Count 120
    b) Checkerboard destruct pattern with ultraviolet visible “Secure” image

Use 99% isopropyl or ethyl alcohols to clean the surface area at each tamper evident label security seal placement location. Cleaning alcohol is not provided in the kit. However, cleaning 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.

The Crypto Officer is responsible for securing and having control of any unused seals at all times.

Tamper evidence information

When a tamper evident label security seal is removed from the surface to which it has been applied, several tamper indications are apparent:

- The seal that has been removed shows a checkerboard destruct pattern.
- The graphics printed within the seal are uniquely split between the removed seal and the residue left on the surface. The residue is visible under ultraviolet light.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

16.1 Brocade FCX 624 and FCX 648 Devices

16.1.1 FCX 624S, FCX 624S-HPOE-ADV and FCX 624S-F-ADV devices

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

- Brocade FCX624S
- Brocade FCX624S-HPOE-ADV
- Brocade FCX624S-F-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 80 and Figure 81 display a Brocade FCX624S with seals as a model for the seal placement on the Brocade FCX 624S, FCX 624S-HPOE-ADV and FCX 624S-F-ADV. Each of these devices requires the placement of Fourteen (14) 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 80 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 80 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 80).
- **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 80 for correct seal orientation and positioning. Affix one seal over the console port covering it and adhering it on the left side. See Figure 80 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 81 for correct seal orientation and positioning.

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

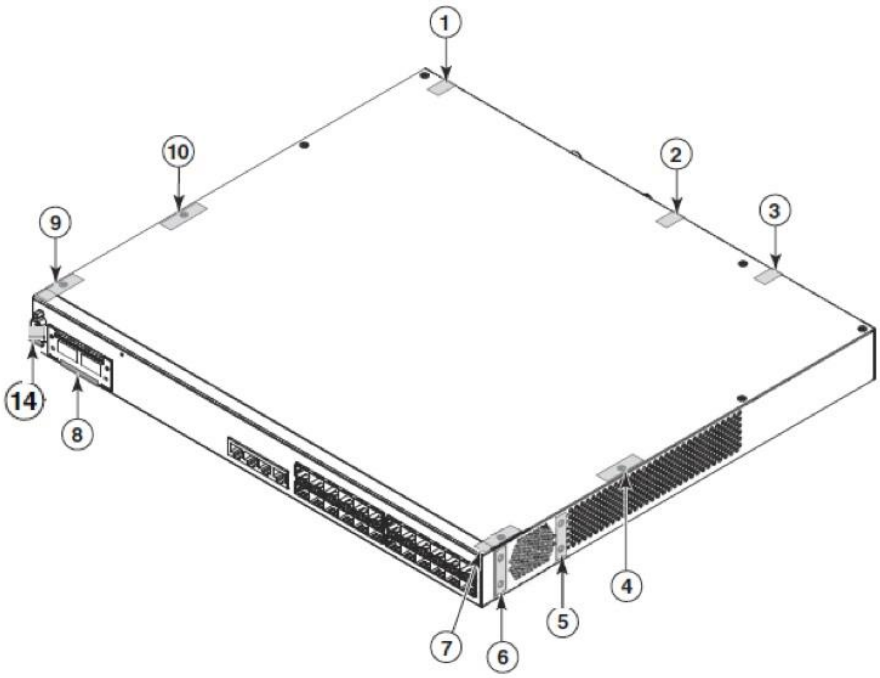

Figure 80 - FCX 624S, FCX 624S-HPOE-ADV and FCX 624S-F-ADV - Front, top and right side views with security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

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

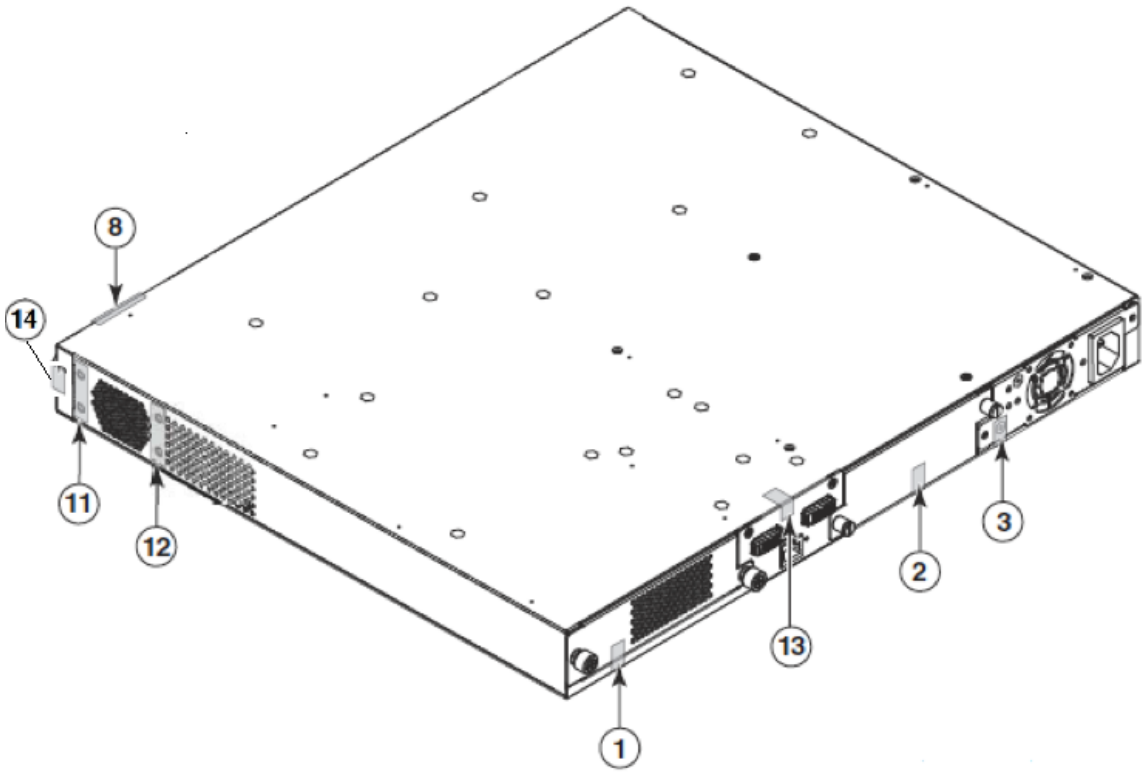

Figure 81 - FCX 624S, FCX 624S-HPOE-ADV and FCX 624S-F-ADV - Rear, bottom and left side views with tamper evident label security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

16.1.2 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 FCX648S
- Brocade FCX648S-HPOE
- Brocade FCX648S-HPOE-ADV

Figure 82 and Figure 83 display a Brocade FCX648S with seals as a model for the seal placement on the Brocade FCX648S, FCX648S-HPOE and FCX648S-HPOE-ADV. Each of these devices requires the placement of fourteen (14) 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 82 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 82 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 82).
- **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 82 for correct seal orientation and positioning. Affix one seal over the console port covering it and adhering it on the left side. See Figure 82 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 83 for correct seal orientation and positioning.

Figure below illustrates, front, top and right side views of a Brocade FCX648S, FCX648S-HPOE and FCX648S-HPOE-ADV device with security seals

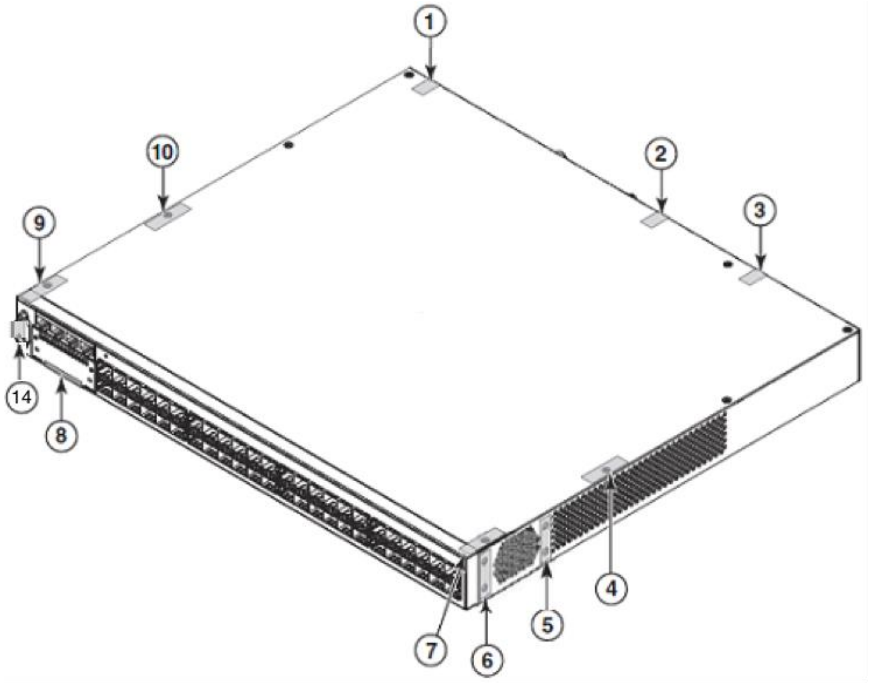

Figure 82 - FCX648S, FCX648S-HPOE and FCX648S-HPOE-ADV - Front, top and right side views with tamper evident label security seals

Figure below illustrates rear, bottom, and left side views of a Brocade FCX648S, FCX648S-HPOE and FCX648S-HPOE-ADV device with security seals

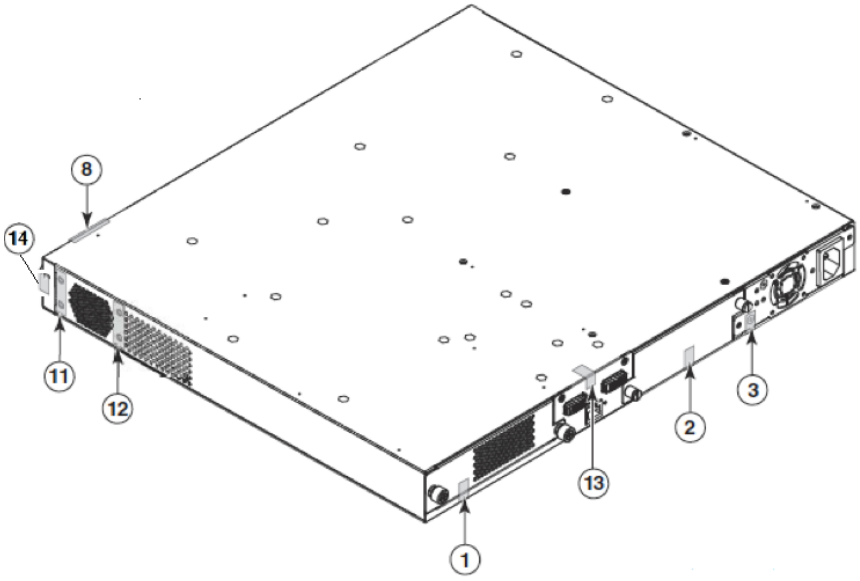

Figure 83 - FCX648S, FCX648S-HPOE and FCX648S-HPOE-ADV - Rear, bottom and left side views with tamper evident label security seals

16.2 SX 800 and SX 1600 Series devices

16.2.1 SX800 devices

Use the figures in this section as a guide for security seal placement on a Brocade FastIron SX800 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 SX800 devices. Each Brocade FastIron SX800 device requires the placement of eighteen (18) seals:

- **Front:** Affix 15 total seals to the front panel of the device. Affix one seal horizontally to the left ear of each module installed in the left side of the chassis. As much of the seal as possible should be affixed to the module directly above the left screw for the left side modules. Affix one seal horizontally to the right ear of each module installed in the right side of the chassis. As much of the seal as possible should be affixed to the module directly below the right screw for the right side modules. Affix one seal vertically from the upper right corner of the fan tray to the chassis. Affix two seals horizontally over the console ports. All 15 of these seals should lie flat against the surface of the device. See Figure 84 for correct seal orientation and positioning.

Figure 84, below, illustrates front view of a Brocade FastIron SX800 device (containing SX-FI-ZMR-XL management modules and SX-FISF Switch Fabric modules) with security seals correctly applied.

Figure 84 - SX800 (containing SX-FI-ZMR-XL management modules and SX-FISF Switch Fabric modules) - Front view with tamper evident label security seals

Figure 85, below, illustrates front view of a Brocade FastIron SX800 device (containing SX-FI-2XGMR-XL management modules and SX-FISF Switch Fabric modules) with security seals correctly applied.

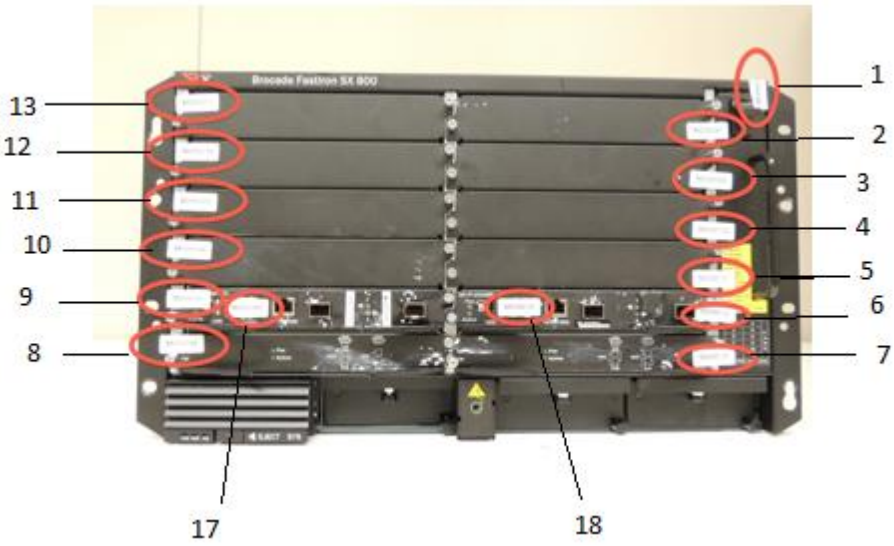

Figure 85 - SX800 (containing SX-FI-2XGMR-XL management modules and SX-FISF Switch Fabric modules) - Front view with tamper evident label security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

- **Rear:** Affix 3 total seals to the rear panel of the device. Affix two seals vertically to 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 to the lower center of the rear panel so that 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 86 for seal orientation and positioning.

Figure below illustrates rear, top and left side panel views of a Brocade FastIron SX800 device with security seals

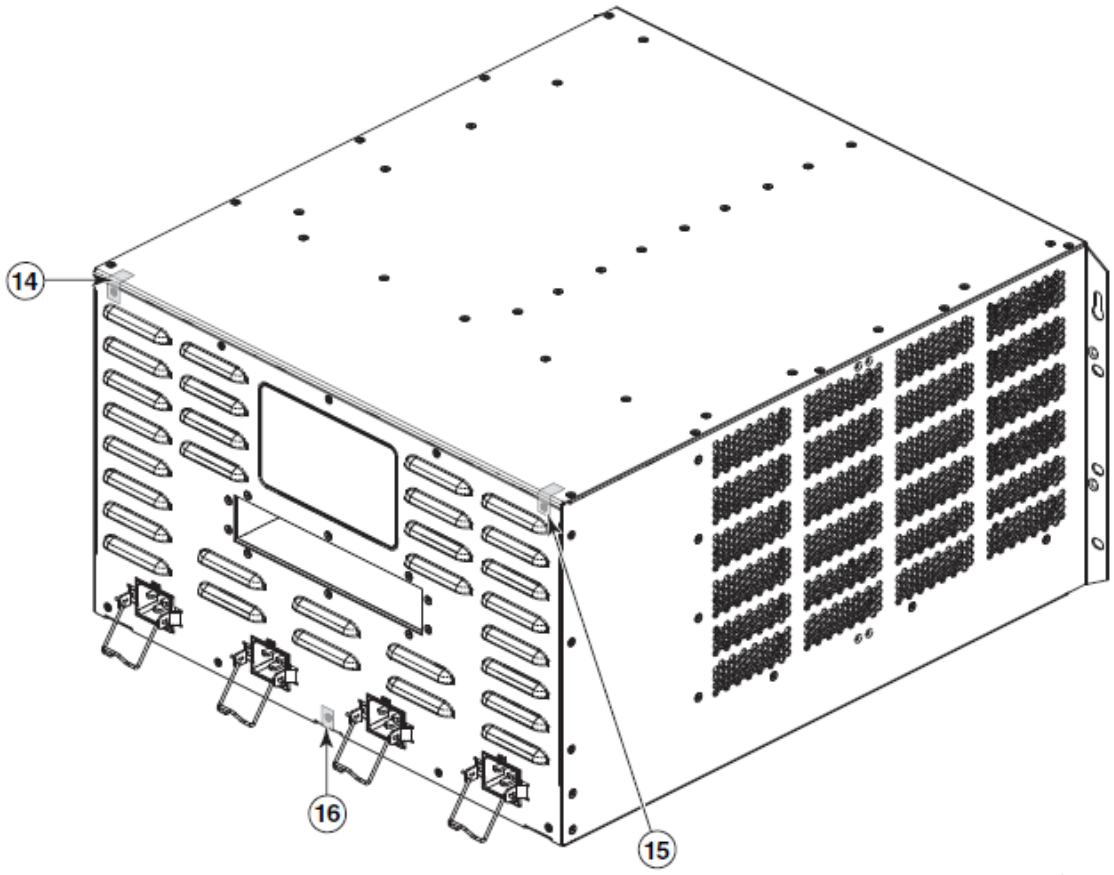

Figure 86 - SX800 - Rear, top and left side panel views with tamper evident label security seals

16.2.2 SX1600 devices

Use the figures in this section as a guide for security seal placement on a Brocade FastIron SX1600 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 SX1600 devices. Each Brocade FastIron SX1600 device requires the placement of twenty-six (26) seals:

- **Front:** Affix 23 total seals to the front panel of the device. Affix one seal vertically to the upper ear of each module installed in the top row of the chassis as shown in Figure 87. As much of the seal as possible should be affixed to the module to the right of the screw that secures each module to the chassis. Affix one seal vertically to the lower ear of each module installed in the bottom row of the chassis as; shown in Figure 87. As much of the seal as possible should be affixed to the module to the left of the screw that secures each module to the chassis. Affix one seal vertically from the upper left corner of the fan tray to the chassis, as shown in Figure 87. Affix one seal vertically over each console port (2 seals total) as shown in Figure 87. All 23 of the seals should lie flat against the surface of the device.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Figure 87 below illustrates front view of a Brocade FastIron SX1600 device (containing SX-FI-ZMR-XL management modules and SX-FISF Switch Fabric modules) with security seals correctly applied.

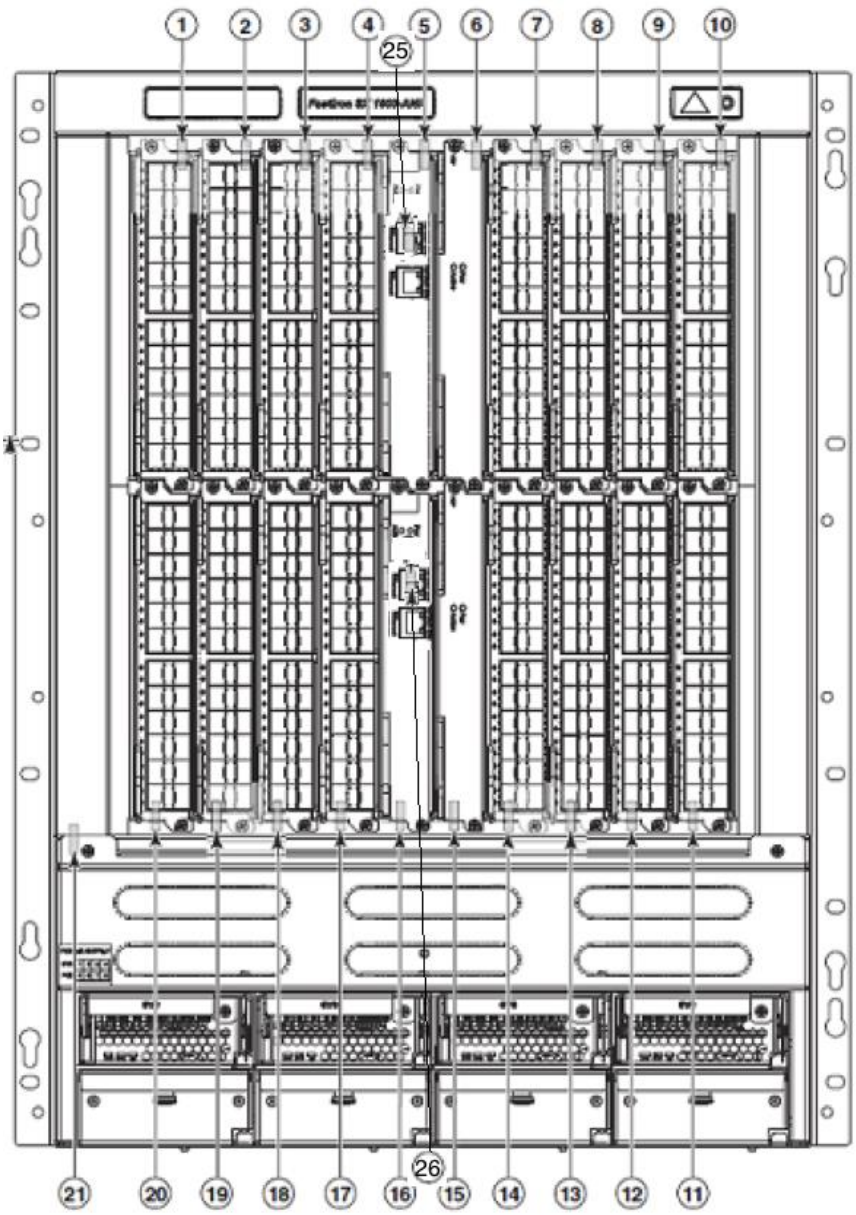

Figure 87 - SX1600 (containing SX-FI-ZMR-XL management modules and SX-FISF Switch Fabric modules) - Front view with tamper evident label security seals

Next page →

Figure 88 below illustrates front view of a Brocade FastIron SX1600 device (containing SX-FI-2XGMR-XL management modules and SX-FISF Switch Fabric modules) with security seals correctly applied.

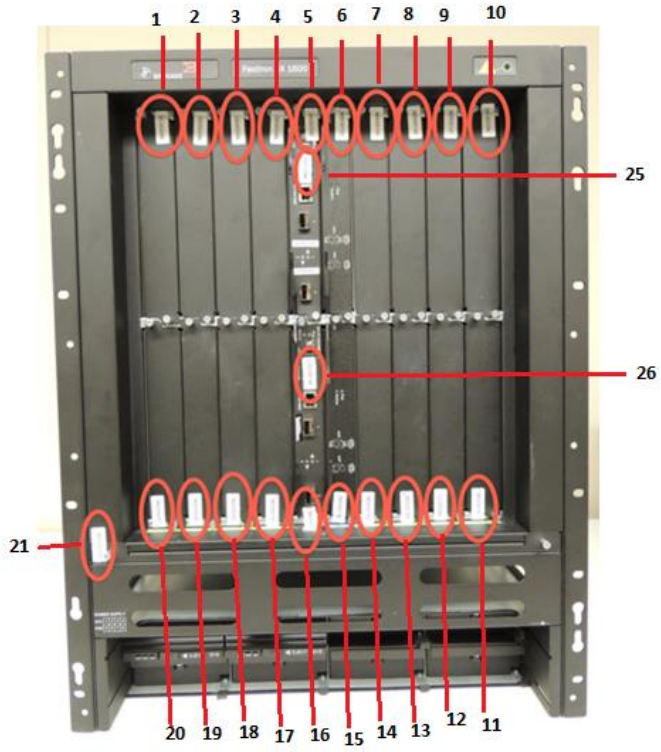

Figure 88 - SX1600 (containing SX-FI-2XGMR-XL management modules and SX-FISF Switch Fabric modules) - Front view with tamper evident label security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

- Rear: Affix 3 total seals to the rear panel of the device. Affix two seals vertically to the upper right and left 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 half of the seal is affixed to the rear panel of the device and half of the seal is affixed to the bottom panel. You must bend this seal to place it correctly. See Figure 89 for correct seal orientation and positioning.

Figure below illustrates rear view of the FastIron SX1600 device with security seals

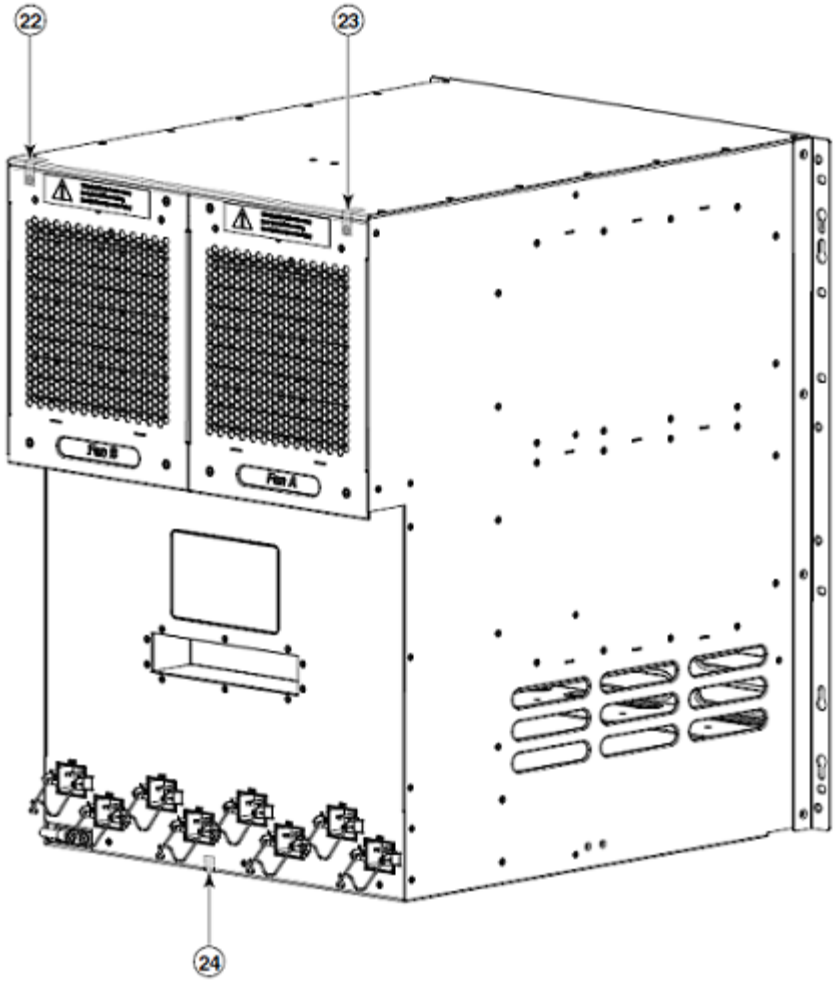

Figure 89 - SX1600 - Rear view with tamper evident label security seals

16.3 ICX 6450 Devices

16.3.1 ICX6450-24 Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 6450-24 device. Each device requires the placement of seven (7) seals:

- **Top:** Affix 3 seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal is on the metal cover and the other part is affixed over the top of the front panel. See Figure 90 for correct seal orientation and positioning.
- **Rear:** Affix 3 seals to the rear of the device between bottom of the chassis and the rear removable cover. Place the seals in a 90 degree bend, so that part of the seal is affixed to the chassis bottom and the other part is affixed to the rear cover as shown. Refer to Figure 91 for correct seal orientation and positioning.
- **Console port**: Affix 1 seal over the console port, as shown in Figure 98.

Figure below illustrates top view of a Brocade ICX6450-24 device with security seals

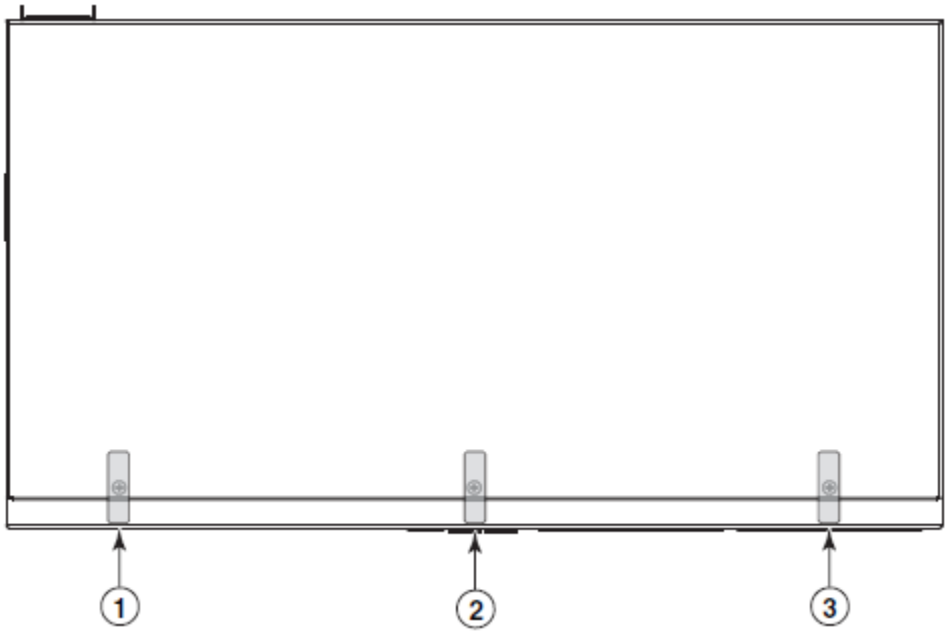

Figure 90 - ICX6450-24 - Top view with tamper evident label security seals

Figure below illustrates rear view of a Brocade ICX6450-24 device with security seals

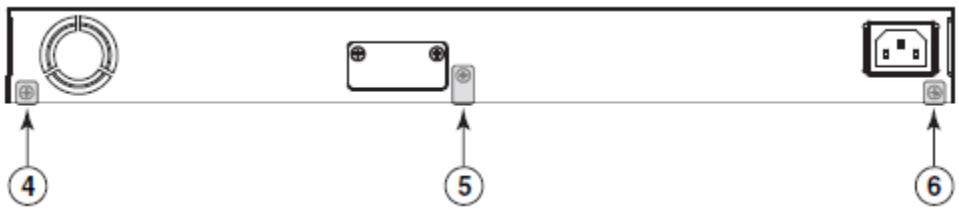

Figure 91 - ICX6450-24 - Rear view with tamper evident label security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

16.3.2 ICX6450-24P Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX6450-24P device. Each device requires the placement of seven (7) seals:

- **Top:** Affix 3 seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal is on the metal cover and the other part is affixed over the top of the front panel as shown. See Figure 92 for correct seal orientation and portioning.
- **Rear:** Affix 3 seals to the back side of the device between bottom of the chassis and the rear removable cover. Place the seals in a 90 degree bend, so that part of the seal is affixed to the chassis bottom and other part is affixed to the rear cover as shown. Refer to Figure 93 for correct seal orientation and positioning.
- **Console Port:** Affix 1 seal over the console port, as shown in Figure 98.

Figure below illustrates top view of a Brocade ICX6450-24P device with security seals

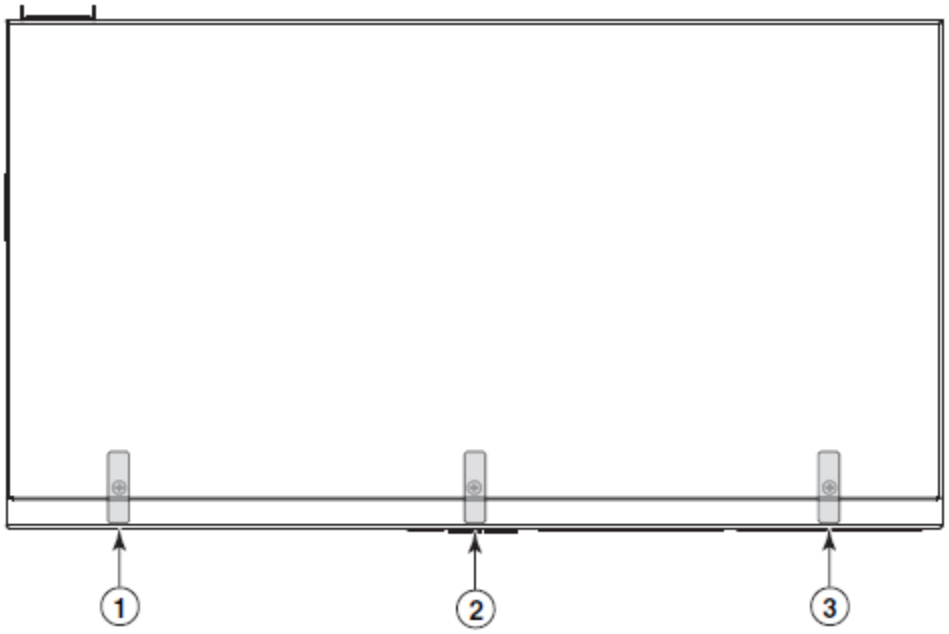

Figure 92 - ICX6450-24P - Top view with tamper evident label security seals

Figure below illustrates rear view of a Brocade ICX6450-24P device with security seals

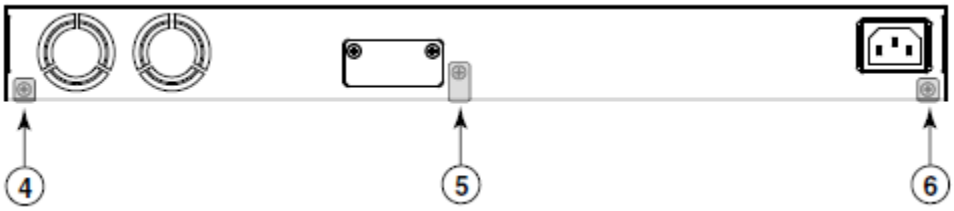

Figure 93 - ICX6450-24P - Rear view with tamper evident label security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

16.3.3 ICX6450-48 Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX6450-48 device. Each device requires the placement of seven (7) seals:

- **Top:** Affix 3 seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal is on the metal cover and the other part is affixed over the top of the front panel. See Figure 94 for correct seal orientation and positioning.
- **Rear:** Affix 3 seals to the rear of the device between bottom of the chassis and the rear removable cover. Place the seals in a 90 degree bend, so that part of the seal is affixed to the chassis bottom and the other part is affixed to the rear cover as shown. Refer to Figure 95 for correct seal orientation and positioning.
- **Console port:** Affix 1 seal over the console port, as shown in Figure 99 and Figure 100. Place the seal so that part of the seal entirely covers the console port while the remainder of the seal wraps around the side of the chassis as shown.

Figure below illustrates top view of a Brocade ICX6450-48 device with security seals

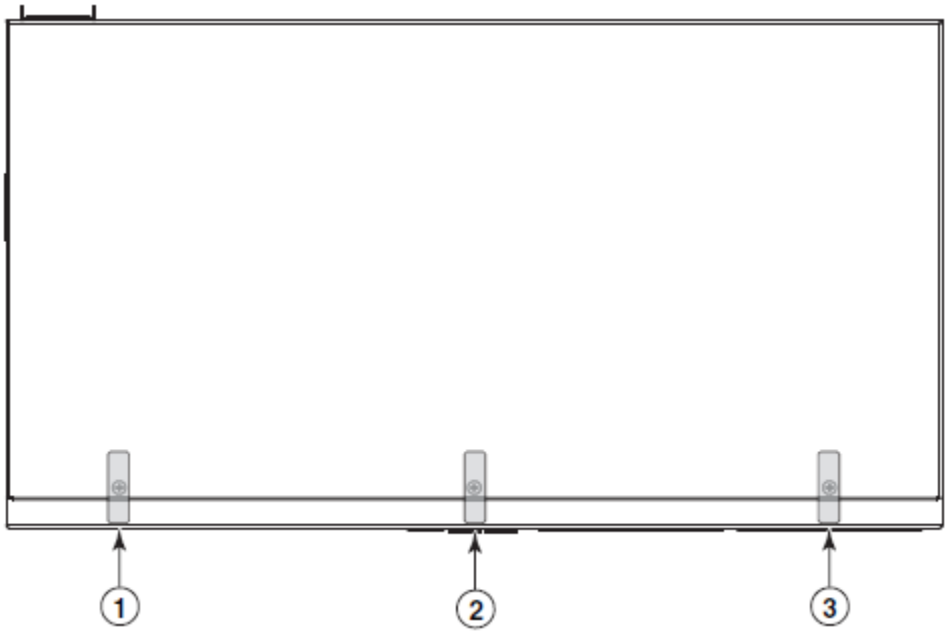

Figure 94 - ICX6450-48 - Top view with tamper evident label security seals

Figure below illustrates rear view of a Brocade ICX6450-48 device with security seals

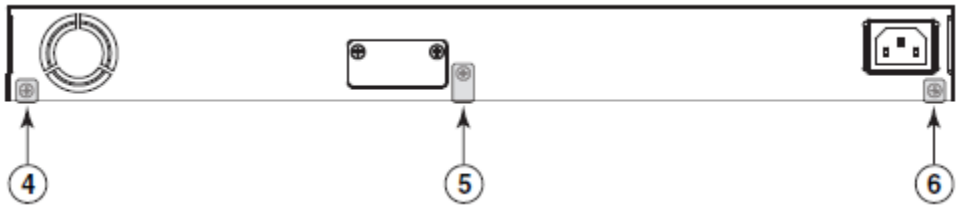

Figure 95 - ICX6450-48 - Rear view with tamper evident label security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

16.3.4 ICX6450-48P Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX6450-48P device. Each device requires the placement of seven (7) seals:

- **Top:** Affix 3 seals between the top of the front panel and the top removable metal cover of the device. Apply each seal flat over the seam between the top cover and front panel so that part of the seal is on the metal cover and the other part is affixed over the top of the front panel as shown. See Figure 96 for correct seal orientation and portioning.
- **Rear:** Affix 3 seals to the back side of the device between bottom of the chassis and the rear removable cover. Place the seals in a 90 degree bend, so that part of the seal is affixed to the chassis bottom and the other part is affixed to the rear cover as shown. Refer to Figure 97 for correct seal orientation and positioning.
- **Console port:** Affix 1 seal over the console port, as shown in Figure 99 and Figure 100. Place the seal so that part of the seal entirely covers the console port while the remainder of the seal wraps around the side of the chassis as shown.

Figure below illustrates top view of a Brocade ICX6450-48P device with security seals

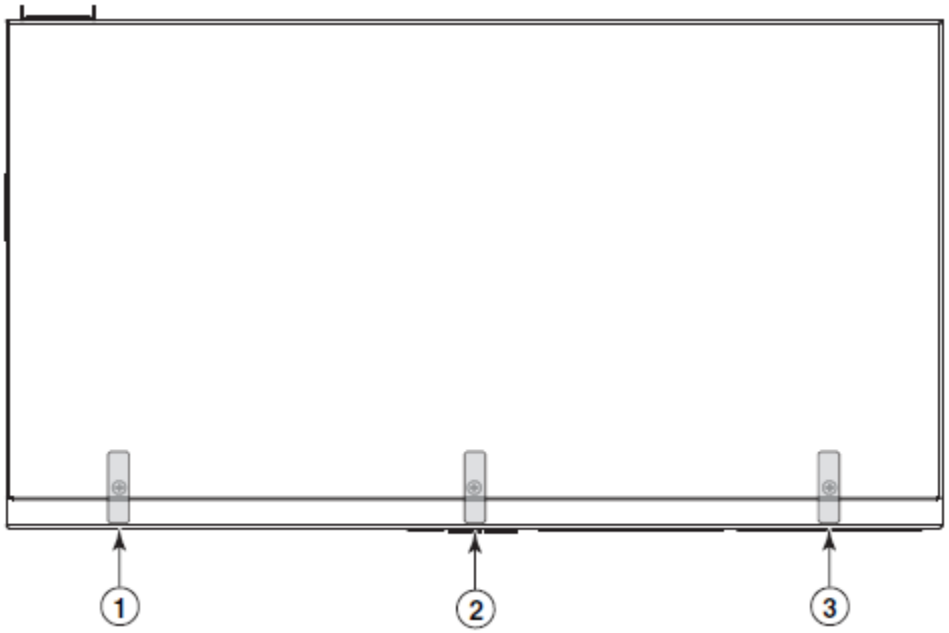

Figure 96 - ICX6450-48P - Top view with tamper evident label security seals

Figure below illustrates rear view of a Brocade ICX6450-48P device with security seals

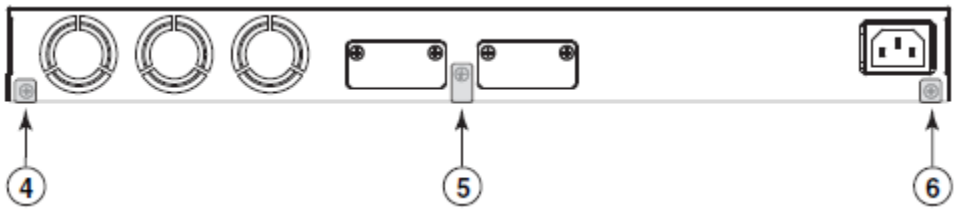

Figure 97 - ICX6450-48P - Rear view with tamper evident label security seals

Figure below illustrates placement of Security Seal over the console port on the Brocade ICX6450-24 and ICX6450-24P devices

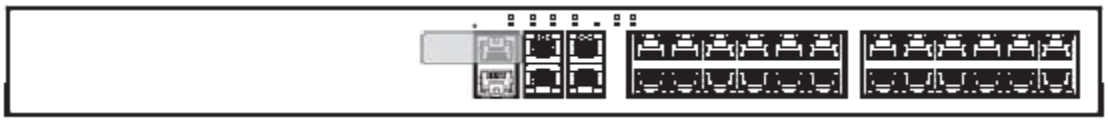

Figure 98 - ICX6450-24 and ICX6450-24P – Tamper evident label security seal over the console port

Figure below illustrates placement of Security Seal over the console port on the Brocade ICX6450-48 and ICX6450-48P devices

Figure 99 - ICX6450-48 and ICX6450-48P – Tamper evident label security seal over the console port

Figure below illustrates side view of Security Seal over the console port on the Brocade ICX6450-48 and ICX6450-48P

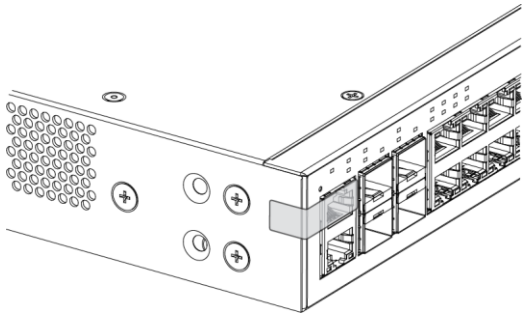

Figure 100 - ICX6450-48 and ICX6450-48P - Side View of tamper evident label security seal over the console ports

16.3.5 ICX6450-C12-PD Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX6450-CP12-PD device. Each device requires the placement of sixteen (16) seals:

- **Front:** Affix a seal, at seal locations 1 and 2, which wraps from the front panel to the side panel on the left and right side, respectively. Each seal must bridge the seam between the front panel and the side panel. See Figure 101 and Figure 102 for the correct seal orientation and portioning. Affix one seal over the console port. Three (3) seals are required to complete this step of the procedure.
- **Right:** Affix a seal at locations 10, 11 and 12 on the right side of the module, as seen in Figure 102. Three (3) seals are required to complete this step of the procedure.
- **Left:** Affix a seal at locations 14, 15 and 16 on the left side of the module, as seen in Figure 104. Three (3) seals are required to complete this step of the procedure.
- **Back:** Affix a seal at location 13, as seen in Figure 104. One (1) seal are required to complete this step of the procedure.
- **Bottom:** Affix a seal, at seal locations 3 through 8, which covers the screws that attach the bottom panel to the chassis to chassis cover. Each seal must bridge the seam between the bottom panel and the chassis cover. See Figure 103 for the correct seal orientation and portioning. Six (6) seals are required to complete this step of the procedure.

Figure below illustrates front view of a Brocade ICX6450-CP12-PD device with security seals

Figure 101 - ICX6450-CP12-PD - Front view with tamper evident label security seals

Figure below illustrates front right side view of a Brocade ICX6450-CP12-PD device with security seals

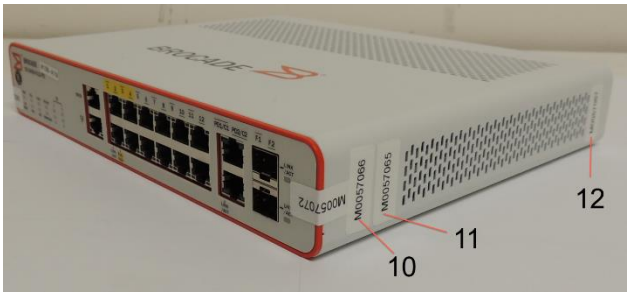

Figure 102 - ICX6450-CP12-PD - Front right side view with tamper evident label security seals

Figure below illustrates bottom side view of a Brocade ICX6450-CP12-PD device with security seals

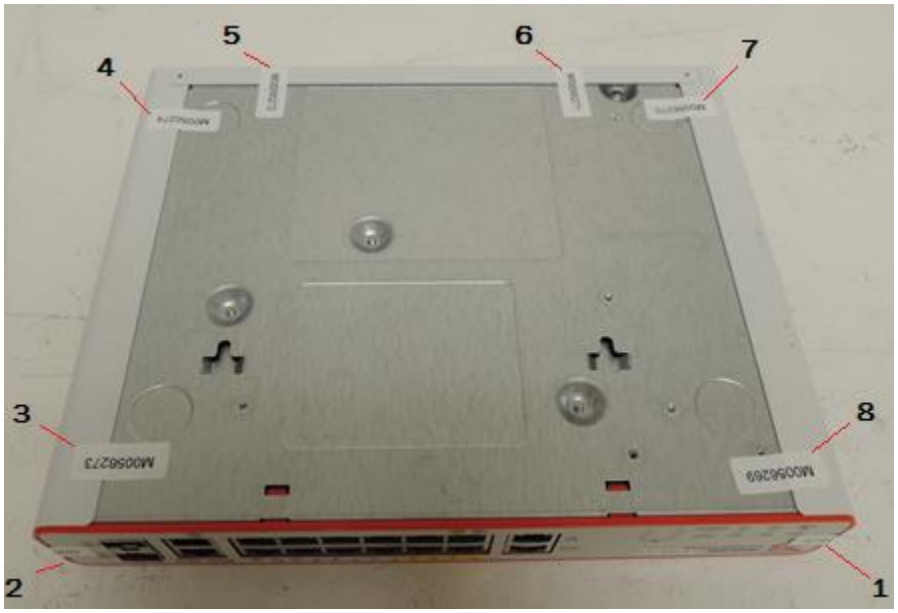

Figure 103 - ICX6450-CP12-PD - Bottom side view with tamper evident label security seals

Figure below illustrates back left side view of a Brocade ICX6450-CP12-PD device with security seals

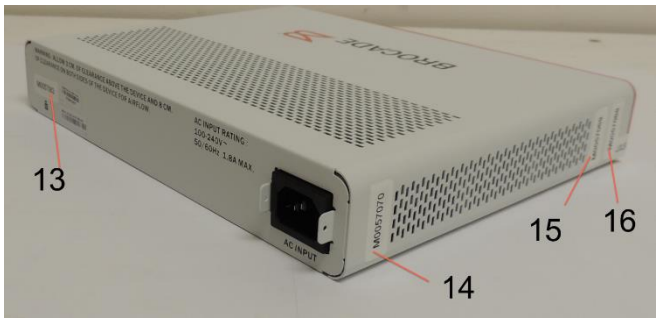

Figure 104 - ICX6450-CP12-PD - Back left side view with tamper evident label security seals

16.4 ICX 7250 Devices

Seven (7) sealing labels are required to complete the tamper evident sealing requirements on the Brocade ICX7250. The seal application is the same for 24-port (ICX725-24, ICX725-24G, ICX725-24P) and 48-port (ICX725-48, ICX725-48P) devices.

- **Top-front:** Affix a seal at the seal location 1, 2, 3, and 4.

  For ICX7250 24 port devices see Figure 105 and Figure 106.

  For ICX7250 48 port devices see Figure 107 and Figure 108

Figure 105 - ICX7250 24 ports front side seal locations (Tamper labels #1, #2, #3, and #4)

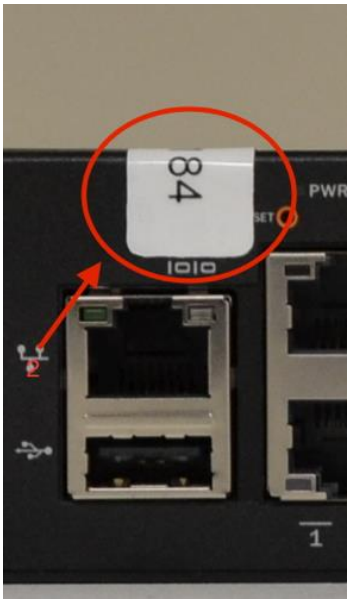

Figure 106 - ICX7250 24 ports front side seal location (close-up of tamper label #2)

Figure 107 - ICX7250 48 ports front side seal locations (tamper labels #1, #2, #3, and #4)

Figure 108 - ICX7250 48 ports front side seal location (close-up of tamper label #2)

- **Left:** Affix one seal at seal location 5

  For ICX7250 24 port devices see Figure 109.

  For ICX7250 48 port devices see Figure 110.

Figure 109 - ICX7250 24 ports left side seal location (tamper label #5)

Figure 110 - ICX7250 48 ports left side seal location (tamper label #5)

- **Rear:** Affix one seal at the seal location 6

  For ICX7250 24 port devices see Figure 111.

  For ICX7250 48 port devices see Figure 112.

Figure 111 - ICX7250 24 ports rear side seal location (tamper label #6)

Figure 112 - ICX7250 48 ports rear side seal location (tamper label #6)

Next page →

- **Right:** Affix one seal at the seal location 7

  For ICX7250 24 port devices see Figure 113.

  For ICX7250 48 port devices see Figure 114.

Figure 113 - ICX7250 24 ports right side seal location (tamper label #7)

Figure 114 - ICX7250 48 ports right side seal location (tamper label #7)

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

16.5 ICX 7750 Devices

Use the figures in this section as a guide for security seal placement on a FIPS-compliant Brocade ICX 7750 devices. The seal placement for ICX7750-48C, ICX7750-48F and ICX7750-26Q are equivalent. Each device requires the placement of fourteen (14) seals.

- **Top front**: Affix a seal, at seal locations 1, 2, 3, and 4, which covers the screw that attaches the top cover to the front panel and bridges the seam between the top of the front panel and the removable metal cover of the device. Affix a seal, at seal location 5, which covers the console port of the module. See Figure 115 for correct seal orientation and positioning. Five (5) tamper evident label seals are required to complete this step of the procedure.
- **Top right side**: Affix a seal at location 13, which attaches the top cover to the right side panel and wraps around the 90 degree angle formed by the side panel and the removable metal cover of the device. See Figure 116 for correct seal orientation and positioning. One (1) tamper evident label seal is required to complete this step of the procedure.
- **Top left side**: Affix a tamper evident label seal at location 6, which attaches the top cover to the left side panel and wraps around the 90 degree angle formed by the side panel and the removable metal cover of the device. See Figure 117 for correct seal orientation and positioning. One (1) tamper evident label seal is required to complete this step of the procedure.
- **Rear:** Affix a tamper evident label seal, at seal locations 7, 8, 9, 10, 11, 12 and 14, which attaches the top cover to the rear panel and wraps around the 90 degree angle formed by the rear panel and the removable metal cover of the device. See Figure 118 for correct seal orientation and positioning. Seven (7) tamper evident label security seals are required to complete this step of the procedure.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

Figure below illustrates front top view of Brocade ICX7750 device with security seals

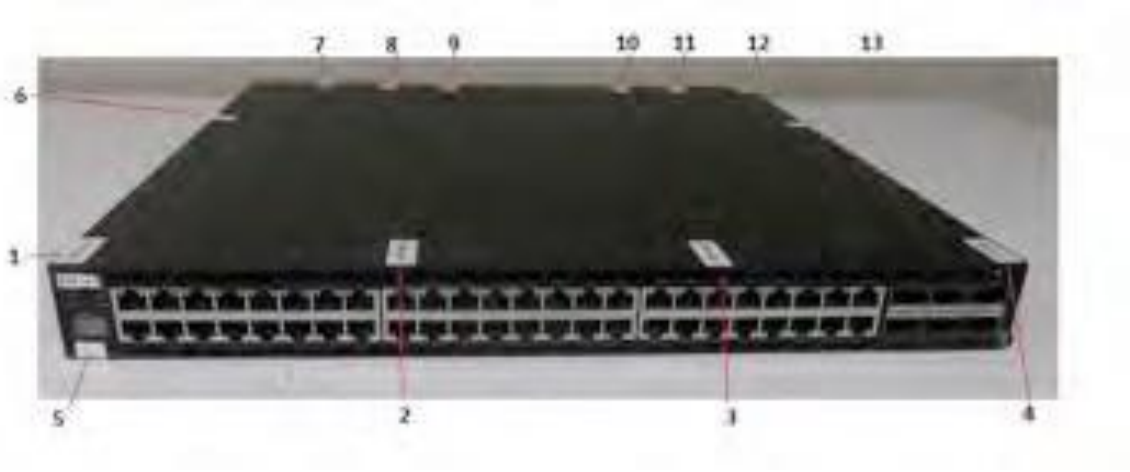

Figure 115 - ICX7750 - Front top view with tamper evident label security seals

Figure below illustrates right side view of the ICX7750 with tamper evident label seals.

Figure 116 - ICX7750 - Right and top side view with tamper evident label security seals

Figure below illustrates left side view of the ICX7750 with tamper evident label seals.

Figure 117 - ICX7750 - Left and top sides view with tamper evident label security seals

Next page →

Figure below illustrates rear top view of Brocade ICX7750 device with tamper evident label seals.

Figure 118 - ICX7750 - Rear and top view with tamper evident label security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.

Next page →

17 Appendix B: Critical Security Parameters

The module supports the following CSPs and public keys:

1) SSHv2 Host RSA Private Key (2048 bit)

- Description: Used to authenticate SSHv2 server to client

- Type: RSA Private Key

- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.

- Establishment: N/A

- Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9

- Output: N/A

- Storage: Plaintext in RAM and BER encoded (plaintext) in Compact Flash

- Key-to-Entity: Process

- Zeroization: "fips zeroize all" command

2) SSHv2 DH Private Key (2048 bit)

- Description: Used in SCP and SSHv2 to establish a shared secret

- Type: DH Private Key

- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; allowed method as per FIPS 140-2 IG D.8 Scenario 4

- Establishment: N/A

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: Process

- Zeroization: Session termination and "fips zeroize all" command

3) SSHv2 DH Shared Secret Key (2048 bit)

- Description: Output from the DH Key agreement primitive - (K) and (H). Used in SSHv2 KDF to derive (client and server) session keys.

- Type: DH Shared Secret Key

- Generation: N/A

- Establishment: SSHv2 DH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: User

- Zeroization: Session termination and "fips zeroize all" command

4) SSHv2/SCP Session Keys (128 and 256 bit AES CBC)

- Description: AES encryption key used to secure SSHv2/SCP

- Type: AES CBC Key

- Generation: N/A

- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: User

- Zeroization: Session termination and "fips zeroize all" command

5) SSHv2/SCP Authentication Key (HMAC-SHA-1)

- Description: Session authentication key used to authenticate and provide integrity of SSHv2 session

- Type: HMAC-SHA-1

- Generation: N/A

- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: User

- Zeroization: Session termination and "fips zeroize all" command

6) SSHv2 KDF Internal State

- Description: Used to generate Host encryption and authentication key

- Type: KDF

- Generation: N/A

- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: User

- Zeroization: Session termination and "fips zeroize all" command

7) TLS Host RSA Private Key (RSA 2048 bit)

- Description: RSA key used to establish TLS v1.0/1.1 and v1.2 sessions

- Type: RSA Private Key

- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.

- Establishment: N/A

- Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9

- Output: N/A

- Storage: Plaintext in RAM and BER encoded (plaintext) in Compact Flash

- Key-to-Entity: Process

- Zeroization: "fips zeroize all" command

8) TLS Pre-Master Secret

- Description: Secret value used to establish the Session and Authentication key

- Type: TLS v1.0/1.1 and v1.2 CSP

- Generation: N/A, established during the TLS v1.0/1.1 and v1.2 handshake using RSA key

transport

- Establishment: Key transport: RSA key wrapped over TLS v1.0/1.1 and v1.2 session; allowed as per FIPS 140-2 IG D.9.

- Entry: Key transport: RSA key wrapped over TLS v1.0/1.1 and v1.2 session; allowed as per FIPS 140-2 IG D.9.

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: User

- Zeroization: Session termination and "fips zeroize all" command

9) TLS Master Secret

- Description: 48 bytes secret value used to establish the TLS v1.0/1.1 and v1.2 Session Key and TLS Authentication Key

- Type: TLS v1.0/1.1 and v1.2 CSP

- Generation: N/A

- Establishment: TLS v1.0/1.1 and v1.2 KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: User

- Zeroization: Session termination and "fips zeroize all" command

10) TLS KDF Internal State

- Description: Values of the KDF internal state

- Type: TLS v1.0/1.1 (HMAC-SHA-1, HMAC-MD5) as per SP800-135 and TLS v1.2 (HMAC-SHA-256) as per SP800-135

- Generation: Approved TLS v1.0/1.1 and v1.2 KDF

- Establishment: N/A

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: User

- Zeroization: Session termination and "fips zeroize all" command

11) TLS Session Key

- Description: 128 or 256 bit AES CBC key used to secure TLS v1.0/1.1 and v1.2 sessions

- Type: AES CBC

- Generation: N/A

- Establishment: TLS v1.0/1.1 and v1.2 KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: User

- Zeroization: Session termination and "fips zeroize all" command

12) TLS Authentication Key

- Description: HMAC-SHA-1key used to provide data authentication for TLS v1.0/1.1 sessions; HMAC-SHA-1 and HMAC-SHA-256 key used to provide data authentication for TLS v1.2

- Type: TLS v1.0/1.1 (HMAC-SHA-1) and TLS v1.2 (HMAC-SHA-1 and HMAC-SHA-256)

- Generation: N/A

- Establishment: TLS v1.0/1.1 and v1.2 KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4.

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: User

- Zeroization: Session termination and "fips zeroize all" command

13) DRBG Seed

- Description: Seeding material for the SP800-90A CTR_DRBG

- Type: DRBG Seed material

- Generation: internally generated; raw random data from NDRNG

- Establishment: N/A

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: Process

- Zeroization: Session termination and "fips zeroize all" command

14) DRBG Value V

- Description: Internal State of SP800-90A CTR_DRBG

- Type: SP800-90A DRBG

- Generation: SP800-90A DRBG

- Establishment: N/A

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

15) DRBG Key
- Description: Internal State of SP800-90A CTR_DRBG
- Type: SP800-90A DRBG
- Generation: SP800-90A DRBG
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

16) DRBG Internal State
- Description: Internal State of SP800-90A CTR_DRBG
- Type: SP800-90A DRBG
- Generation: SP800-90A DRBG
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

17) User Password
- Description: Password used to authenticate User (8 to 48 characters)
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
- Output: MD5 hashed in configuration, output encrypted/authenticated over SSHv2 session

- Storage: MD5 digest in plaintext in Compact Flash
- Key-to-Entity: User
- Zeroization: "fips zeroize all" command

18) Port Administrator Password
- Description: Password used to authenticate Port Configuration Administrator (8 to 48 characters)
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
- Output: MD5 hashed in configuration, output encrypted/authenticated over SSHv2 session
- Storage: MD5 digest in plaintext in Compact Flash
- Key-to-Entity: User
- Zeroization: "fips zeroize all" command

19) Crypto Officer Password
- Description: Password used to authenticate Crypto Officer (8 to 48 characters)
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
- Output: MD5 hashed in configuration, output encrypted/authenticated over SSHv2 session
- Storage: MD5 digest in plaintext in Compact Flash
- Key-to-Entity: User
- Zeroization: "fips zeroize all" command

20) RADIUS Secret
- Description: Used to authenticate the RADIUS server (8 to 64 characters)
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
- Output: MD5 hashed in configuration, output encrypted/authenticated over SSHv2 session

- Storage: Plaintext in RAM, Brocade proprietary two-way encrypted using base-64 (plaintext) in RAM and Compact Flash

- Key-to-Entity: Process

- Zeroization: "fips zeroize all" command

21) TACACS+ Secret

- Description: Used to authenticate the TACACS+ server (8 to 64 characters)

- Type: Authentication data

- Generation: N/A

- Establishment: N/A

- Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session

- Output: MD5 hashed in configuration, output encrypted/authenticated over SSHv2 session

- Storage: Plaintext in RAM, Brocade proprietary two-way encrypted using base-64 (plaintext) in RAM and Compact Flash

- Key-to-Entity: Process

- Zeroization: "fips zeroize all" command

22) Firmware Integrity / Firmware Load RSA Public Key

- Description: RSA 2048-bit public key used to verify signature of firmware of the module

- Type: RSA Public Key

- Generation: N/A, Generated outside the module

- Establishment: N/A

- Entry: Through firmware update

- Output: N/A

- Storage: Plaintext in RAM, Plaintext in Compact Flash

- Key-to-Entity: Process

23) SSHv2 Host RSA Public Key

- Description: (2048 bit); Used to establish shared secrets

- Type: RSA Public Key

- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.

- Establishment: N/A

- Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9

- Output: Plaintext

- Storage: Plaintext in RAM, Plaintext in Compact Flash

- Key-to-Entity: Process

24) SSHv2 Client RSA Public Key

- Description: (2048 bit); Used to establish shared secrets

- Type: RSA Public Key

- Generation: N/A, generated outside the module

- Establishment: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9

- Entry: Configured by the operator; Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9

- Output: N/A

- Storage: Plaintext in RAM, Plaintext in Compact Flash

- Key-to-Entity: Process

25) SSHv2 DH Public Key

- Description: (2048 bit modulus); Used to establish shared secrets (SSHv2)

- Type: DH Public Key

- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; allowed method as per FIPS 140-2 IG D.8 Scenario 4

- Establishment: N/A

- Entry: N/A

- Output: Plaintext

- Storage: Plaintext in RAM, Plaintext in Compact Flash

- Key-to-Entity: Process

26) SSHv2 DH Peer Public Key

- Description: (2048 bit modulus); Used to establish shared secrets (SSHv2)

- Type: DH Peer Public Key

- Generation: N/A

- Establishment: N/A

- Entry: Plaintext

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: Process

27) TLS Host Public Key (RSA 2048 bit)

- Description: Used by client to encrypt TLS Pre-Master secret

- Type: TLS host Public key

- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.

- Establishment: N/A

- Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9

- Output: Plaintext

- Storage: Plaintext in RAM, Plaintext in Compact Flash

- Key-to-Entity: Process

28) TLS Peer Public Key (RSA 2048 bit)

- Description: Used to authenticate the client

- Type: TLS Peer Public Key

- Generation: N/A

- Establishment: N/A

- Entry: Plaintext during TLS v1.0/1.1 and v1.2 handshake protocol

- Output: N/A

- Storage: Plaintext in RAM, Plaintext in Compact Flash

- Key-to-Entity: Process

29) SNMPv3 secret

- Description: Used for authentication (SHA1, Password is 8 to 16 characters long) and for privacy (AES-CFB 128-bit, Password 12 to 20 characters)

- Type: Authentication data and privacy

- Generation: N/A - generated outside of the module

- Establishment: N/A

- Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session

- Output: SHA1 hashed in configuration, output encrypted / authenticated over SSHv2 session
- Storage: SHA1 digest and AES are stored in Compact Flash
- Key-to-Entity: Process: User
- Zeroization: Session termination and "fips zeroize all" command

30) NTP secret
- Description: Authentication (SHA1, Password is 8 to 16 characters long)
- Type: Authentication data
- Generation: N/A - generated outside of the module
- Establishment: N/A
- Entry: Configured by the operator, entered authenticated over SSHv2 session
- Output: SHA1 hashed in configuration, output authenticated over SSHv2 session
- Storage: SHA1 digest is stored in Compact Flash
- Key-to-Entity: Process: User
- Zeroization: Session termination and "fips zeroize all" command

THIS IS THE LAST PAGE OF THIS DOCUMENT
AND
REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK.