Brocade 7500 SAN Extension Switch Cryptographic Module Security Policy

Document *Version 1.2*

Brocade Communications

November 11, 2009

Copyright Brocade Communications 2009. May be reproduced only in its original entirety [without revision].

TABLE OF CONTENTS

1. Module Overview

The Brocade 7500 SAN Extension Switch Cryptographic Module (HW P/N Brocade 7500 Version H; FW Version Fabric OS v6.0.0) is a multiple-chip standalone cryptographic module, as defined by FIPS 140-2. The module is enclosed in a hard, opaque, commercial grade metal chassis. The module is a Fibre-channel and Gigabit Ethernet routing switch that provides secure network services and network management.

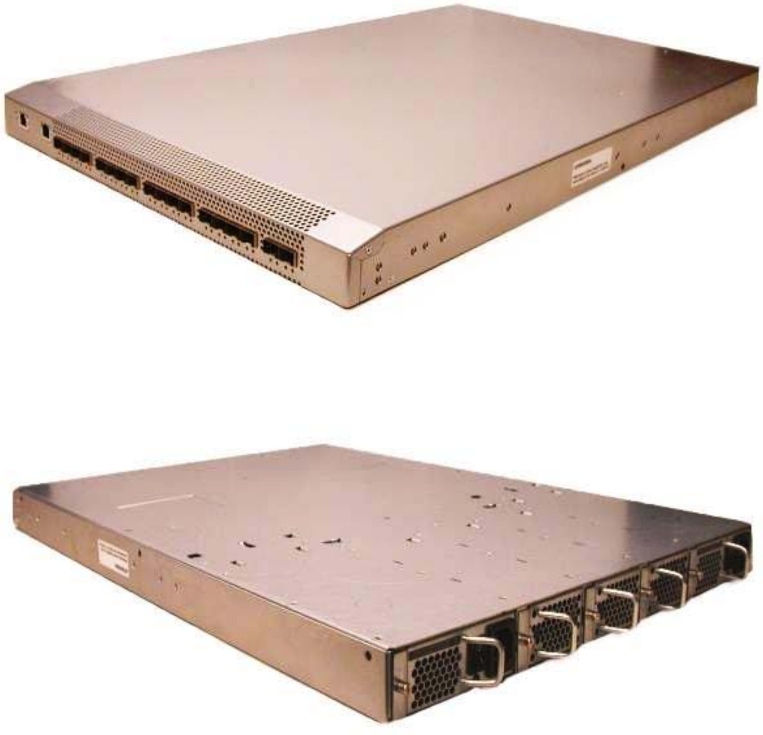

Figure 1 - Brocade 7500 SAN Extension Switch Cryptographic Module

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
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
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved mode of operation

The cryptographic module supports the following Approved algorithms in firmware (OpenSSL):

- AES (Cert. #731)
- Triple-DES (Cert. #652)
- SHA-1 (Cert. #749)
- SHA-256 (Cert. #749)
- HMAC-SHA-1 (Cert. #397)
- HMAC-SHA-256 (Cert. #397)
- RNG – ANSI x9.31 with 2 key TDES (Cert. #426)
- RSA (Cert. #342)

The following non-Approved algorithms and protocols are allowed within the Approved mode of operation:

- RSA Key Wrapping (key establishment methodology; 1024 bit keys provide 80 bits of encryption strength)
- Diffie-Hellman (DH) (key agreement; key establishment methodology provides 80 bits of encryption strength)
- SNMPv3 (Cryptographic functionality does not meet FIPS requirements and is considered plaintext)
- HMAC-MD5 to support Radius authentication
- NDRNG – used for seeding Approved RNG
- SSHv2 KDF
- TLS KDF with HMAC-MD5

The following algorithm is non-Approved and shall not be used as a security function in the Approved mode of operation.

- RC4

The cryptographic module shall be configured for FIPS mode via execution of the following procedure:

1. Disable Telnet, HTTP, Remote Procedure Call (RPC)
2. Enable HTTPS, Secure-RPC
3. Do not use FTP
    - Config Upload
    - Config Download
    - Support Save
    - FW Download
4. Disable Root Access
5. Do not use MD5 within Authentication Protocols: Diffie-Hellman with Challenge-Handshake Authentication Protocol (DH-CHAP) and FCAP
6. Do not define IKE or IPSec policies
7. Disable LDAP
8. Configure SNMP Access List for read-only access.
9. Enable Self-Tests
10. Within Radius, only use PEAP MS-CHAP V2

11. Enable Signed FW Download
12. Apply tamper seals (reference Section 9 for additional information)
13. Enable FIPS mode via the “fipscfg – enable fips” command

The operator can determine if the cryptographic module is running in FIPS vs. non-FIPS mode via execution of the CLI command, “fipscfg -- show” service. The module will return the following as an indicator for the FIPS Mode of Operation: “FIPS mode is: Enabled”. When operating in the Non-Approved mode of operation the following will be displayed “FIPS mode is: Disabled.”

Non-Approved mode of operation

In non-Approved mode, an operator will have no access to CSPs used within the Approved mode. When switching between FIPS and non-FIPS mode of operation, the operator is required to zeroize (by calling FIPSCfg –zeroize) the module’s plaintext CSPs.

4. Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

- Fiber Channel: Data Input, Data Output, Control Input, Status Output
- Gig-E: Data Input, Data Output, Control Input, Status Output
- Ethernet: Control Input, Status Output
- Serial port: Control Input, Status Output
- Power: Power Input, Control Input, Status Output
- Fan Tray Connector: Control Input, Status Output
- LEDs: Status Output

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module supports four operator roles. The cryptographic module shall enforce the separation of roles using role-based operator authentication. An operator must enter a username and its password to log in. The username is an alphanumeric string of maximum 40 characters. The password is an alphanumeric string of eight to 40 characters randomly chosen from the 96 printable and human-readable characters. Upon correct authentication, the role is selected based on the username of the operator and the context of the module. At the end of a session, the operator must log-out.

The module supports a maximum of 256 operators and five Radius servers that may be allocated the following roles:

Table 3 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Admin (Crypto-Officer)	Role-based operator authentication	Username and Password
User (User role)	Role-based operator authentication	Username and Password
Security Admin (Other role)	Role-based operator authentication	Username and Password
Fabric Admin (Other role)	Role-based operator authentication	Username and Password
Host/Server/Peer Switch (Other role)	Role-based operator authentication	PKI (FCAP) or Shared Secret (DH-CHAP)

Table 4 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/96^8 which is less than 1/1,000,000. The module can be configured to restrict the number of consecutive failed authentication attempts. If the module is not configured to restrict failed authentication attempts, then the maximum possible within one minute is 20. The probability of successfully authenticating to the module within one minute is 20/96^8 which is less than 1/100,000.
Digital Signature Verification (PKI)	The probability that a random attempt will succeed or a false acceptance will occur is 1/2^80 which is less than 1/1,000,000. The module will restrict the number of consecutive failed authentication attempts to 10. The probability of successfully authenticating to the module within one minute is 10/2^80 which is less than 1/100,000.
Knowledge of a Shared Secret	The probability that a random attempt will succeed or a false acceptance will occur is 1/96^8 which is less than 1/1,000,000.

	The maximum possible authentication attempts within one minute is 16. The probability of successfully authenticating to the module within one minute is 16/96^8 which is less than 1/100,000.

Table 5 – Service Descriptions

Service Name	Description
Authentication	Fabric element authentication, including selection of authentication protocols, protocol configuration selection and setting authentication secrets.
FIPSCfg	Control FIPS mode operation and related functions; zeroize all CSPs.
FirmwareManagement	Control firmware management.
PKI	PKI configuration functions, including FOS switch certificates and SSL certificates.
RADIUS	RADIUS configuration functions.
UserManagement	User and password management.

6. Access Control Policy

Roles and Services

Table 6 – Services Authorized for Roles

	User	Admin	FabricAdmin	SecurityAdmin	Host/Server/Peer Switch
Authentication		X		X	X
FIPSCfg		X		X	
FirmwareManagement	X	X	X	X	
PKI	X	X	X	X	

	User	Admin	FabricAdmin	SecurityAdmin	Host/Server/Peer Switch
RADIUS		X		X	
UserManagement		X		X	

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

- Self-tests: This service executes the suite of self-tests required by FIPS 140-2. Self-tests may be initiated by power-cycling the module.
- Show Status: This service is met through the various status outputs provided by the services provided above, as well as the LED interfaces.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- DH Private Keys for use with 1024 bit modulus.
- Fibre-Channel Security Protocol (FCSP) CHAP Secret
- Fibre-Channel Authentication Protocol (FCAP) Private Key (RSA 1024)
- SSH Session Key - 128, 192, and 256 bit AES CBC or TDES 2 and 3 key
- Secure Copy (SCP) Session Key - 128, 192, and 256 bit AES CBC or TDES 2 and 3 key
- TLS Private Key (RSA 1024)
- TLS Pre-Master Secret
- TLS Session Key - 128 bit AES
- TLS Authentication Key for HMAC-SHA-1
- RNG Seed Material
- Passwords
- Radius Secret

Definition of Public Keys

The following are the public keys contained in the module:

- DH Public Key (1024 bit modulus)
- DH Peer Public Key (1024 bit modulus)
- FCAP Public Key (RSA 1024)
- FCAP Peer Public Key (RSA 1024)
- TLS Public Key (RSA 1024)
- TLS Peer Public Key (RSA 1024)
- FW Download Key (RSA 1024)

Definition of CSPs Modes of Access

Table 6 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

R:	Read
W:	Write
N:	No Access
Z:	Zeroize

Table 7 – CSP Access Rights within Roles & Services

	SSH and SCP CSPs	TLS CSPs	RNG Seed Key	Passwords	RADIUS Secret	FCSP CHAP Secret	FCAP Private Key
Authentication	N	N	N	RW	N	RW	RW
FIPSCfg	Z	Z	Z	Z	Z	Z	Z
FirmwareManagement	R	N	N	N	N	N	N
PKI	RW	N	N	N	N	N	N
RADIUS	N	N	N	RW	RW	N	N
UserManagement	N	N	N	RW	N	N	N

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device supports a non-modifiable operational environment; only trusted, validated code signed by RSA may be executed.

8. Security Rules

The 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 security requirements of this FIPS 140-2 Level 2 module.

1. The cryptographic module shall provide four distinct operator roles.
2. The cryptographic module shall provide role-based authentication.
3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
4. The cryptographic module shall perform the following tests:
    - A. Power up Self-Tests:
        1. Cryptographic algorithm tests:
            - a. TDES KAT
            - b. AES KAT
            - c. HMAC SHA-1 KAT
            - d. SHA-1 KAT
            - e. HMAC SHA-256 KAT (SHA-256 tested within this self-test)
            - f. RNG KAT
            - g. RSA Sign/Verify KAT
            - h. RSA Encrypt/Decrypt KAT
        2. Firmware Integrity Test (128-bit EDC)
        3. Critical Functions Tests: N/A
    - B. Conditional Self-Tests:
        1. Continuous Random Number Generator (RNG) test – performed on NDRNG and RNG
        2. RSA Pairwise Consistency Test (Sign/Verify & Encrypt/Decrypt)
        3. Firmware Load Test (RSA Signature Verification)
5. Results of power up and conditional self-tests are recorded in the system log or are output to the local console. This includes logging both passing and failing results.
    - A. Status is indicated by the listing of the test condition and then "successful" (e.g.,

"AES encryption/decryption...successful")

B. Failure is indicted by error code and the listing of the failure condition (e.g., "24557:error:2A068065:lib(42):FIPS_selftest_aes:selftest failed")

6. At any time the cryptographic module is in an idle state, the operator shall be capable of commanding the module to perform the power-up self-test. Power-up self tests will be initiated by power cycling the module.
7. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

9. Physical Security Policy

To operate in FIPS Approved mode the tamper evident seals shall be installed as indicated.

The cryptographic boundary is defined as being the outer perimeter of the enclosure excluding one power supply unit and one fan tray unit. These excluded components are non-security relevant.

Physical Security Mechanisms

The multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure with tamper evident seals.
- Tamper evident seals. Reference Appendix A for detailed instructions on tamper seal placement.

Operator Required Actions

The operator is required to periodically inspect tamper evident seals.

Table 8 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals	12 months	The removed seal 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.

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.

Appendix A - Brocade 7500 SAN Extension Switch Tamper Seal Placement

To operate in FIPS Approved mode the tamper evident seals shall be installed as indicated.

Seal Application Instructions (20 Tamper Evident Seals)

For all seal applications, observe the following instructions.

- All surfaces to which the seals will be applied must be clean and dry. Use alcohol to clean the surfaces. Do not use other solvents.
- Do not use bare fingers to handle the seals. Use tweezers to avoid contaminating the adhesive. Slowly peel the backing from each seal, taking care not to touch the adhesive.
- When applying the seal, use a firm pressure across the entire seal surface to ensure maximum adhesion.
- Allow at least 30 minutes for the adhesive to cure. Tamper evidence may not be apparent until the adhesive cures.

Applying seals to the underside of the switch

You must apply the seals to the underside of the switch.

1. Attach one (1) seal (#1) covering the screw that holds the front cover on the left front underside of the enclosure. The seal should cover the screw head and bridge the seam between the front plate and the bottom plate.

   Ensure that the screw head is completely covered by the seal. See Figure A.1.

2. Attach six (6) seals (#2 - #7) covering the six rectangular holes on the underside of the enclosure.

   Ensure that each hole is completely covered by the seal. See Figure A.1.

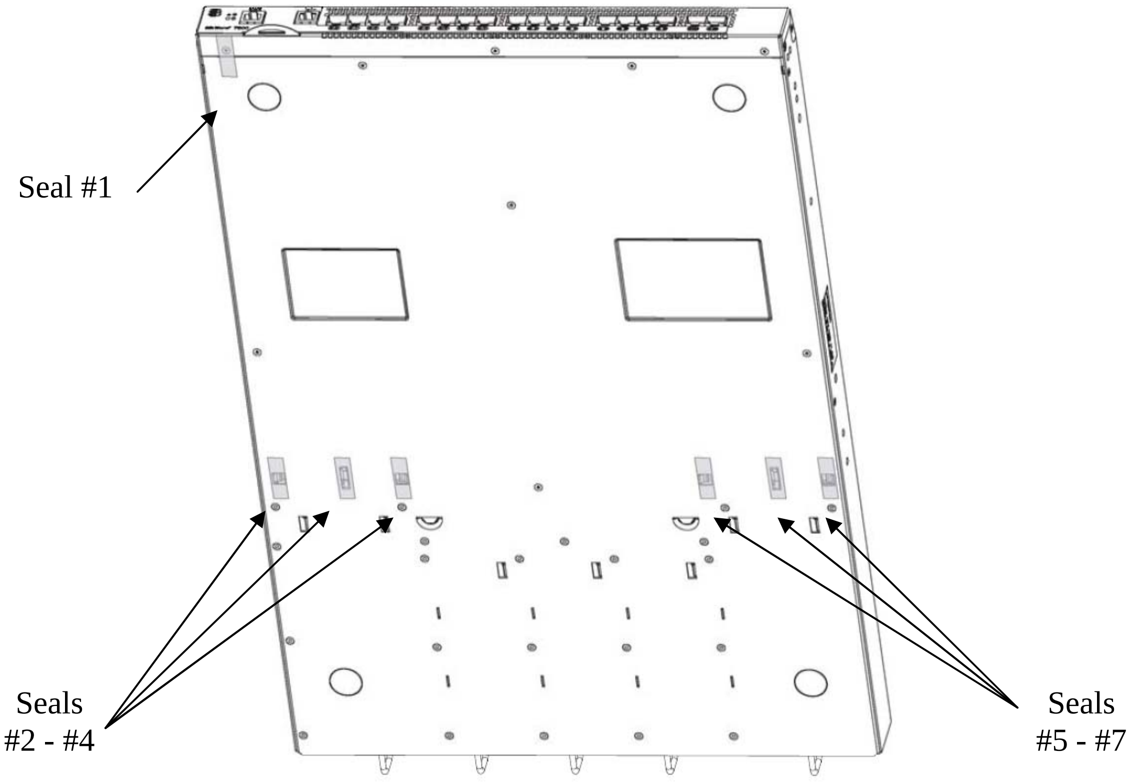

Figure A.1 – Brocade 7500 Switch Underside Seal Locations

Applying side panel seals

Cover exposed holes/screw locations as defined below for all mounting methods.

1. Attach four (4) seals (#8 - #12) oriented horizontally covering the seven (7) rail mounting screw holes on the left side of the enclosure. Ensure that all of the holes are completely covered. Working front to back, the first seal covers three holes, the second seal covers one hole, the third seal covers one hole, and the fourth seal covers two holes. Be sure the third seal does not cover any of the "Attention:" label. Attach one (1) seal oriented vertically covering the two holes near the front of the left side of the switch. Reference Figure A.2.
2. Repeat using five (5) seals (#13 - #17) on the right side of the enclosure. The seal arrangement is the same as the left side. Reference Figure A.3.

   Ensure that each hole is completely covered by the seal.

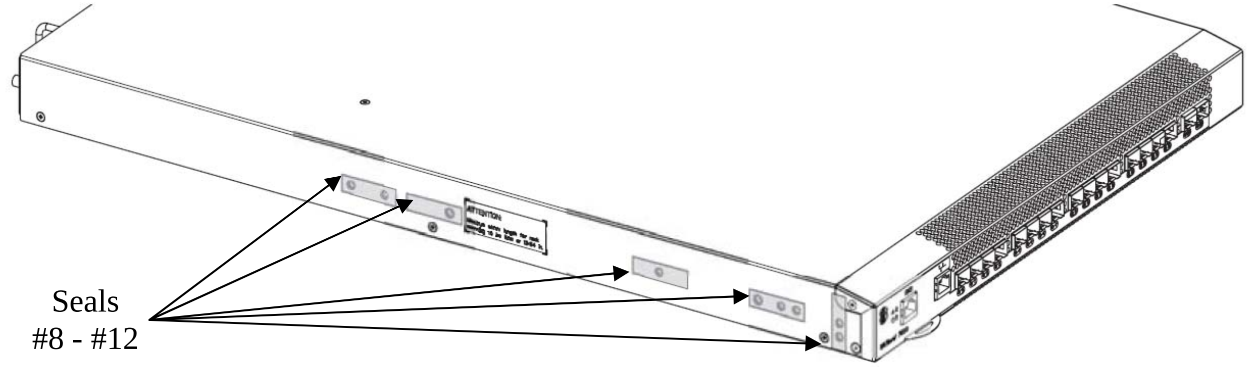

Figure A.2 –Left Side Seal Locations

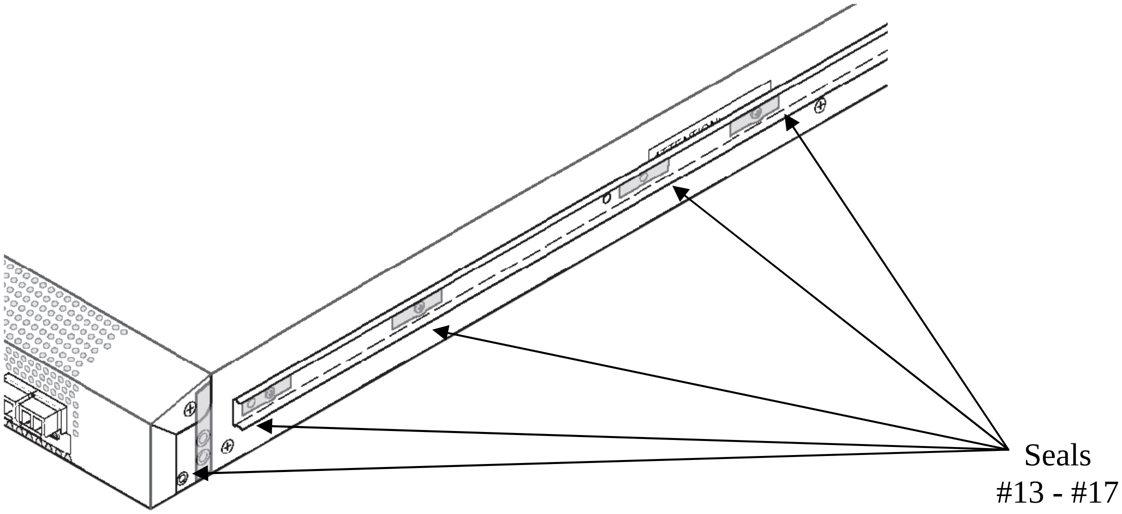

Figure A.3 - Right Side Seal Locations

Applying seals to the rear non-port side of the switch

You must apply seals (#18 - #20) to one of the power supplies and two of the fan assemblies to fully secure the non-port side of the switch.

See Figure A.4.

1. Attach one (1) seal oriented vertically to power supply #2. This is the leftmost power supply, on the non-port side of the switch. Apply the seal just above the thumbscrew and run it up and over the edge of the enclosure onto the top. Attach one (1) seal each, oriented vertically to fan assemblies #3 and #2. These are the two fans to the left on the non-port side of the switch. Apply the seals just above the thumbscrews and run them up and over the edge of the enclosure onto the top.

NOTE: Power supply #1 and fan assembly #1, the two field-replaceable units to the right, do not need security seals.

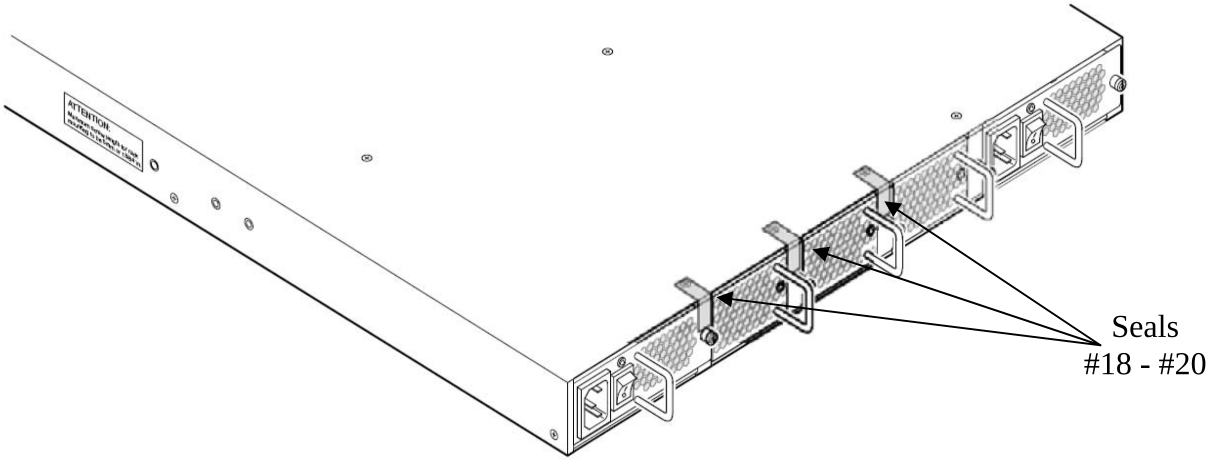

Figure A.4 – Brocade 7500 Switch Non-port Side (Rear) Seal Locations