BROCADE

Brocade VDX 6740, VDX 6740T and VDX 8770 Switches

FIPS 140-2 Non-Proprietary Security Policy

Document Version 1.02

Brocade Communications

12/17/2015

Revision History

Revision Date	Revision	Summary of Changes
8/25/2014	1.0	Initial Release
11/24/2015	1.01	Updates provided
12/17/2015	1.02	Updates provided

This Brocade Communications Systems Security Policy for Brocade VDX6740, VDX6740T and VDX8770 series of switches embodies Brocade Communications Systems' confidential and proprietary intellectual property. Brocade Systems retains all title and ownership in the Specification, including any revisions.

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

1 Module Overview

The VDX 6740, VDX 6740T and VDX 8770 are multi-chip standalone cryptographic modules, as defined by FIPS 140-2. The module(s) are available in multiple configurations that vary based on the hardware enclosure.

The cryptographic boundary for each module is the hard opaque commercial grade metal chassis enclosure with removable cover installed with tamper evident seals.

For the VDX 6740, and VDX 6740T the power supply and fan assemblies are not part of the cryptographic boundary. For VDX 8770 modules the power supply and fan assemblies are part of the cryptographic boundary. The module is a Gigabit Ethernet routing switch that provides secure network services and network management.

For each module to operate in a FIPS Approved mode of operation, the tamper evident seals supplied in Brocade XBR-000195 must be installed, as defined in Appendix A.

The 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 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.

Table 1 Firmware Version

Firmware	Part Number
Network OS (NOS) v5.0.0	63-1001501-01

Table 2 Validated VDX 6740 Configurations

SKU/MFG Part Number	Product Description	Firmware	FIPS KIT
SKU: BR-VDX6740-24-F P/N: 80-1007295-01	VDX6740,24-Port, AC, Non-port side exhaust[1]	NOS v5.0.0	XBR-000195
SKU: BR-VDX6740-24-R P/N: 80-1007294-01	VDX6740, 24-Port, AC, Port side exhaust[1]	NOS v5.0.0	XBR-000195
SKU: BR-VDX6740-48-F P/N: 80-1007483-01	VDX6740,24-Port, AC, SW-VDX-24POD10G LIC, Non-port side exhaust	NOS v5.0.0	XBR-000195
SKU: BR-VDX-6740-48-R P/N: 80-1007481-01	VDX6740, 48-Port, AC, SW-VDX-24POD10G LIC, Port side exhaust	NOS v5.0.0	XBR-000195
SKU: BR-VDX6740-64-ALLSW-F P/N: 80-1007484-01	VDX6740,64-Port, FCOE, AC, SW-FCOE-NOS-01, SW-VCSNOS-01, SWVDX-24POD10G and SW-VDX-4POD40G LIC, Non-port side exhaust	NOS v5.0.0	XBR-000195

SKU/MFG Part Number	Product Description	Firmware	FIPS KIT
SKU: BR-VDX6740-64-ALLSW-R P/N: 80-1007482-01	VDX6740,64-Port, FCOE, AC, SW-FCOE-NOS-01, SW-VCSNOS-01, SWVDX-24POD10G and SW-VDX-4POD40G LIC, Port side exhaust	NOS v5.0.0	XBR-000195

Table 2 Notes:

1. Port side and non-port side exhaust indicates whether the external fan direction causes air to be draw into the non-port side air vents and exhausted from the port side air vents or vice versa.

Table 3 Validated VDX 6740T Configurations

SKU/MFG Part Number	Product Description	Firmware	FIPS KIT
SKU: BR-VDX-6740T-24-F P/N: 80-1007273-01	VDX 6740T, 24-Port, 10GB-T, AC, Non-port side exhaust[1]	NOS v5.0.0	XBR-000195
SKU: BR-VDX-6740T-24-R P/N: 80-1007274-01	VDX 6740T, 24-Port, 10GB-T, AC, Port side exhaust[1]	NOS v5.0.0	XBR-000195
SKU: BR-VDX-6740T-48-F P/N: 80-1007485-01	VDX 6740T, 48-Port, 10GB-T, AC, SW-VDX-24POD10G LIC, Non-port side exhaust	NOS v5.0.0	XBR-000195
SKU: BR-VDX-6740T-48-R P/N: 80-1007487-01	VDX 6740T, 48-Port, 10GB-T, AC, SW-VDX-24POD10G LIC Port side exhaust	NOS v5.0.0	XBR-000195
SKU: BR-VDX6740T-64-ALLSW-F P/N: 80-1007486-01	VDX6740T,64-Port, 10GB-T, FCOE, AC, SW-FCOE-NOS-01, SW-VCSNOS-01, SWVDX-24POD10G and SW-VDX-4POD40G LIC, Non-port side exhaust	NOS v5.0.0	XBR-000195
SKU: BR-VDX6740T-64-ALLSW-R P/N: 80-1007488-01	VDX6740T,64-Port, 10GB-T, FCOE,AC, SW-FCOE-NOS-01, SW-VCSNOS-01, SWVDX-24POD10G and SW-VDX-4POD40G LIC, Port side exhaust	NOS v5.0.0	XBR-000195
SKU: BR-VDX6740T-56-1G-R P/N: 80-1007863-03	Brocade VDX 6740T-1G, 48P 1000BASE-T and 2 40 GbE QSFP+ ports, upgradable to 10GBASE-T via license only—no optics, AC, port-side exhaust airflow	NOS v5.0.0	XBR-000195
SKU: BR-VDX6740T-56-1G-F P/N: 80-1007864-03	Brocade VDX 6740T-1G, 48P 1000BASE-T and 2 40 GbE QSFP+ ports, upgradable to 10GBASE-T via license only—no optics, AC, non-port-side exhaust airflow	NOS v5.0.0	XBR-000195

Table 3 Notes:

1. Port side and non-port side exhaust indicates whether the external fan direction causes air to be draw into the non-port side air vents and exhausted from the port side air vents or vice versa.

Table 4 Validated VDX 8770 Configurations

SKU/MFG Part Number	Product Description	Firmware	FIPS KIT
SKU: BR-VDX8770-4-BND-AC P/N: 80-1005850-02	VDX 8770 4 I/O Slot chassis with three Switch Fabric Modules, one Management Module, two exhaust Fans and two 3000W AC PSU	NOS v5.0.0	XBR-000195
SKU: BR-VDX8770-4-BND-DC P/N: 80-1006532-03	VDX 8770 4 I/O Slot chassis with three Switch Fabric Modules, one Management Module, two exhaust Fans and two 3000W DC PSU	NOS v5.0.0	XBR-000195
SKU: BR-VDX8770-8-BND-AC P/N: 80-1005905-02	VDX 8770 8 I/O Slot chassis with six Switch Fabric Modules, one Management Module, 4 exhaust Fans and three 3000W AC PSU	NOS v5.0.0	XBR-000195
SKU: BR-VDX8770-8-BND-DC P/N: 80-1006533-03	VDX 8770 8 I/O Slot chassis with six Switch Fabric Modules, one Management Module, 4 exhaust Fans and three 3000W DC PSU	NOS v5.0.0	XBR-000195

The following field removable components: line cards, modules, power supplies and filler panels listed below may be used within validated Brocade VDX 8770-4 and VDX 8770-8 configurations:

Table 5 Components of the VDX 8770

Component of the cryptographic boundary		SKU/MGF Part Number
Field Replaceable Unit – Power Supply Module	AC	SKU XBR-ACPWR-3000 P/N 80-1006540-01
	DC	SKU XBR-DCPWR-3000 P/N 80-1006539-02
Field Replaceable Unit – Filler Panel for Power Supply Slot		SKU XBR-BLNK-PSU P/N 80-1006430-01
Field Replaceable Unit – Fan Module		SKU XBR-FAN-FRU P/N 80-1006080-01
Field Replaceable Unit – Switch Fabric Module		SKU BR-VDX8770-SFM-1 P/N 80-1006295-01
Field Replaceable Unit – Management Module		SKU BR-VDX8770-MM-1 P/N 80-1006294-02

Component of the cryptographic boundary		SKU/MGF Part Number
Field Replaceable Unit – Line Card Unit	48X1G Line Card	SKU BR-VDX8770-48X1G-SFP-1 P/N 80-1006049-02
	12X40GE Line Card	SKU BR-VDX8770-12X40G-QSFP-1 P/N 80-1006293-02
	48X10G Line Card	SKU BR-VDX8770-48X10G-SFPP-1 P/N 80-1006048-02
Field Replaceable Unit – Filler Panel for Line Card Slot		SKU XBR-BLNK-FULL P/N 80-1006431-01
Field Replaceable Unit – Half-Slot Filler Panel for Switch Fabric Module Slot or Management Module Slot		SKU XBR-BLNK-HALF P/N 80-1006429-01

Figure 1 through Figure 3 illustrate the cryptographic module configurations. With the exception of VDX 8770-4 and VDX 8770-8 shown below, power supplies and fan assemblies are not within cryptographic boundary.

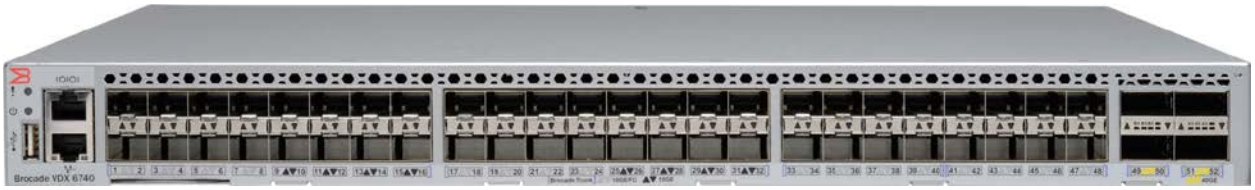

Figure 1 VDX 6740-24, VDX 6740-48 and VDX 6740-64

Table 2 lists the validated configurations for the VDX 6740-24, VDX 6740-48[1] and VDX 6740-64[2].

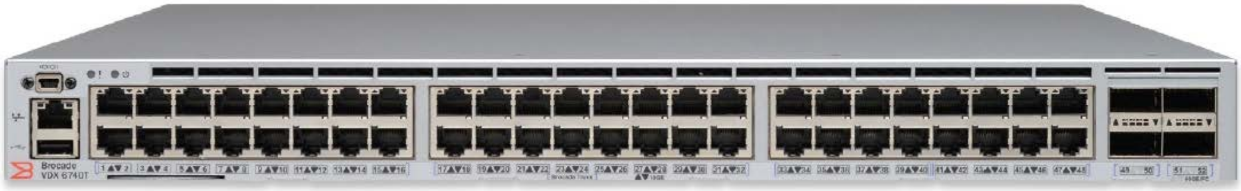

Figure 2A VDX 6740T-24, VDX 6740T-48[3] and VDX 6740T-64[4]

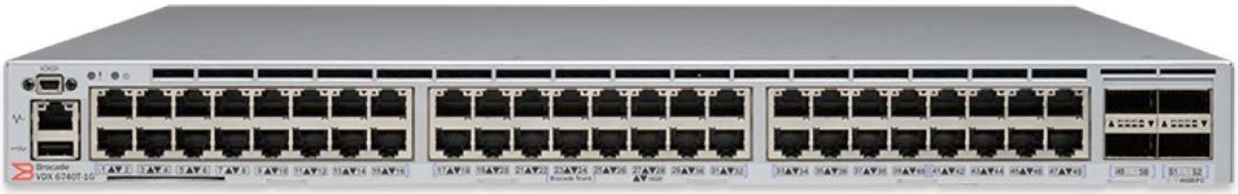

Figure 2B VDX 6740T-56-1G and VDX 6740T-56-1G

[1] The SW-VDX-24POD10G license enables additional ports

[2] SW-FCOE-NOS-01, SW-VCSNOS-01, SWVDX-24POD10G and SW-VDX-4POD40G licenses enable additional ports and features

[3] The SW-VDX-24POD10G license enables ports 25 to 48

[4] SW-FCOE-NOS-01, SW-VCSNOS-01, SWVDX-24POD10G and SW-VDX-4POD40G LIC enable ports 25 to 64

Table 3 lists the validated configurations for the VDX 6740T-24, VDX 6740T-48 and VDX 6740T-64.

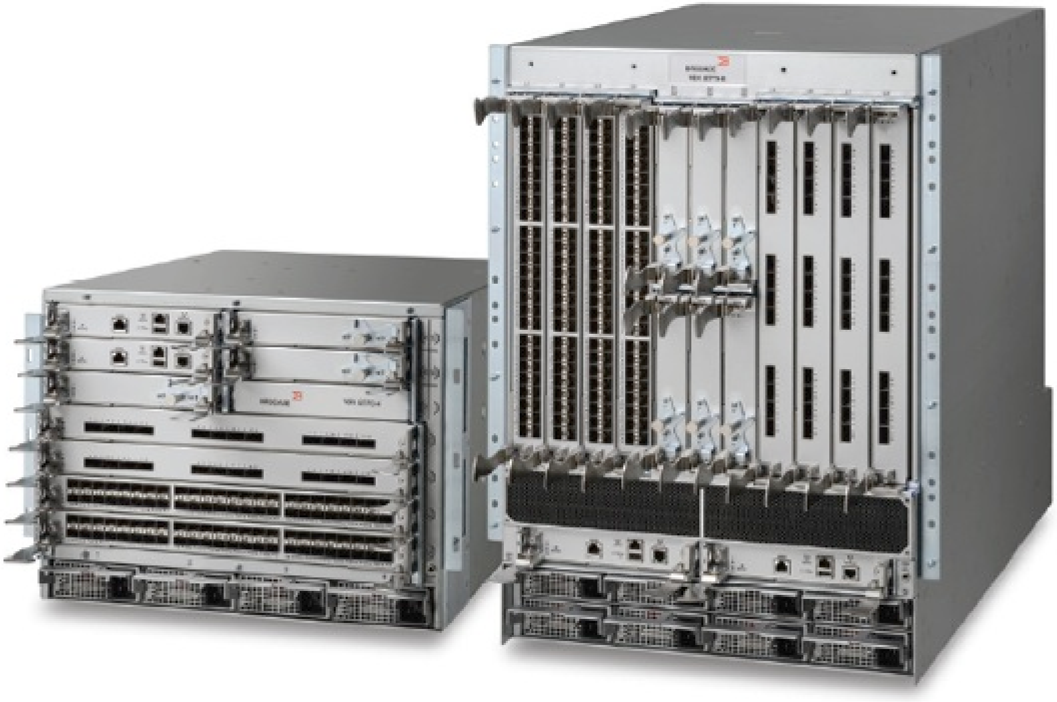

Figure 3 VDX 8770-4 and VDX 8770-8[5]

1.1 Security Level Definitions

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

Table 6 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

[5] Each removable module in the chassis (except the fans) has a matching filler panel that must be in place if no module is installed in a slot. The two modules shown in this picture are fully populated with management modules, switch fabric modules, line cards, and power supplies per Table 5 Components of the VDX 8770. There are no filler panels for the fans since all fans must be installed on the chassis.

2 Modes of Operation

2.1 FIPS Approved mode of operation

The cryptographic module supports the following Approved algorithms in firmware

Table 7a FIPS Approved Cryptographic Functions

Label	Cryptographic Function	Certificate Number
AES	Advanced Encryption Algorithm	2937
Triple-DES	Triple Data Encryption Algorithm	1745
SHS	Secure Hash Algorithm	2473
HMAC	Keyed-Hash Message Authentication code	1861
RSA	Rivest Shamir Adleman Signature Algorithm	1540
ECDSA	Elliptic Curve Digital Signature Algorithm	530
RNG	Random Number Generator	1296
CVL	SP800-135 KDF (TLS v1.0/1.1 and v1.2)**	338
CVL	SP800-135 KDF (SSHv2) **	338
CVL	SP800-56A ECC CDH Primitive	337

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.

** NOTE: As per FIPS 140-2 Implementation Guidance D.11, Brocade hereby states that the following protocols have not been reviewed or tested by the CAVP or CMVP:

- TLS v1.0/1.1
- TLS v1.2
- SSHv2

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

- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- HMAC-MD5 to support RADIUS authentication
- MD5 (used for password hash, considered as plain text)
- Non-deterministic random number generator for seeding ANSI X9.31 DRNG
- OSPF is considered as plaintext interface (No protection is claimed for protocol data exchange).

The cryptographic module may be configured for FIPS 140-2 mode via execution of the following procedure.

- Install removable front cover (as applicable) and apply tamper labels
- Login as authorized user with admin role.
- Configure the system in standalone or fabric cluster mode as needed.

- Disable Boot PROM Access.
- For LDAP authentication, Configure FIPS 140-2 compliant ciphers (AES256-SHA, AES128-SHA, DES-CBC3-SHA) for LDAP.
- Configure FIPS 140-2 compliant ciphers (HMAC-SHA1 (mac) , AES128-CBC, AES256-CBC) for SSHv2.
- Disable root access.
- If TACACS+ is configured, then remove the configuration.
- If dot1x is configured, disable it.
- If vCenter is configured, then remove the configuration.
- *If FC-SP authentication is configured, update DH group to use key sizes greater than 2048.*
- *If autoupload is enabled, disable it.*
- Enter the following commands:
    - cipherset ssh sha256
    - cipherset ssh
    - cipherset ldap
    - cipherset radius
- Enable FIPS 140-2 Self tests i.e. Execute 'fips selftests'
- Execute 'fips zeroize' (automatically reboot(s) the system).
- After reboot, Http, HTTPS, Telnet and some ports of Brocade internal servers must be blocked in FIPS 140-2 mode. Once the switch is in the fips compliant mode, HTTP (80), HTTPS (443), Telnet (23) and Brocade internal server ports (TCP: 2301, 2401, 3016, 3516, 4516, 5016, 7013, 7110, 7710, 9013, 9110, 9710, 9910-10110. UDP: 33351, 36851, 37731, and 50690) must be blocked, and passwords of the default accounts (admin and user) should be changed after every zeroization operation to maintain FIPS 140-2 compliance.
    - Note:
        - If SSHv2 access is required, configure to open ports 22 and 830(netconf).
        - If remote access is required, such as through SCP or LDAP, configure to allow UDP and TCP traffic on ports 1024 through 65535.
- For LDAP authentication, import minimum 2048 bits RSA LDAP CA certificate.
- For RADIUS authentication, configure the RADIUS server with PEAP-MSCHAPv2 mode and shared secret.
  Note: This is a protocol that relies on the strength of TLSv1.0, which is utilizing RSA 2048 with SHA-256 and FIPS Approved cipher suites (AES, HMAC-SHA-1). TLSv1.2 is not supported for RADIUS.
- If secure sys log is needed, import minimum 2048 bits RSA CA certificate. In FIPS 140-2 compliant state,
    - Do not use FTP for following operations
    - Config Upload
    - Config Download
    - Support Save
    - FW Download
    - Do not use outbound SSHv2 and telnet commands (clients).
    - With regards to SCP client on the switch, remote SCP server must employ RSA host keys with minimum length of 2048 bits and DH with minimum length of 2048 bit. FIPS 140-2 compliant ciphers (HMAC-SHA1 (mac), AES128-CBC, AES256-CBC) are enforced on the client side.
- The use of the "disable cipherconfig" command is not allowed in FIPS mode.
- Externally generated RSA key pairs shall only be imported if they are RSA 2048 and SHA-256.
- Do not expire Admin account.
- Do not enable Admin lockout.

NOTES:

1. Firmware packages are always signed at build time and validated during the firmwaredownload operation.
2. USB interface: Authorized operator is required to maintain the physical possession (at all times) of the USB token and shall not provide to unauthorized individuals/entities.

The operator can determine if the cryptographic module is running in FIPS 140-2 vs. non-Approved mode by performing the following operations

- Display the status of self-tests, and accounts.
- Display the status of boot prom access.
- Display of cipherset configuration.
- Display of IP ACLs configuration.
- Confirm LDAP server's root CA certificate.

2.2 Non-Approved Mode of Operation

In non-Approved mode, an operator will have no access to CSPs used within the FIPS Approved mode. When switching from FIPS Approved mode to a non-Approved mode of operation, the operator is required to zeroize the module's plaintext CSPs, by calling "fips zeroize".

NOTE: The module provides the following non-FIPS approved algorithms only in non-FIPS mode of operation. The use of any such service is an explicit violation of this Security Policy and is explicitly disallowed by this Security Policy.

Table 7b NonFIPS Mode Services

Crypto Function/Service	*User Role Change*	*Additional Details*
Cipher suites for SSL and TLS	Crypto-Officer	AES-128-ECB (non-compliant); AES-192-CBC (non-compliant); AES-192-ECB (non-compliant); AES-256-ECB (non-compliant); BF; BF-CBC; BF-CFB; BF-ECB; BF- OFB; CAST; CAST-CBC; CAST5-CBC; CAST5-CFB; CAST5-ECB; CAST5-OFB; DES; DES-CBC; DES-CFB; DES-ECB; DES-EDE; DES-EDE- CBC; DES-EDE-CFB; DES-EDE-OFB; DESEDE3; DES-EDE3-CBC; DES-EDE3-CFB; DES-EDE3-OFB; DES-OFB; DES3; DESX; RC2; RC2-40-CBC; RC2-64-CBC; RC2-CBC; RC2-CFB; RC2-ECB; RC-OFB; RC4; RC4-40
Message Digests for SSL and TLS	Crypto-Officer	MD2; MD4; RMD160
Ciphers and Message Authentication Codes for configuring SSH	Crypto-Officer	Ciphers: AES-128-CTR (non-compliant); AES-192-CTR (non-compliant); AES-256-CTR (non-compliant); ARCFOUR256; ARCFOUR128; 3DES-CBC (non-compliant); BLOWFISH-CBC; CAST128-CBC; AES-192-CBC (non-compliant); ARCFOUR Message Authentication Codes: HMAC-MD5; HMAC-SHA-1 (non-compliant); UMAC-64; HMAC-RIPEMD160; HMAC-SHA-1-96 (non-compliant); HMAC-MD5-96
SNMP	Crypto-Officer	SNMPv1 (plaintext) and SNMPv3 KDF (non-compliant); Algorithms: SHA-1 (non-compliant) and MD5

RADIUS or LDAP	Crypto-Officer	PAP and CHAP authentication method for RADIUS (all considered as plaintext) RADIUS and LDAP are supported with CA certificates of any size (512 to 2048 and above) signed with MD5, SHA-1 (non-compliant), SHA-256 (non-compliant) LDAP uses TLS connections in non-FIPS mode without certificates
Telnet	N/A	N/A
FTP	Crypto-Officer	Config Upload, Config Download, Support Save, FW Download, autoftp
RSA	Crypto-Officer	RSA key size < 2048 bits for SSH and TLS
Diffie-Hellman	Crypto-Officer	DH key size < 2048 bits for SSH

3 Ports and Interfaces

The list of all cryptographic modules along with physical ports and logical interfaces are captured below:

1. VDX 6740-24-F, VDX 6740-24-R, VDX 6740-48-F, VDX 6740-48-R, VDX 6740-64-ALLSW-F, VDX 6740-64-ALLSW-R
   a. Data Port (Qty. 64): Data Input, Data Output, Control Input, Status Output
      - 1G/10G SFP+ ports (Qty. 48) supporting both 1G and 10G data rates
        - ♦ Thirty-two of the forty-eight ports are 10G universal ports which can be configured as Ethernet ports (1G/10G) or Fiber Channel ports (8G/16G)
      - QSFP ports (Qty. 4)
        - ♦ 40G QSFP ports can be used as a native 40G Ethernet port or as four 16G Fiber Channel ports

   b. Management Ethernet Ports (Qty. 1): Control Input, Status Output
   c. Serial port (Qty. 1): Control Input, Status Output
   d. USB (Qty. 1): Data Input, Data Output, Status Output
      - Brocade USB flash device, XBR-DCX-0131

   e. Power Supply and Fan Assembly (Qty. 2)
      - Assembly Connectors (Qty. 2): Power Input, Control Input
      - Assembly Status LED (Qty. 2): Status Output

   f. LEDs: Status Output
      - System Power LED (Qty. 1)
      - System Status LED (Qty. 1)
      - Power Supply and Fan Status LED (Qty. 2)

2. VDX 6740T-24-F, VDX 6740T-24-R, VDX 6740T-48-F, VDX 6740T-48-R, VDX 6740T-64-ALLSW-F, VDX 6740T-64-ALLSW –R, VDX6740T-56-1G-R, VDX6740T-56-1G-F
   a. Data Port (Qty. 64): Data Input, Data Output, Control Input, Status Output
      - 1G/10G SFP+ ports (Qty. 48) supporting both 1G and 10G data rates
        - ♦ Thirty-two of the forty-eight ports are 10G universal ports which can be configured as Ethernet ports (1G/10G) or Fiber Channel ports (8G/16G)
      - QSFP ports (Qty. 4)
        - ♦ 40G QSFP ports can be used as a native 40G Ethernet port or as four 16G Fiber Channel ports

   b. Management Ethernet Ports (Qty. 1): Control Input, Status Output
   c. Serial port (Qty. 1): Control Input, Status Output
   d. USB (Qty. 1): Data Input, Data Output, Status Output
      - Brocade USB flash device, XBR-DCX-0131

   e. Power Supply and Fan Assembly (Qty. 2)
      - Assembly Connectors (Qty. 2): Power Input, Control Input
      - Assembly Status LED (Qty. 2): Status Output

f. LEDs

- System Power LED (Qty. 1)
- System Status LED (Qty. 1)
- Power Supply and Fan Status LED (Qty. 2)

3. VDX 8770-4 and VDX 8770-8

a. Line card:

- BR-VDX8770-48X10G-SFPP-1 (48x10G):
    - 10 GbE port (Qty. 48): Data Input, Data Output
    - LEDs: Status Output
        i. Status LED (Qty. 1)
        ii. Power LED (Qty. 1)
        iii. Status Port LED (Qty. 48)
- BR-VDX8770-12X40G-QSFP-1 (12x40G):
    - 40 GbE port (Qty. 12): Data Input, Data Output
    - LEDs: Status Output
        i. Status LED (Qty. 1)
        ii. Power LED (Qty. 1)
- Status Port LED (Qty. 12)
- BR-VDX8770-48X1G-SFP-1:
    - 1 GbE port (Qty. 48): Data Input, Data Output
    - LEDs: Status Output
        i. Status LED (Qty. 1)
        ii. Power LED (Qty. 1)
        iii. Status Port LED (Qty. 48)

b. Management Module (MM) (half-slot) :

- USB port (Qty. 1): Data Input, Data Output
- Console Port (RJ45 - serial) (Qty. 1):Control Input, Status Output
- Ethernet port (Mgmt IP) (RJ45) (Qty. 1): Control Input, Status Output
- Ethernet port (Service IP) (Qty. 1): Control Input, Status Output
- LEDs: Status Output
    - Status LED (Qty. 1)
    - Power LED (Qty. 1)
    - Active LED (Qty. 1)
    - Ethernet management link (upper left) (Qty. 1)
    - Ethernet management link activity (upper right) (Qty. 1)

c. Switch Fabric Module (SFM)

- LEDs: Status Output
    - Status LED (Qty. 1)
    - Power LED (Qty. 1)

d. Power Supply
- AC Inlet (quantity 1): Power
- LEDs: Status Output
  - ♦ AC power input LED (AC OK) (Qty. 1)
  - ♦ DC power output LED (DC OK) (Qty. 1)
  - ♦ Alarm LED (ALM) (Qty. 1)

e. Fan Assembly
- LEDs: Status Output
  - ♦ Power LED (Qty. 1)
  - ♦ Fault LED (Qty. 1)

NOTE: LEDs display power status and port activity status.

4 Identification and Authentication Policy

4.1 Assumption of roles

The cryptographic module supports five 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 forty (40) characters. The password is an alphanumeric string of eight (8) to forty (40) characters randomly chosen from the ninety-six (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.

Forty-eight (48) concurrent operators are allowed on the switch.

Table 8 Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Admin (Crypto-Officer): Admin role has the permission to access and execute all the available services.	Role-based operator authentication	Username and Password
User (User role): User role has the permission to display general configuration.	Role-based operator authentication	Username and Password
Maximum Permissions (for a custom role): A custom role can be created and assigned the custom permissions.	Role -based operator authentication	Username and Password
LDAP: If LDAP is configured, LDAP server authenticates to the cryptographic module.	Role-based operator authentication	LDAP Root CA certificate
RADIUS: If RADIUS is configured, RADIUS server authenticates to the cryptographic module.	Role-based operator authentication	RADIUS Shared Secret

Table 9 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 a minute are 16. The probability of successfully authenticating to the module within one minute is 16/96^8 which is less than 1/100,000.

Table 10 Service Descriptions

Service Name	Description
User Management	User and password management.
Login Session Management	Controls the user session management,
LDAP	LDAP configuration functions.
RADIUS	RADIUS configuration functions
FIPS	Control FIPS mode operation and related functions
Firmware Management	Control firmware management.
PKI	Import LDAP root CA certificate.
Clock Management	Clock and Time zone Management
Debug & Diagnostics	Debug & Diagnostics tools.
CLI Management	CLI Management tools
Platform	Platform tools
Display	Display configuration and operational commands
Terminal Configuration	Terminal configuration operations
Ethernet	Ethernet Management
License	License Management
VCS	Cluster services
vCenter	VMware-ESX hosts Management
SNMP	SNMP (Non-compliant. Only allowed in non-Approved mode of operation.)
System Monitor	Status configuration & monitoring
Zeroize	Destroy all CSPs
FCSP	Security policies for Fibre Channel ports
Switch Connection Policy	Policy to allow/block switches into the fabric

5 Access Control Policy

5.1 Roles and Services

Table 11 Services Authorized for Roles

SERVICE \ ROLE	User	Admin	Maximum Permissions	LDAP	RADIUS
User Management		X	X		
Login Session Management		X	X		
PKI	X	X	X		
Firmware Management	X	X	X		
FIPS		X	X		
Zeroize		X	X		
Clock Management		X	X		
Debug & Diagnostics		X	X		
CLI Management		X	X		
Platform		X	X		
Display		X	X		
RADIUS		X	X		X
LDAP		X	X	X	
Terminal Configuration		X	X		
Ethernet		X	X		
License		X	X		
VCS		X	X		
vCenter		X	X		
SNMP (Non-compliant. Only allowed in Non-Approved mode of operation.)		X	X		
System Monitor		X	X		
FCSP		X	X		
Switch Connection Policy		X	X		

5.2 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.

5.3 Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module. The module generates cryptographic keys whose strengths are modified by available entropy.

SSHv2 and SCP CSPs:

- DH Private Keys (256 bits) for use with 2048 bit modulus
- SSHv2/SCP/SFTP Session Keys- 128 and 256 bit AES CBC
- SSHv2/SCP/SFTP Authentication Key
- SSHv2 KDF Internal State
- SSHv2 DH Shared Secret Key (2048 bits)
- SSHv2 ECDSA Host Private Key (P-256)
- Value of K during SSHv2 256 ECDSA session
- SSHv2 ECDH Shared Secret Key (P-256, P-384 and P-521)
- SSHv2 ECDH Private Key (P-256, P-384 and P-521)
- SSHv2 RSA 2048 bit Host Private Key

TLS CSPs:

- TLS Pre-Master Secret
- TLS Master Secret
- TLS KDF Internal State
- TLS Session Key – 128, 256 bit AES CBC, Triple-DES 3 Key CBC
- TLS Authentication Key for HMAC-SHA-1, HMAC-SHA-256

RNG Seed CSPs:

- Approved RNG Seed Material
- ANSI X9.31 DRNG Internal State

Operator Authentication/Passwords:

- Passwords
- RADIUS Secret

5.4 Definition of Public Keys:

The following are the public keys contained in the module:

- DH Public Key (2048 bit modulus)
- SSHv2 DH Peer Public Key (2048 bit modulus)
- DH Keys for FC-SP (2048 bit modulus)
- TLS v1.0 Peer Public Key (RSA 2048)
- Firmware Download Public Key (RSA 2048 SHA-256)
- LDAP ROOT CA certificate (RSA 2048)
- SSHv2 RSA 2048 bit Peer Public Key
- SSHv2 RSA 2048 bit Host Public key
- SSHv2 ECDSA Host Public Key (P-256)
- SSHv2 ECDSA Peer Public Key (P-256)
- SSHv2 ECDH Public Key (P-256, P-384 and P-521)

5.5 Definition of Service Categories:

Table 12 Services and Command Line Instructions (CLI)

Services	CLIs
User Management	Username role password-attributes rule encryption-level unlock
Login Session Management	tacacs-server ldap-server aaa logout banner ssh telnet
PKI	Certutil
Firmware Management	Firmware
Fips	fips selftests cipherset prom-access
Zeroize	fips zeroize
Clock Management	Clock Ntp
Debug & Diagnostics	Debug diag ping l2traceroute traceroute top undebug
CLI Mgmt	no delete configure dir exit help history quit rename abort do pwd unhide unhide fips prompt1 prompt2 rbridge-id

Services	CLIs
Platform	reload chassis clear copy fastboot usb logging service switch-attributes support auditlog autoupload beacon cidrecov df ha oscmd power-off power-on linecard
Display	Show
Terminal Configuration	send terminal end line
Ethernet	dot1x cee-map interface ip ipv6 lacp mac mac-address-table port-profile protocol qos rmon sflow vlan monitor arp class-map mac-rebalance police-priority-map policy-map resequence reserved-vlan route-map router system-max fabric fcoe bp-rate-limit zoning

Services	CLIs
License	License Dpod
VCS	Vcs
vCenter	Vcenter Vnetwork
SNMP (Non-compliant. Only allowed in Non-Approved mode of operation.)	snmp-server
System Monitor	system-monitor system-monitor-mail threshold-monitor
FCSP	Fcsp
Switch connection policy	secpolicy

Legend:

N – Not used
R - Read
W - Write
Z - Zeroize

Table 13 CSP Access Rights within Roles & Services

	SSHv2 and SCP CSPs[6]	TLS CSPs[7]	RNG Seed Key[8]	Operator Authentication/Passwords	RADIUS Secret	FCSP Secret	SSHv2 RSA 2048 Public Key
Login Session Management	N	N	N	RW	N	N	N
Zeroize	Z	Z	Z	Z	Z	Z	N
Firmware Management	R	N	N	N	N	N	N
PKI	RW	N	N	N	N	N	RW
RADIUS	N	N	N	RW	RW	N	N
User Management	N	N	N	RW	N	N	N
FCSP	N	N	N	N	N	RW	N

[6] Includes the following CSPs: DH Private Keys (256 bits) for use with 2048 bit modulus, SSHv2/SCP/SFTP Session Keys- 128 and 256 bit AES CBC , SSHv2/SCP/SFTP Authentication Key , SSHv2 KDF Internal State, SSHv2 DH Shared Secret Key (2048 bits), SSHv2 ECDSA Host Private Key (P-256), Value of K during SSHv2 256 ECDSA session, SSHv2 ECDH Shared Secret Key (P-256, P-384 and P-521) , SSHv2 ECDH Private Key (P-256, P-384 and P-521), SSHv2 RSA 2048 bit Host Private Key

[7] Includes the following CSPs: TLS Pre-Master Secret, TLS Master Secret, TLS KDF Internal State, TLS Session Key – 128, 256 bit AES CBC, Triple-DES 3 Key CBC, TLS Authentication Key for HMAC-SHA-1, HMAC-SHA-256

[8] Includes the following CSPs: Approved RNG Seed Material; ANSI X9.31 DRNG Internal State

6 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device supports a limited operational environment; only trusted, validated code signed by RSA 2048 with SHA256 digest may be executed.

6.1 Security Rules

The cryptographic modules' design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The cryptographic module shall provide five 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:
        i. Cryptographic algorithm tests:
            (1) Three Key Triple-DES CBC KAT (encrypt/decrypt)
            (2) AES (128, 192, 256) CBC KAT (encrypt)
            (3) AES (128, 192, 256) CBC KAT (decrypt)
            (4) ANSI X9.31 DRNG KAT
            (5) SHA-1, 256, 384, 512 KAT
            (6) HMAC SHA-1, 224, 256, 384, 512 KAT
            (7) RSA 2048 SHA 256 Sign/Verify KAT
            (8) SP800-135 TLS v1.0 KDF KAT
            (9) SP800-135 TLS v1.2 KDF KAT
            (10)SP800-135 SSHv2 KDF KAT
            (11) EC-DH KAT
            (12) ECDSA KAT
        ii. Firmware Integrity Test (128-bit EDC)
        iii. Critical Functions Tests:
            (1) RSA 2048 Encrypt/Decrypt KAT
    b. Conditional Self Tests:
        i. Continuous Random Number Generator (RNG) test – performed on Non-deterministic hardware based random number generator and ANSI X9.31 DRNG
        ii. RSA 2048 SHA- 256 Pairwise Consistency Test (Sign/Verify & Encrypt/Decrypt)
        iii. RSA 2048 Pair wise Consistency Test (Encrypt/Decrypt)
        iv. ECDSA Pairwise Consistency Test (Sign/Verify)
        v. Firmware Load Test (RSA 2048 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 shall be capable of commanding the module to perform the power-up self-tests by rebooting the module.
6. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
7. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

8. The serial port may only be accessed by the Crypto-Officer when the Crypto-Officer is physically present at the cryptographic boundary, via a direct connection without any network access or other intervening systems.
9. The following protocols have not been reviewed or tested by the CAVP nor CMVP:
   a. TLS v1.0
   b. TLS v1.2
   c. SSHv2
   d. SNMPv3 (non-compliant; Only allowed in Non-Approved mode of operation)
10. As per FIPS 140-2 Implementation Guidance 7.9, the authorized operator performing the zeroization service shall be physically present at the cryptographic boundary and in full control of the module for the duration of the zeroization to observe that the zeroization was completed successfully.
    The operator shall follow this procedure to zeroize and confirm the successful completion:
    a. Issue the zeroize command, "`fips zeroize`"
    b. Confirm the status by examining the following status on the console:
       i. "`FIPS Zeroize operation executed successfully`"

7 Physical Security Policy

7.1 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.

7.2 Operator Required Actions

The operator must periodically inspect the tamper evident seals applied to the modules within the operator's scope of responsibility for evidence of tampering.

Table 14 Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test
Tamper Evident Seals	12 months

8 Mitigation of Other Attacks Policy

These modules have not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.

9 Definitions and Acronyms

10 GbE	10 Gigabit Ethernet
AES	Advanced Encryption Standard
Blade	Blade server
CBC	Cipher Block Chaining
CLI	Command Line interface
CSP	Critical Security Parameter
DH	Diffie-Hellman
FIPS	Federal Information Processing Standard
FOS	Fabric Operating System
GbE	Gigabit Ethernet
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
KAT	Known Answer Test
KDF	Key Derivation Function
LED	Light Emitting Diode
LDAP	Lightweight Directory Access Protocol
LIC	License
MAC	Message Authentication Code
MM	Management Module
NTP	Network Time Protocol
NOS	Network Operating System
PKI	Public Key Infrastructure
PROM	Programmable read-only memory
PSU	Power Supply Unit
RADIUS	Remote Authentication Dial In User Service
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SCP	Secure Copy Protocol
SFM	Switch Fabric Module
SHA	Secure Hash Algorithm
SSHv2	Secure Shell Protocol
TLS	Transport Layer Security Protocol

Appendix A: Tamper Evident Seal Application Procedures

Use ethyl alcohol to clean the surface area at each tamper evident seal placement location. 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 ethyl alcohol to clean off any residual adhesive remover before applying a new seal.

Applying seals to the Brocade VDX 6740

Twenty (20) tamper evident seals are required to complete the physical security requirements for the –R and –F configurations of the BR-VDX 6740-24, BR-VDX 6740-48 and BR-VDX 6740-64-ALLSW. See Figure 4 through Figure 8 for details on how to position each seal.

1. Apply one (1) seal over the screws along the bottom port side surface of the chassis. Five (5) seals, 1 to 5, are required to complete this step. See Figure 4 for details on how to position each seal.
2. Apply three (3) seals, 6 to 8, across the seam between the left side of the top cover and the bottom side of the chassis. Each seal must wrap across a 90 degree angle from the bottom of the chassis to the side of the top cover. See Figure 5 on how to position each seal.
3. Apply three (3) seals, 9 to 11, across the seam between the right side of the top cover and the bottom of the chassis. Each seal must wrap across a 90 degree angle from the bottom of the chassis to the side of the top cover. See Figure 6 on how to position each seal.
4. Six (6) seals, 12 to 17, are required to complete this step. Seals 13, 14 and16 must wrap across a 90 degree angle from the top of the chassis to the external surface of the combination power supply and fan module. Seals 15 and 17 must wrap across a 90 degree angle from the bottom of the chassis to the external surface of the combination power supply and fan module. Seal 12 bridges the seam between the chassis the combination power supply and fan module on the left side of the non-port side of the chassis. See Figure 7 for details on how to position each seal.
5. Apply one (1) seal over the screws along the top port side surface of the chassis. Three (3) seals, 18 to 20, are required to complete this step. See Figure 8 for details on how to position each seal.

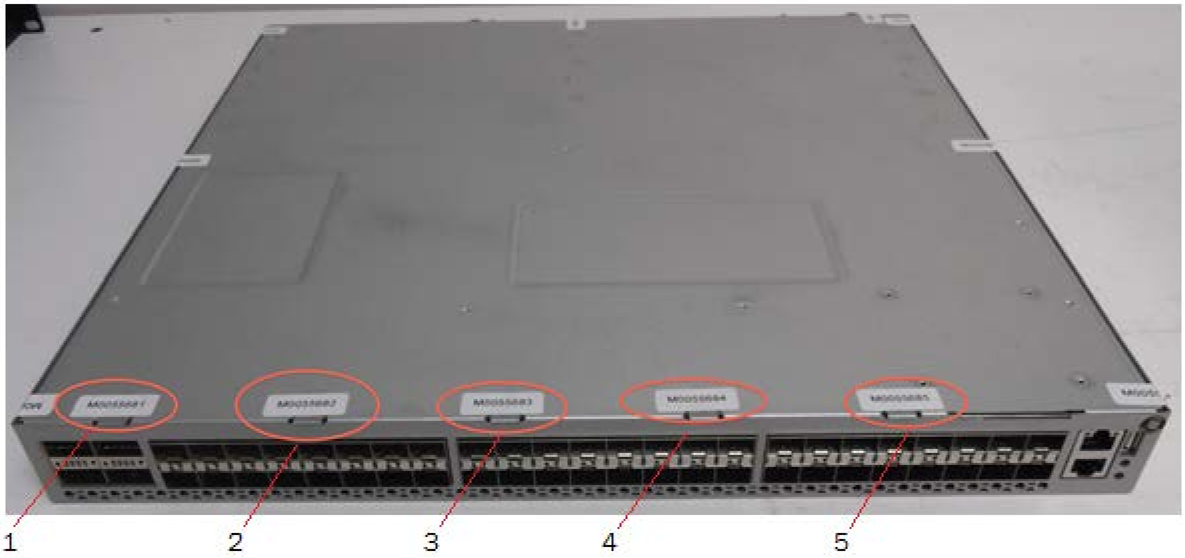

Figure 4 VDX 6740-24, VDX 6740-48 and VDX 6740-64-ALLSW bottom port side seal locations

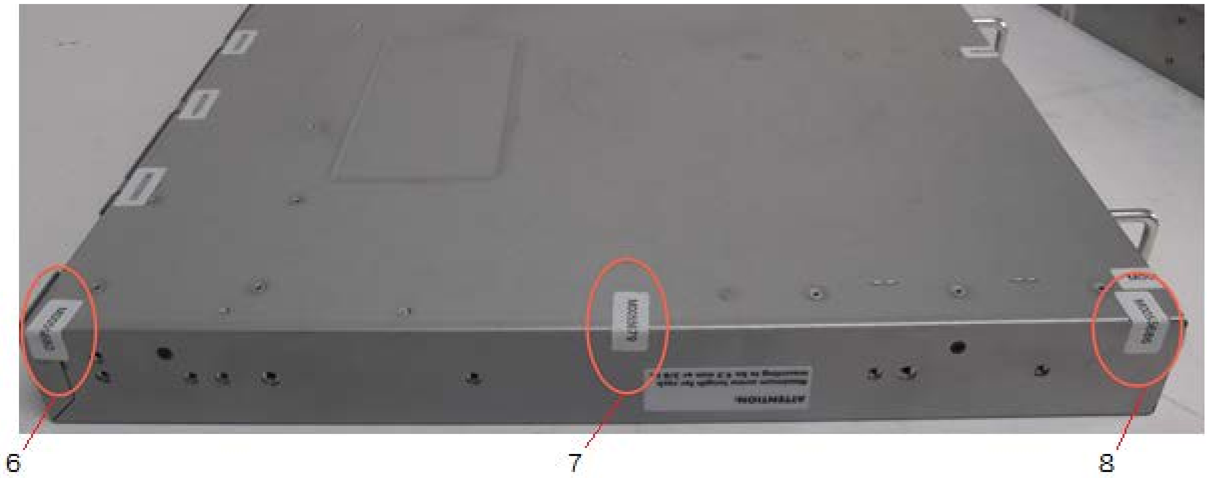

Figure 5 VDX 6740-24, VDX 6740-48 and VDX 6740-64-ALLSW bottom left side seal locations

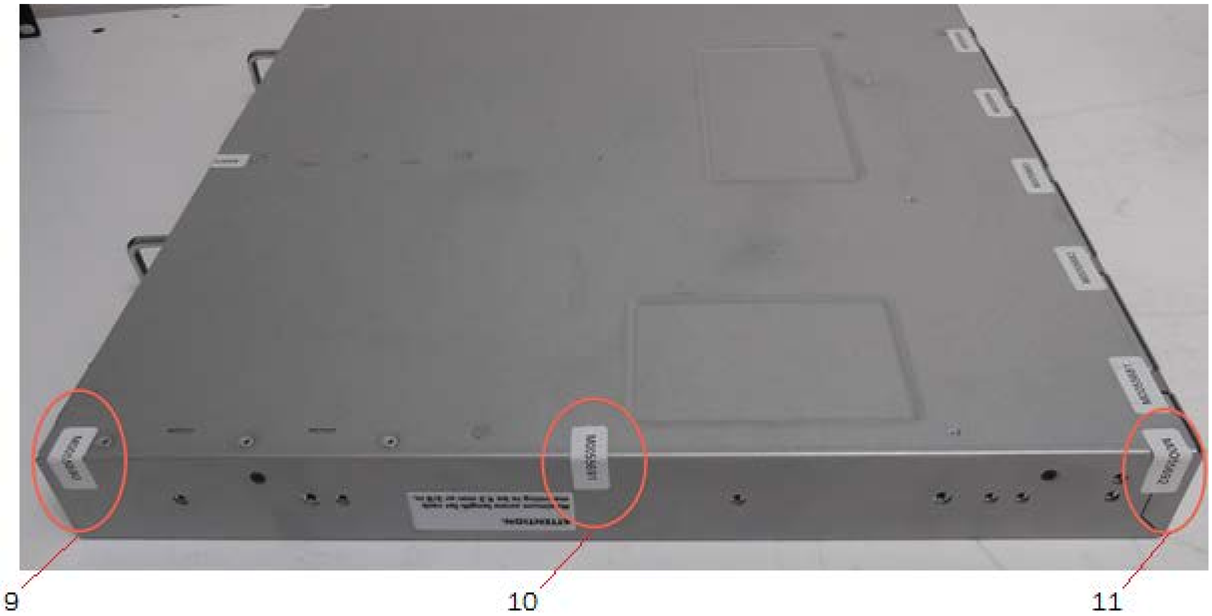

Figure 6 VDX 6740-24, VDX 6740-48 and VDX 6740-64-ALLSW bottom right side seal locations

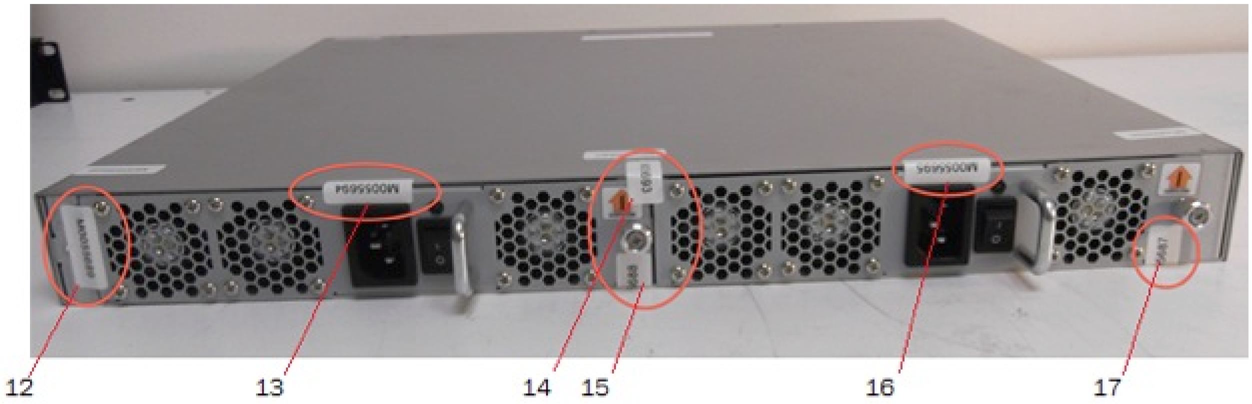

Figure 7 VDX 6740-24, VDX 6740-48 and VDX 6740-64-ALLSW top non-port side fan and power supply seal locations

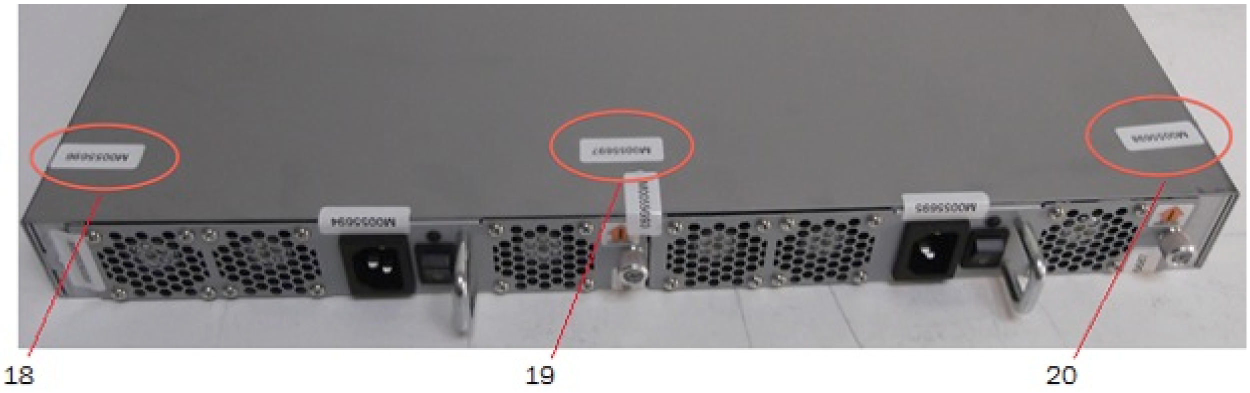

Figure 8 VDX 6740-24, VDX 6740-48 and VDX 6740-64-ALLSW top non-port side top cover seal locations

Applying seals to the Brocade VDX 6740T-24, VDX 6740T-48, VDX 6740T-64 and VDX 6740T-56-1G

Twenty-Nine (29) tamper evident seals are required to complete the physical security requirements for the VDX 6740T-24, VDX 6740T-48, VDX 6740T-64 and VDX 6740T-56-1G. See Figure 9 through Figure 13 for details on how to position each seal.

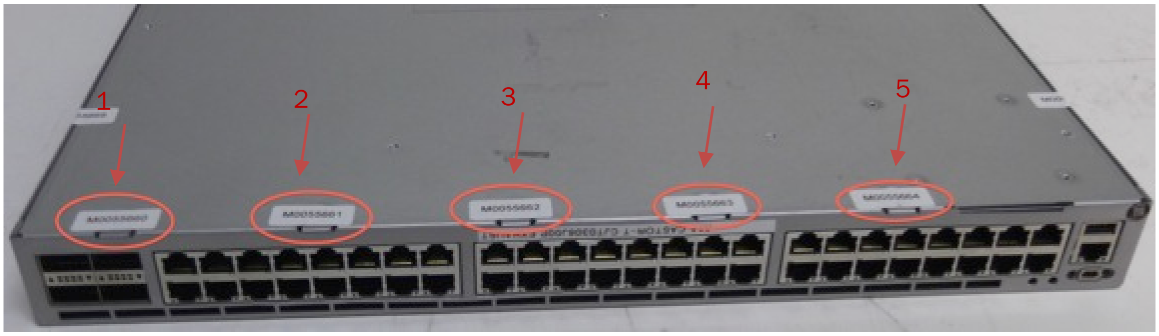

Figure 9 VDX 6740T-24, VDX 6740T-48, VDX 6740T-64 and VDX 6740T-56-1G bottom/front seal locations

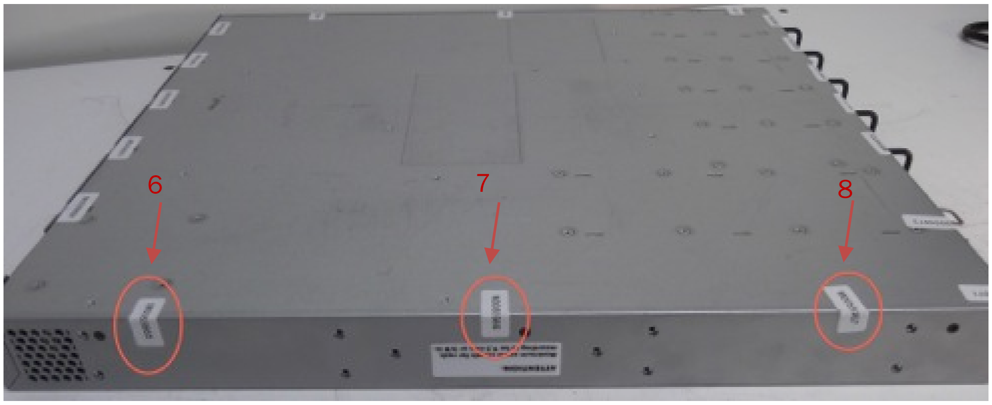

Figure 10 VDX 6740T-24, VDX 6740T-48, VDX 6740T-64 and VDX 6740T-56-1G bottom left side seal locations

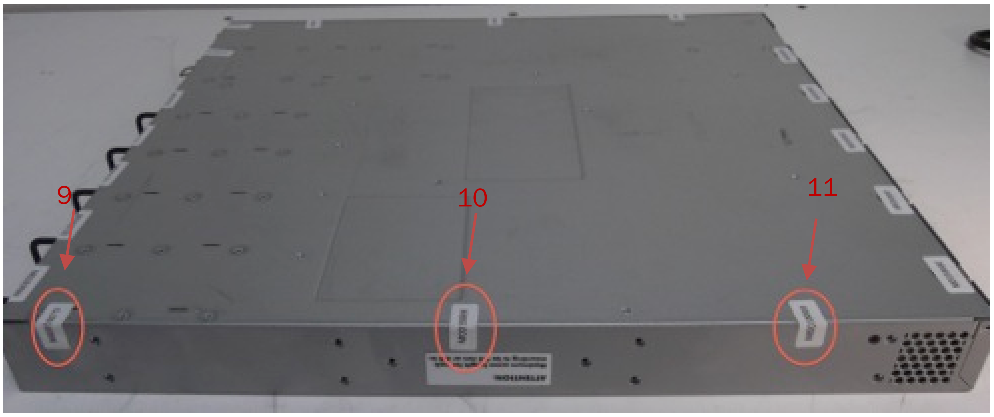

Figure 11 VDX 6740T-24, VDX 6740T-48, VDX 6740T-64 and VDX 6740T-56-1G bottom right side seal locations

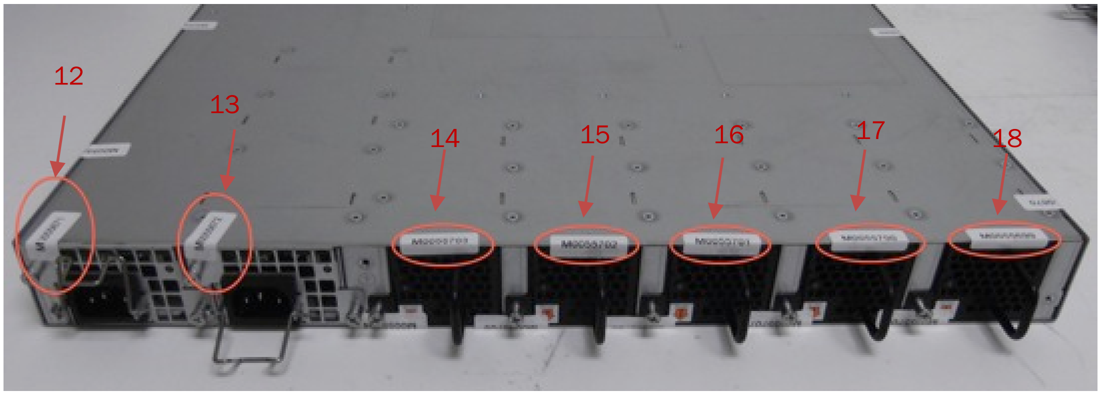

Figure 12 VDX 6740T-24, VDX 6740T-48, VDX 6740T-64 and VDX 6740T-56-1G bottom back side seal locations

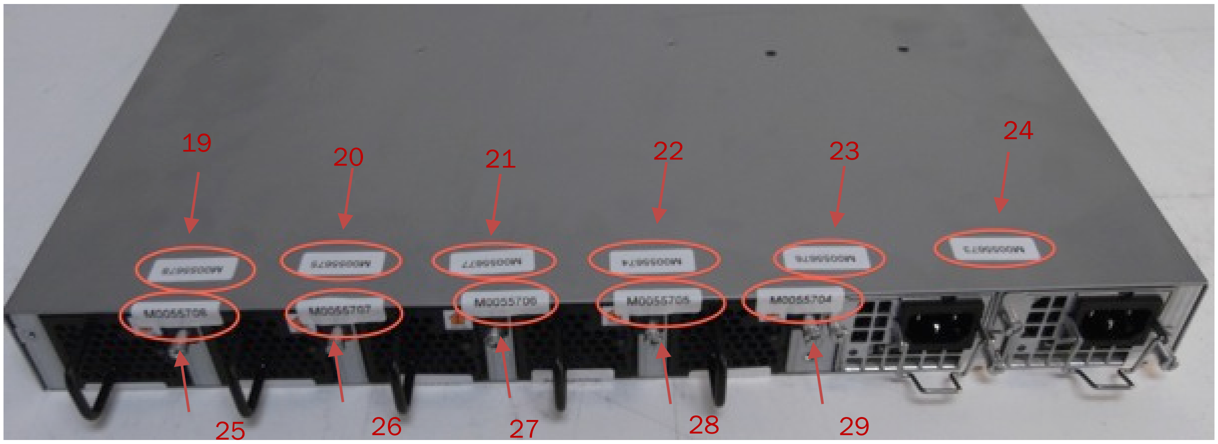

Figure 13 VDX 6740T-24, VDX 6740T-48, VDX 6740T-64 and VDX 6740T-56-1G top back side seal locations

Applying seals to the Brocade VDX 8770-8 with AC and DC Power Supply

Thirty-six (36) tamper evident seals are required to complete the physical security requirements illustrated in Figure 14 to Figure 16.

VDX 8770-8 AC Port Side Tamper Evident Seal Application Procedure

Twenty-eight (28) tamper evident seals are required to complete steps 1 to 6 on the port side as illustrated in Figure 14. Unused slots must be filled with the module or filler panel appropriate for that slot to maintain adequate cooling.

1. Apply one (1) seal to each blade or filler panel installed in line card slots L1 through L8. Eight (8) seals are required to complete this step. See Figures 14A, 14C, 14D and 14E for details on how to position each seal.
2. Apply one (1) seal to each Switch Fabric Module (SFM) or filler panel installed in SFM slots S1, S3 and S5. Three (3) seals are required to complete this step. See Figure 14B and 14E for details on how to position each seal.
3. Apply one (1) seal to each Switch Fabric Module (SFM) or filler panel installed in SFM slots S2, S4 and S6. Three (3) seals are required to complete this step. See Figure 14E and 14G for details on how to position each seal.
4. Apply two (2) seals to each Management Module (MM) or filler panel installed in MM slots M1 and M2. Four (4) seals are required to complete this step. See Figure 14E, 14F and 14H for details on how to position each seal.
5. For VDX 8770-8 with AC Power Supply Units (PSU) see Figures 14E and 14F for details on how to position seals 14-17. Four (4) seals are required to complete this step.
6. See Figure 14E and 14H for details on how to position seals 21-26. Six (6) seals are required to complete this step.

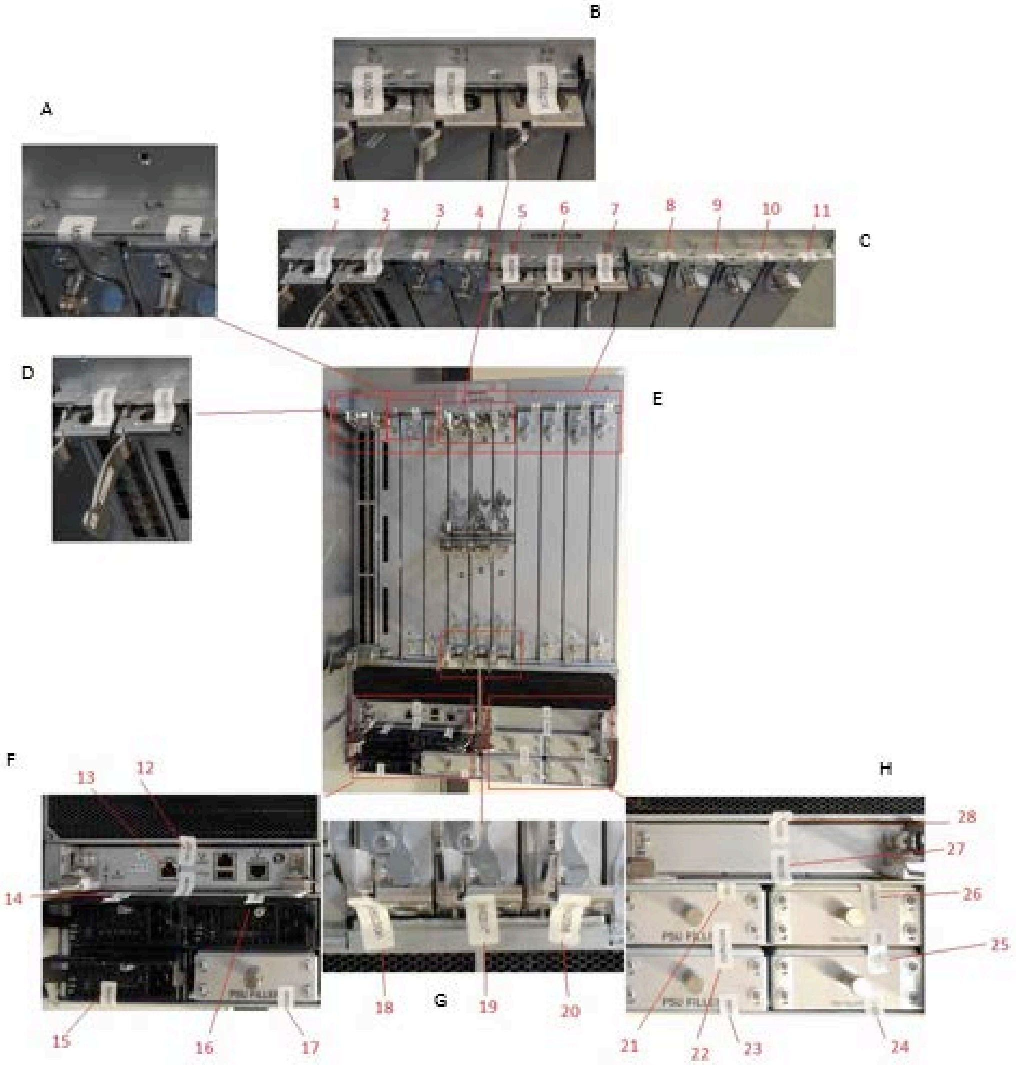

Figure 14 Brocade VDX 8770-8 AC PSU port side seal locations

VDX 8770-8 DC Port Side Tamper Evident Seal Application Procedure

Twenty-eight (28) tamper evident seals are required to complete steps 1 to 6 on the port side as illustrated in Figure 15. Unused slots must be filled with the module or filler panel appropriate for that slot to maintain adequate cooling.

1. Apply one (1) seal to each blade or filler panel installed in line card slots L1 through L8. Eight (8) seals are required to complete this step. See Figures 15A, 15C, 15D and 15E for details on how to position each seal.
2. Apply one (1) seal to each Switch Fabric Module (SFM) or filler panel installed in SFM slots S1, S3 and S5. Three (3) seals are required to complete this step. See Figure 15B and 15E for details on how to position each seal.
3. Apply one (1) seal to each Switch Fabric Module (SFM) or filler panel installed in SFM slots S2, S4 and S6. Three (3) seals are required to complete this step. See Figure 15E and 15H for details on how to position each seal.
4. Apply two (2) seals to each Management Module (MM) or filler panel installed in MM slots M1 and M2. Four (4) seals are required to complete this step. See Figure 15E, 15F and 15I for details on how to position each seal.
5. For VDX 8770-8 with DC Power Supply Units (PSU) refer to Figures 15E, 15F and 15G for details on how to position seals 14-17. Four (4) seals are needed to complete this step.
6. See Figures 15E and 15I on how to position seals 21-26. Six (6) seals are required to complete this step.

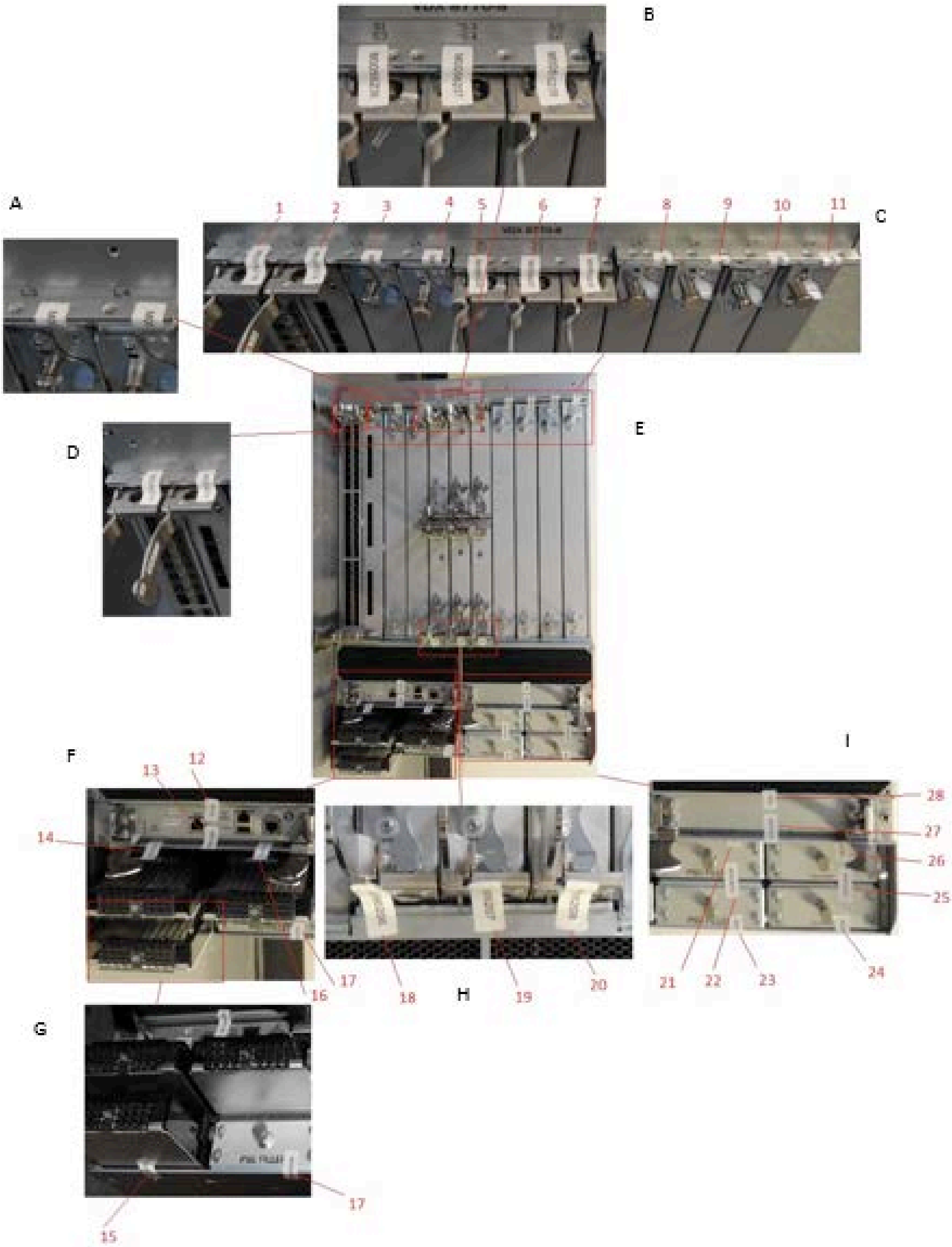

Figure 15 Brocade VDX 8770-8 DC PSU Port Side seal locations

VDX 8770-8 Non-Port Side Tamper Evident Seal Application Procedure

Eight (8) tamper evident seals are required to complete the physical security requirements illustrated in Figure 16. All fan slots must be filled with a FAN FRU or FAN FRU filler panel to maintain adequate cooling.

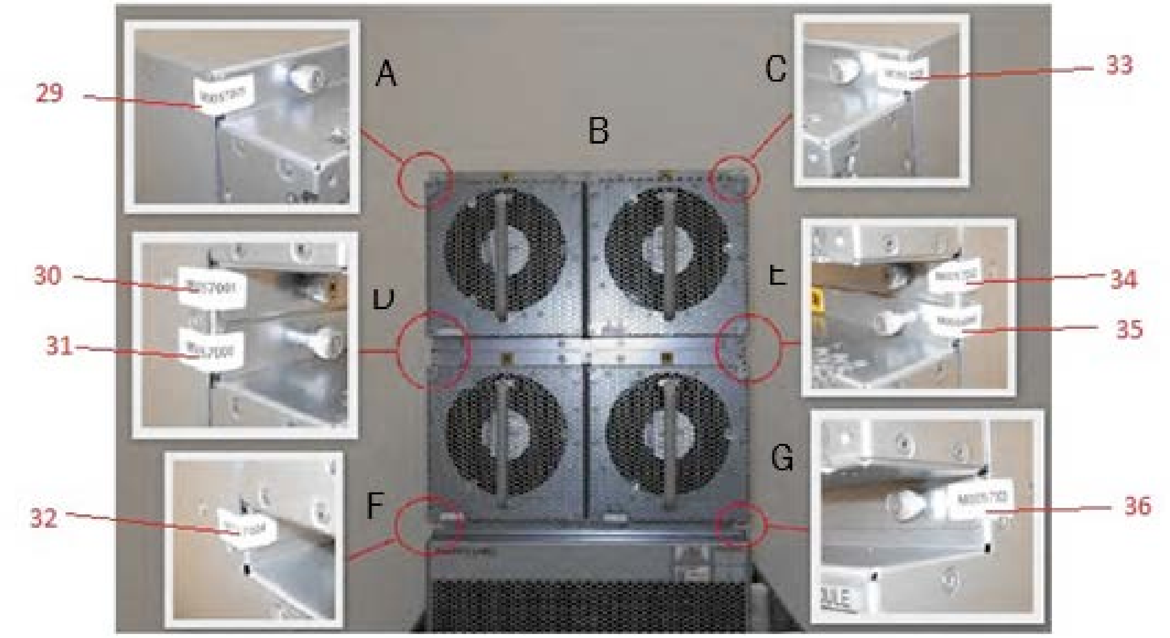

Figure 16 Brocade VDX 8770-8 non-port side seal locations

1. Apply two (2) seals to each FAN FRU or FAN FRU filler panel installed in the non-port side of the VDX 8770-8. Eight (8) seals are required to complete this step. See Figure 16A-G for details on how to position each seal.

Applying seals to the Brocade VDX 8770-4

Twenty-three (23) tamper evident seals are required to complete the physical security requirements illustrated in Figure 17, Figure 18, Figure 19 and Figure 20.

VDX 8770-4 Port Side Tamper Evident Seal Application Procedure

Fifteen (15) tamper evident seals are required to complete the physical security requirements illustrated in Figure 17. Unused slots must be filled with the module or filler panel appropriate for that slot to maintain adequate cooling.

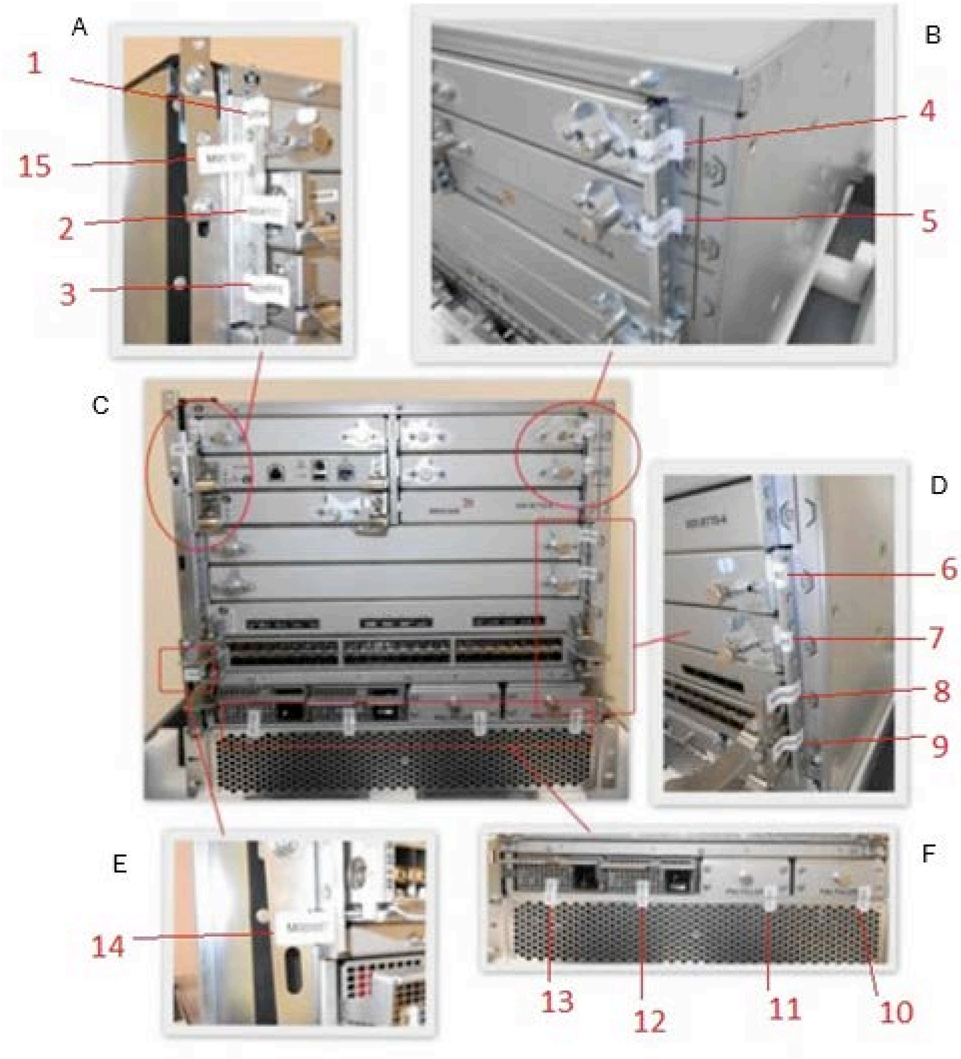

Figure 17 Brocade VDX 8770-4 port side seal locations

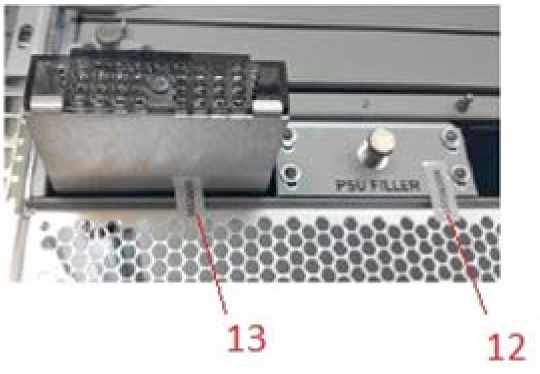

Figure 18 Brocade VDX 8770-4 DC PSU seal locations

1. Apply one (1) seal to each Switch Fabric Module (SFM) or filler panel installed in SFM slots S1, S2 and S3. Three (3) seals are required to complete this step. See Figure 17A and Figure 17C for details on how to position each seal.
2. Apply one (1) seal to each Management Module (MM) or filler panel installed in MM slots M1 and M2. Two (2) seals are required to complete this step. See Figure 17B and Figure 17C for details on how to position each seal.
3. Apply one (1) seal to each blade or filler panel installed in line card slots L1 through L4. Four (4) seals are required to complete this step. See Figure 17C and Figure 17D for details on how to position each seal.
4. The VDX 8770-4 accepts both AC and DC power supply module. Depending on the type of installed power supply module complete step 4a or 4b.
    a. For a VDX 8770-4 with AC Power Supply Units (PSU) apply one (1) seal to each AC PSU or PSU filler panel installed in PSU slots P1 through P4. For this example, an AC PSUs are installed in slots P1 and P2. PSU filler panels are installed in slots P3 and P4. Four (4) seals are required to complete this step. See Figure 17F for details on how to position each seal.
    b. For a VDX 8770-4 with DC Power Supply Units (PSU) apply one (1) seal to each DC PSU or PSU filler panel installed in PSU slots P1 through P4. For this example, a DC PSUs are installed in slot P1. A PSU filler panels are installed in slot P2. Four (4) seals are required to complete this step. See Figure 18 and Figure 17F for details on how to position each seal.
5. Apply one (1) seal on each FIPS bracket. The upper left FIPS bracket is shown in Figure 17A and 17C. The lower left FIPS bracket is shown in Figure 17E and 17C. Two (2) seals are required to complete this step. See Figure 17A and Figure 17E for details on how to position each seal.

VDX 8770-4 Non-Port Side Tamper Evident Seal Application Procedure

Five (5) tamper evident seals are required to complete the physical security requirements illustrated in Figure 19. All fan slots must be filled with a FAN FRU or FAN FRU filler panel to maintain adequate cooling.

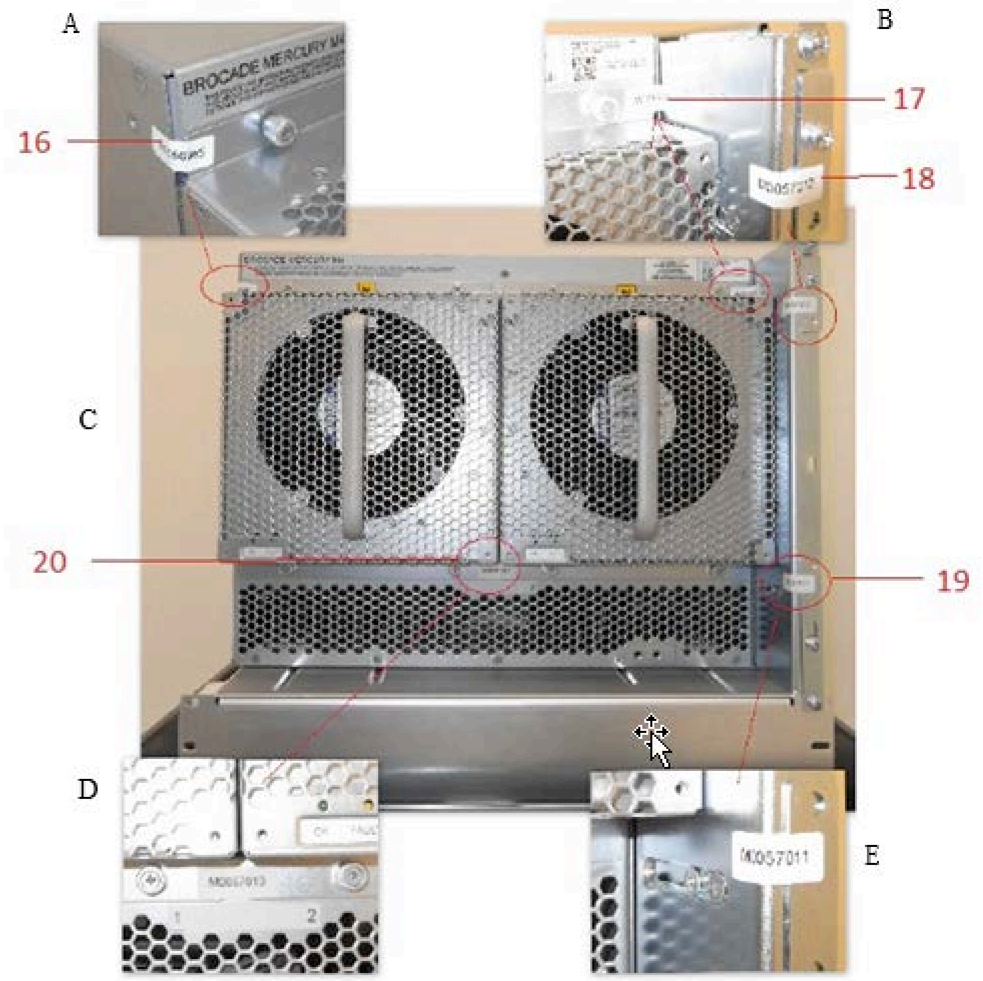

Figure 19 Brocade VDX 8770-4 Non-port side seal locations

1. Apply one (1) seals to each FAN FRU or FAN FRU filler panel installed in the non-port side of the VDX 8770-4. For the FAN FRU on the left the seal wraps from the flange on the FAN FRU or filler around the outside corner of the chassis. For the FAN FRU on the right the seal wraps from the flange on the FAN FRU or filler around the inside corner of the chassis. Two (2) seals are required to complete this step. See Figure 19A, 19B and 19C for details on how to position each seal.
2. Apply one (1) seals that bridges the gap between the FAN FRU positions installed in the non-port side of the VDX 8770-4. One (1) seal is required to complete this step. See Figure 19 for details on how to position each seal.

3. Apply one (1) seal on each FIPS bracket. The upper right FIPS bracket is shown in Figure 19. The lower right FIPS bracket is shown in Figure 19. Two (2) seals are required to complete this step. See Figure 19 for details on how to position each seal.

VDX 8770-4 Air Duct Tamper Evident Seal Application Procedure

Three (3) tamper evident seals are required to complete the physical security requirements illustrated in Figure 20. Relative to the port side of the VDX 8770-4 chassis the air duct is secured to the left side of the chassis.

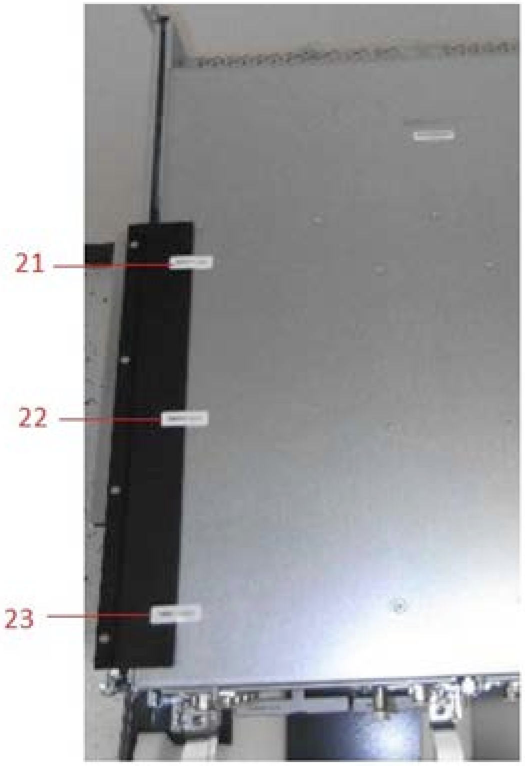

Figure 20 Brocade VDX 8770-4 Air Duct side seal locations

1. Apply thee (3) seals to the rubber flap that touches the top of the VDX 8770-4. Position each seal such that approximately half of each seal adheres to the rubber flap and half of each seal adheres to the top of the chassis. Three (3) seals are required to complete this step. See Figure 20 for details on how to position each seal.

Appendix B: Block Diagram

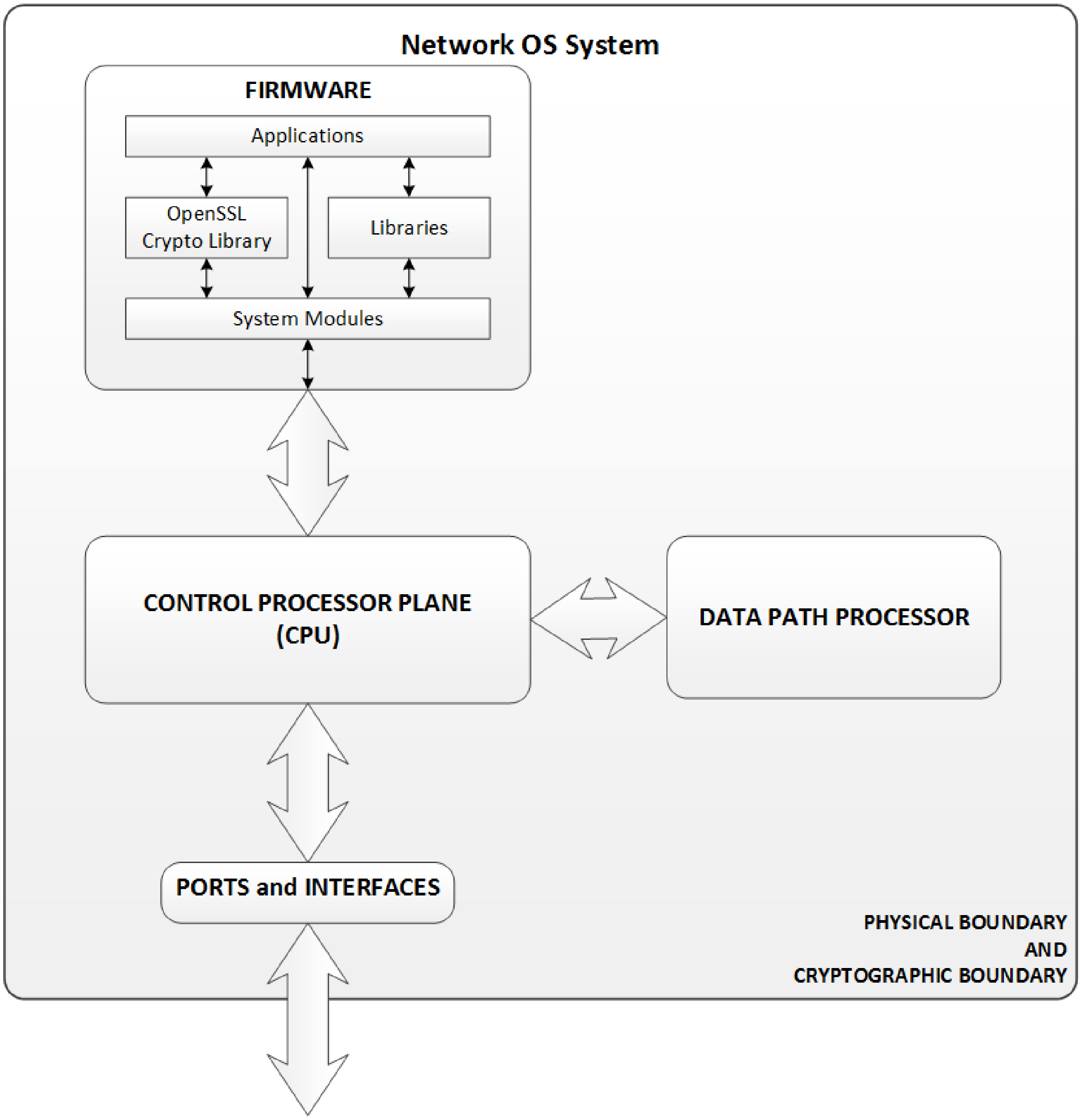

Figure 21 Block Diagram

Appendix C: Critical Security Parameters and Public Keys

The module supports the following CSPs and public keys:

- - SSHv2 and SCP Protocol Keys- - -

1. DH Private Keys (256 bits) for use with 2048 bit modulus
- Description: Used in DHCHAP, and SSHv2 to establish a shared secret
- 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 ANSI X9.31 DRNG; this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Destruction: Session termination and "fips zeroize" command

2. SSHv2/SCP/SFTP Session Keys - 128 and 256 bit AES CBC
- Description: AES encryption key used to secure SSHv2/SCP/SFTP sessions
- 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
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Destruction: Session termination or "fips zeroize" command

3. SSHv2/SCP/SFTP Authentication Key
- Description: Session authentication key used to authenticate and provide integrity of SSHv2 session (HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512)
- 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
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Destruction: Session termination or "fips zeroize" command

4. SSHv2 KDF Internal State
- Description: Used to generate Host encryption and authentication 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
- Storage: RAM in plaintext
- Entry: N/A
- Output: N/A
- Destruction: Session termination or "fips zeroize" command

5. SSHv2 DH Shared Secret Key (2048 bits)
- Description: Shared secret from the DH Key agreement primitive - (K) and (H). Used in SSHv2 KDF to derive (client and server) session keys.
- 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
- Destruction: Session termination or "fips zeroize" command

6. SSHv2 ECDSA Host Private Key (P-256)
- Description: Used to authenticate SSHv2 server to client

- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
- Storage: RAM in plaintext
- Entry: N/A
- Output: N/A
- Destruction: "fips zeroize" command

7. Value of K during SSHv2 256 ECDSA session
- Description: Used to authenticate generate keys that signs and verify
- Generation: ANSI X9.31 RNG, as per FIPS 186-4
- Storage: RAM in plaintext
- Entry: N/A
- Output: N/A
- Destruction: Session termination or “fips zeroize” command

8. SSHv2 ECDH Shared Secret Key (P-256, P-384 and P-521)
- Description: Shared secret from the ECDH Key Agreement primitive. Used in SSHv2 KDF to derive (client and server) session keys.
- Generation: N/A
- Establishment: SSHv2 ECDH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Entry: N/A
- Output: N/A
- Destruction: Session termination or fips zeroize command

9. SSHv2 ECDH Private Key (P-256, P-384 and P-521)
- Description: Private key from the ECDH Key Agreement primitive. Used in SSHv2 KDF to derive (client and server) session keys.
- Generation: N/A
- Establishment: SSHv2 ECDH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Entry: N/A
- Output: N/A
- Destruction: Session termination or fips zeroize command

10. SSHv2 RSA 2048 bit Host Private Key
- Description: Used to authenticate SSHv2 server to client
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
- Storage: RAM in plaintext
- Entry: N/A
- Output: N/A
- Destruction: "fips zeroize" command

- - - - TLS Protocol Keys - - - - - - -

11. TLS Pre-Master Secret
- Description: Secret value used to establish the Session and Authentication key
- Generation: Approved SP800-90A DRBG
- Establishment: RSA key wrapped by the module during TLS session; allowed as per FIPS 140-2 IG D.9
- Storage: Plaintext in RAM
- Entry: N/A
- Output: RSA key wrapped by the module during TLS session
- Destruction: Session termination or "fips zeroize" command

12. TLS Master Secret
- Description: 48 bytes secret value used to establish the Session and Authentication key
- Generation: N/A
- Establishment: TLS KDF as per SP800-135 Section 4.2.1 and 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4

- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Destruction: Session termination or "fips zeroize" command

13. TLS KDF Internal State
- Description: values of the KDF internal state
- Generation: N/A
- Establishment: TLS KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Destruction: Session termination or "fips zeroize" command

14. TLS Session Key - 128, 256 bit AES CBC, Triple-DES 3 key CBC
- Description: TDES or AES key used to secure TLS sessions
- Generation: N/A
- Establishment: TLS KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Destruction: Session termination or "fips zeroize" command

15. TLS Authentication Key for HMAC-SHA-1, HMAC-SHA-256
- Description: HMAC-SHA-1, HMAC-SHA-256 key used to provide data authentication for TLS sessions
- Generation: N/A
- Establishment: TLS KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Destruction: Session termination

- - - RNG Seed CSPs - - -

16. Approved RNG Seed Material
- Description: ANSI X9.31 DRNG seed and seed key
- Generation: Internally generated; raw random data from NDRNG
- Storage: Plaintext in RAM
- Entry: N/A
- Output: N/A
- Destruction: Session termination or "fips zeroize" command

17. ANSI X9.31 DRNG Internal State
- Description: DRNG Internal State
- Generation: ANSI X9.31 DRNG seeded by RNG Seed Material from NDRNG
- Storage: RAM (plaintext)
- Entry: N/A
- Output: N/A
- Destruction: "fips zeroize" command

- - - Operator Authentication/Passwords - - - -

18. Passwords
- Description: Password used to authenticate operators (8 to 40 characters)
- Generation: N/A

- Storage: MD5 digest (plaintext) in Compact Flash
- Entry: Configured by the operator during account maintenance and authentication
- Output: MD5 hashed to associated devices
- Destruction: "fips zeroize" command

19. RADIUS Secret
- Description: Used to authenticate the RADIUS Server (8 to 40 characters)
- Generation: N/A
- Storage: Plaintext in RAM and Compact Flash
- Entry: Configured by an operator during the "aaaconfig - add" command
- Output: CLI through "aaaconfig -show" and "configupload"
- Destruction: "fips zeroize" command

- - - - - - - - - - - - PUBLIC KEYS - - - - - - - - - - - -

1. DH Public Key (2048 bit modulus)
- Description: Used to establish shared secrets (SSHv2 and DHCHAP)
- 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 ANSI X9.31 DRNG; ephemeral public key calculated from the domain parameters and the ephemeral private key (DH Private Key); this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Storage: Plaintext in RAM
- Entry: N/A
- Output: plaintext

2. SSHv2 DH Peer Public Key (2048 bit modulus)
- Description: Used to establish shared secrets (SSHv2 and DHCHAP)
- Generation: N/A
- Storage: Plaintext in RAM
- Entry: plaintext
- Output: N/A

3. DH Keys for FC-SP (2048 bit modulus)
- Description: Used to establish shared secrets (FC-SP)
- 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 ANSI X9.31 DRNG; ephemeral public key calculated from the domain parameters and the ephemeral private key (DH Private Key); this is an allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Storage: Plaintext in RAM
- Entry: N/A
- Output: plaintext

4. TLS v1.0 Peer Public Key (RSA 2048)
- Description: Used by client to encrypt TLS Pre-Master secret
- Generation: N/A
- Storage: Plaintext in RAM
- Entry: Plaintext during TLS handshake protocol
- Output: N/A

6. Firmware Download Public Key (RSA 2048 SHA-256)
- Description: Used to update the FW of the module.
- Generation: N/A Generated outside the module
- Storage: Plaintext in Compact Flash
- Entry: Through firmwarekeyupdate cmd or through FW Update.
- Output: Through firmwarekeyshow cmd.

7. LDAP ROOT CA certificate (RSA 2048)
- Description: Used to authenticate LDAP server
- Generation: N/A
- Storage: Plaintext in Compact Flash

- Entry: Plaintext
- Output: N/A

8. SSHv2 RSA 2048 bit Peer Public Key
-Description: Used to authenticate SSHv2 session
-Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
-Storage: Plaintext in Compact Flash
-Entry: Plaintext
-Output: N/A

9. SSHv2 RSA 2048 bit Host Public Key
-Description: Used to authenticate SSHv2 session
-Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
-Storage: Plaintext in Compact Flash
-Entry: Plaintext
-Output: N/A

10. SSHv2 ECDSA Host Public Key (P-256)
-Description: Used to authenticate SSHv2 session
-Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
-Storage: Plaintext in Compact Flash
-Entry: N/A
-Output: N/A

11. SSHv2 ECDSA Peer Public Key (P-256)
- Description: Used to authenticate SSHv2 server to client
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
- Storage: RAM in plaintext
- Entry: N/A
- Output: Plaintext

12. SSHv2 ECDH Public Key (P-256, P-384 and P-521)
- Description: Shared secret from the ECDH Key Agreement primitive. Used in SSHv2 KDF to derive (client and server) session keys.
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the elliptic curve is the output of the ANSI X9.31 DRNG; ephemeral public key calculated from the domain parameters and the ephemeral private key (SSHv2 ECDH Private Key); this is Approved as per SP800-56A.
- Establishment: SSHv2 ECDH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Entry: N/A
- Output: Plaintext