Brocade VDX 6740, VDX 6740T, VDX 6940 and VDX 8770 Switches

FIPS 140-2 Non-Proprietary Security Policy

Document Version 1.0

Brocade Communications Systems, Inc.

10/10/2016

Revision History

Revision Date	Revision	Summary of Changes
10/10/2016	1.0	Initial Release

This Brocade Communications Systems Security Policy for Brocade VDX 6740, VDX 6740T, VDX 6940 and VDX 8770 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.

Table of Contents

Table of Tables:

Table of Figures

1 Module Overview

The VDX 6740, VDX 6740T, VDX 6940 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 and VDX 6940 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.

Brocade VDX 6740 and 6740T Switches provide the advanced feature set that data centers require while delivering the high performance and low latency virtualized environments demand. They are all Ethernet fabric Top-of-Rack (ToR) switches that support a demanding data center environment. These switches provide 1/10 GbE connections delivering the high performance computing needed to keep up with the demands of a virtualized data center, allowing organizations to reduce network congestion, improve application performance, and meet the capacity required by 1 GbE and 10 GbE servers.

The Brocade VDX 6740 offers forty-eight (48) 10 Gigabit Ethernet (GbE) SFP+ ports and four 40 GbE QSFP+ ports. Each 40 GbE port can be broken out into four independent 10 GbE SFP+ ports, providing an additional sixteen (16) 10 GbE SFP+ ports.

The Brocade VDX 6740T offers 48 10GBASE-T ports and four 40 GbE QSFP+ ports. Each 40 GbE port can be broken out into four independent 10 GbE SFP+ ports, providing an additional 16 10 GbE SFP+ ports.

The Brocade VDX 6740T-1G offers 48 1000BASE-T ports and two 40 GbE QSFP+ ports. Each 40 GbE port can be broken out into four independent 10 GbE SFP+ ports, providing an additional eight 10 GbE SFP+ ports for uplink.

The Brocade VDX 6940-36Q is a fixed 40 Gigabit Ethernet (GbE) optimized switch in a 1U form factor. It offers thirty-six (36) 40 GbE QSFP+ ports and can be deployed as a spine or leaf switch. Each 40 GbE port can be broken out into four independent 10 GbE SFP+ ports, providing a total of one hundred forty-four (144) 10 GbE SFP+. Deployed as a spine, it provides options to connect either 40 GbE or 10 GbE uplinks from leaf switches. By deploying this high-density, compact switch, administrators can reduce their TCO through savings on power, space, and cooling.

The Brocade VDX 6940-144S provides up to twelve (12) 40 GbE quad small form factor pluggable (QSFP) ports and 96 fixed 10 GbE ports for connecting devices in a VCS fabric. The base model of this 2U form factor device contains 64 fixed 10 GbE base ports and no 40 GbE ports. Two 10G Port Upgrade licenses can provide the full complement of 96 fixed 10 GbE ports in two 16 port increments. Two 40G Port Upgrade licenses provide up to twelve (12) 40 GbE ports in two 6 port increments. It can be used as a high-density 10GbE switch for the Top of the Rack (TOR) or Middle of the Row (MOR) or for End of the Row (EOR) configurations.

The Brocade VDX 8770 Switch is a highly scalable, low-latency modular switch, perfectly suited for helping respond to demanding network environments based on booming data usage and cloud computing. Designed to support Brocade VCS networking fabrics, the VDX 8770 supports complex, highly dynamic environments with dense virtualization, extensive automation and high availability requirements.

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, section 11, Appendix A: Tamper Evident Seal Application Procedures.

Note: For more information, please refer to additional Brocade manuals on MyBrocade website. To access them online, go to the MyBrocade website at http://my.brocade.com.

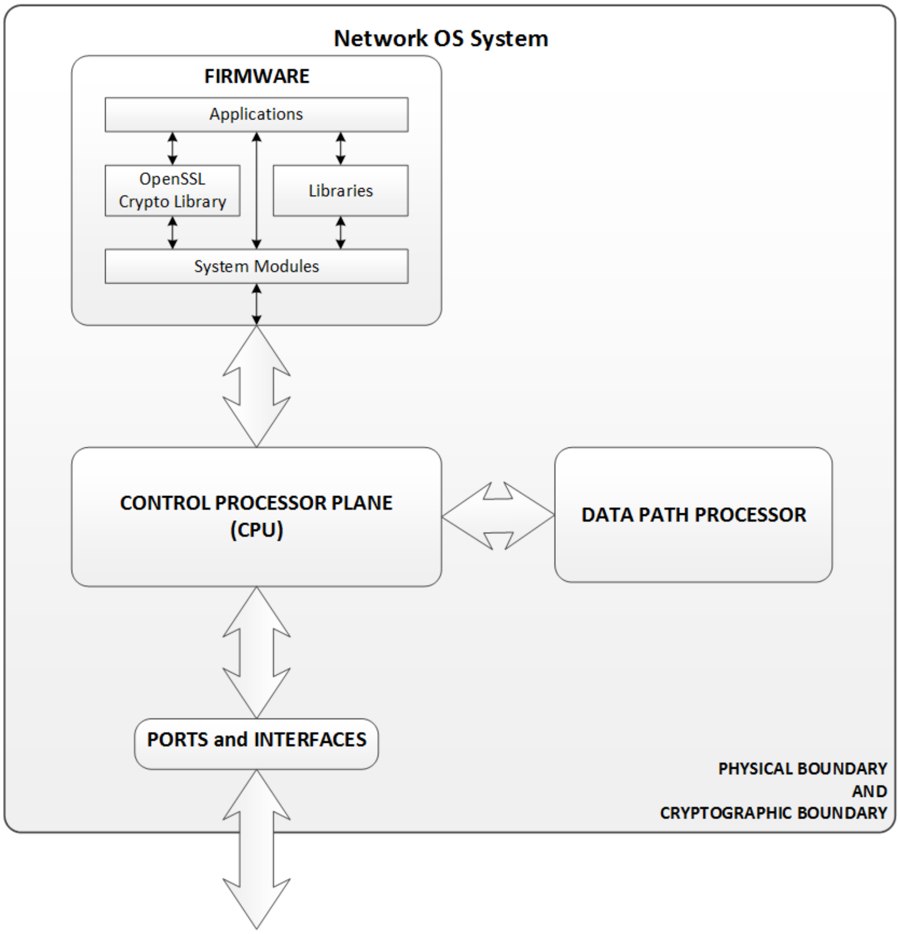
The Crypto-Officer is responsible for storing and controlling the inventory of any unused seals. The unused seals shall be stored in plastic bags in a cool, dry environment between 60° and 70° F (15° to 20° C) and less than 50% relative humidity. Rolls should be stored flat on a slit edge or suspended 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) v6.0.2	63-1001691-01

Figure 1 - Block Diagram



1.1 Brocade VDX 6740

Table 2 - VDX 6740 Configurations

SKU / MFG Part Number	Product Description
SKU: BR-VDX6740-24-F P/N: 80-1007295-01	Brocade VDX 6740 base system with twenty-four 10 Gigabit Ethernet (GbE) SFP+ ports, AC fan/power supply assembly, Non-port side exhaust[1] airflow
SKU: BR-VDX6740-24-R P/N: 80-1007294-01	Brocade VDX 6740 base system with twenty-four 10 Gigabit Ethernet (GbE) SFP+ ports, AC fan/power supply assembly, Port side exhaust[1] airflow
SKU: BR-VDX6740-48-F P/N: 80-1007483-01	Brocade VDX 6740 base system with forty-eight 10 Gigabit Ethernet (GbE) SFP+ SFP+ ports, AC fan/power supply assembly, Non-port side exhaust[1] airflow
SKU: BR-VDX6740-48-R P/N: 80-1007481-01	Brocade VDX 6740 base system with forty-eight 10 Gigabit Ethernet (GbE) SFP+ ports, AC fan/power supply assembly, Port side exhaust[1] airflow
SKU: BR-VDX6740-64-F P/N: 80-1007520-01	Brocade VDX 6740 base system with sixty-four 10 Gigabit Ethernet (GbE) SFP+ ports, AC fan/power supply assembly, Non-port side exhaust[1] airflow
SKU: BR-VDX6740-64-R P/N: 80-1007521-01	Brocade VDX 6740 base system with sixty-four 10 Gigabit Ethernet (GbE) SFP+ ports, AC fan/power supply assembly Port side exhaust[1] airflow
SKU: XBR-000195 P/N: 80-1002006-02	FIPS Kit containing tamper evident labels to be affixed to the module per, section 11, Appendix A: Tamper Evident Seal Application Procedures, in this document. All SKUs listed above utilize this kit to satisfy the physical security requirements

Note for table, above:

1. Port side (-R) and non-port side exhaust (-F) 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.

Figure 2 - VDX 6740-24, VDX 6740-48 and VDX 6740-64

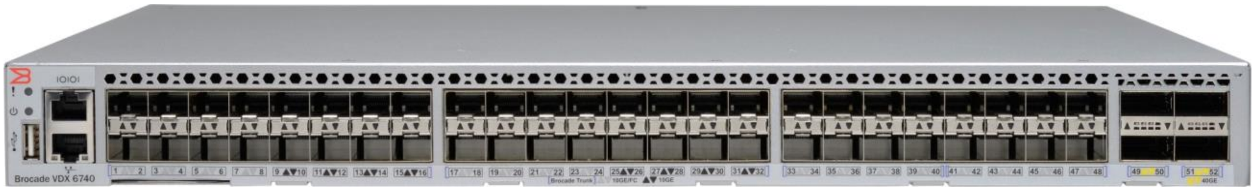


Table 2 lists available configurations for the VDX 6740-24, VDX 6740-48 and VDX 6740-64 SKUs.

1.2 Brocade VDX 6740T

Table 3 - VDX 6740T Configurations

SKU / Part Number	Product Description
SKU: BR-VDX6740T-24-F P/N: 80-1007273-01	Brocade VDX 6740T-64 base system with twenty-four 10 Gigabit Ethernet (GbE) SFP+ ports enabled, AC PSU, Fan, Non-port side exhaust[1] airflow
SKU: BR-VDX6740T-24-R P/N: 80-1007274-01	Brocade VDX 6740T-64 base system with twenty-four 10 Gigabit Ethernet (GbE) SFP+ ports enabled, AC PSU, Fan, Port side exhaust[1] airflow
SKU: BR-VDX6740T-48-F P/N: 80-1007485-01	Brocade VDX 6740T-64 base system with forty-eight 10 Gigabit Ethernet (GbE) SFP+ ports enabled, AC PSU, Fan, Non-port side exhaust[1] airflow
SKU: BR-VDX6740T-48-R P/N: 80-1007487-01	Brocade VDX 6740T-64 base system with forty-eight 10 Gigabit Ethernet (GbE) SFP+ ports enabled, (10GB-T ports; no optics), AC PSU, Fan, Port side exhaust[1] airflow
SKU: BR-VDX6740T-64-F P/N: 80-1007522-01	Brocade VDX6740T-64 base system with sixty-four 10 Gigabit Ethernet (GbE) SFP+ ports enabled, AC PSU, Fan, Non-port side exhaust[1] airflow
SKU: BR-VDX6740T-64-R P/N: 80-1007523-01	Brocade VDX6740T-64 base system with sixty-four 10 Gigabit Ethernet (GbE) SFP+ ports enabled, AC PSU, Fan, Port side exhaust[1] airflow
SKU: BR-VDX6740T-56-1G-R P/N: 80-1007863-03	Brocade VDX 6740T-1G system with forty-eight 1000BASE-T ports and two 40 Gigabit Ethernet ports (to operate effectively as fifty-six 1000BASE-T) ports enabled, AC PSU, Fan, port-side exhaust[1] airflow
SKU: BR-VDX6740T-56-1G-F P/N: 80-1007864-03	Brocade VDX 6740T-1G system with forty-eight 1000BASE-T ports and two 40 Gigabit Ethernet ports (to operate effectively as fifty-six 1000BASE-T) ports enabled, AC PSU, Fan, non-port side exhaust[1] airflow
SKU: XBR-000195 P/N: 80-1002006-02	FIPS Kit containing tamper evident labels to be affixed to the module per section 11, Appendix A: Tamper Evident Seal Application Procedures, in this document. All SKUs listed above utilize this kit to satisfy the physical security requirements

Note for table, above:

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.

Figure 3 - VDX 6740T-24, VDX 6740T-48 and VDX 6740T-64

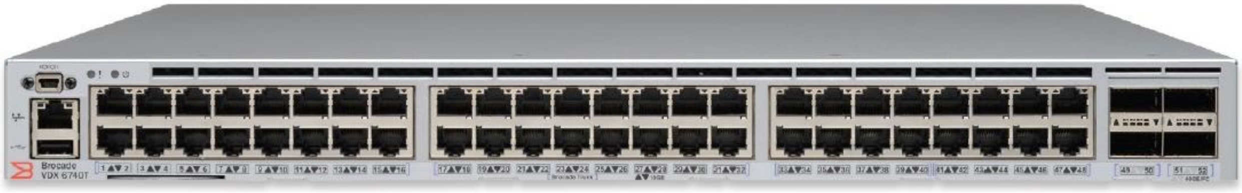


Figure 4 - VDX 6740T-56-1G

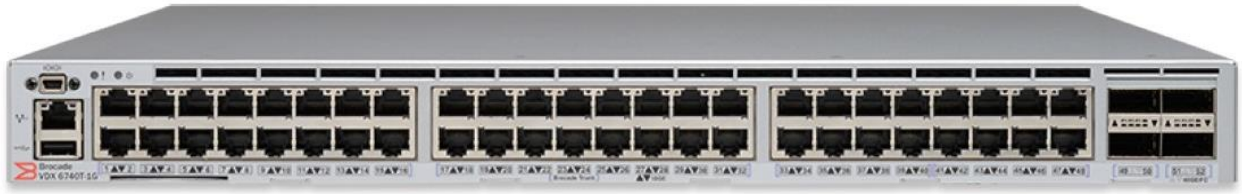


Table 3 lists the validated configurations for the VDX 6740T-24, VDX 6740T-48 and VDX 6740T-64.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

1.3 Brocade VDX 6940

Table 4 - VDX 6940 Configurations

SKU / Part Number	Description
SKU: BR-VDX6940-24Q-AC-F P/N: 80-1008854-01	Brocade VDX 6940-36Q base system with twenty-four 40 Gigabit Ethernet (GbE) QSFP+ ports enabled, AC power supply, Fan, non-port side exhaust[1] airflow
SKU: BR-VDX6940-24Q-AC-R P/N: 80-1008855-01	Brocade VDX 6940-36Q base system with twenty-four 40 Gigabit Ethernet (GbE) QSFP+ ports enabled, AC power supply, Fan, port side exhaust[1] airflow
SKU: BR-VDX6940-36Q-AC-F P/N: 80-1008851-01	Brocade VDX 6940-36Q base system with thirty-six 40 Gigabit Ethernet (GbE) QSFP+ ports enabled, AC power supply, Fan, non-port side exhaust[1] airflow
SKU: BR-VDX6940-36Q-AC-R P/N: 80-1008850-01	Brocade VDX 6940-36Q base system with thirty-six 40 Gigabit Ethernet (GbE) QSFP+ ports enabled, AC power supply, Fan, port side exhaust[1] airflow
SKU: BR-VDX6940-64S-AC-F P/N: 80-1008529-01	Brocade VDX 6940-144S base system with sixty-four 1/10 Gigabit Ethernet (GbE) SFP/SFP+ ports enabled, AC power supply, Fan, non-port-side exhaust[1] airflow
SKU: BR-VDX6940-64S-AC-R P/N: 80-1008526-01	Brocade VDX 6940-144S base system with sixty-four 1/10 Gigabit Ethernet (GbE) SFP/SFP+ ports enabled, AC power supply, Fan, port side exhaust[1] airflow
SKU: BR-VDX6940-96S-AC-F P/N: 80-1008530-01	Brocade VDX 6940-144S base system with ninety-six 1/10 Gigabit Ethernet (GbE) SFP/SFP+ ports enabled, AC power supply, Fan, non-port side exhaust[1] airflow
SKU: BR-VDX6940-96S-AC-R P/N: 80-1008527-01	Brocade VDX 6940-144S base system with ninety-six 1/10 Gigabit Ethernet (GbE) SFP/SFP+ ports enabled, AC power supply, Fan, port side exhaust[1] airflow
SKU: BR-VDX6940-144S-AC-F P/N: 80-1008531-01	Brocade VDX 6940-144S base system with following enabled port count capability: - One-hundred forty-four 10 Gigabit Ethernet (GbE) QSFP+ ports using breakout cables, or - Ninety-six fixed 10 Gigabit Ethernet (GbE) QSFP+ ports and additional forty-eight 10 GbE QSFP+ ports with breakout cables AC power supply, Fan, non-port side exhaust[1] airflow

SKU / Part Number	Description
SKU: BR-VDX6940-144S-AC-R P/N: 80-1008528-01	Brocade VDX 6940-144S base system following enabled port count capability: - One-hundred forty-four 10 Gigabit Ethernet (GbE) QSFP+ ports using breakout cables, or - Ninety-six fixed 10 Gigabit Ethernet (GbE) QSFP+ ports and additional forty-eight 10 GbE QSFP+ ports with breakout cables AC power supply, Fan, port side exhaust[1] airflow
SKU: XBR-000195 P/N: 80-1002006-02	FIPS Kit containing tamper evident labels to be affixed to the module per section 11, Appendix A: Tamper Evident Seal Application Procedures, in this document. All SKUs listed above utilize this kit to satisfy the physical security requirements

Note for table, above:

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.

Figure 5 - VDX6940-24Q and VDX 6940-36Q

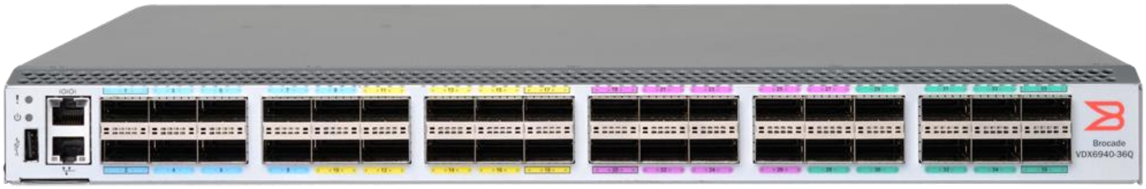


Figure 6 – VDX 6940-64S, VDX 6940-96S and VDX 6940-144S

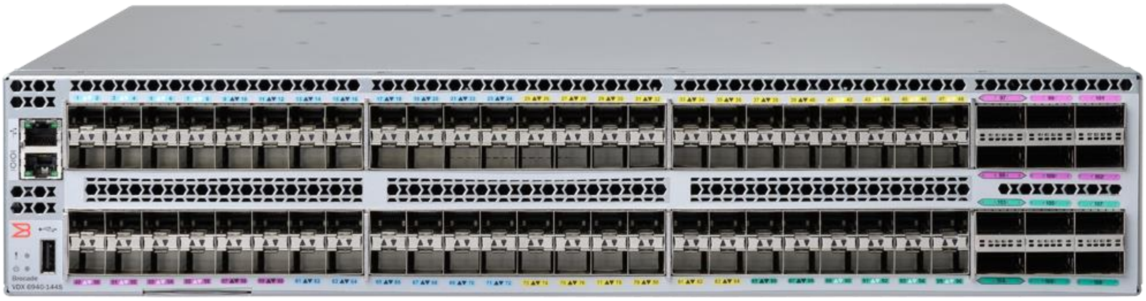


Table 4 lists the configurations for VDX 6940 family of products.

Figures, above, illustrate the cryptographic module configurations.

Next page →

1.4 Brocade VDX 8770

Table 5 - VDX 8770 Part Numbers

SKU / Part Number	Product Description
SKU: BR-VDX8770-4-BND-AC P/N: 80-1005850-02	VDX 8770-4 I/O Slot chassis with three (3) Switch Fabric Modules (BR-VDX8770-SFM-1), one (1) Management Module (BR-VDX8770-MM-1), two (2) exhaust Fan and two (2) 3000W AC Power supply unit Additional Management modules to be ordered separately. Power cord ordered separately
SKU: BR-VDX8770-4-BND-DC P/N: 80-1006532-03	VDX 8770-4 I/O Slot chassis with three (3) Switch Fabric Modules (BR-VDX8770-SFM-1), one (1) Management Module (BR-VDX8770-MM-1), two (2) exhaust Fan and two (2) 3000W DC Power supply unit. Additional Management modules to be ordered separately. Power cord ordered separately
SKU: BR-VDX8770-8-BND-AC P/N: 80-1005905-02	VDX 8770-8 I/O Slot chassis with six (6) Switch Fabric Modules (BR-VDX8770-SFM-1), one (1) Management Module (BR-VDX8770-MM-1), four (4) exhaust Fan and three (3) 3000W AC Power supply unit. Additional Management modules to be ordered separately. Power cord ordered separately.
SKU: BR-VDX8770-8-BND-DC P/N: 80-1006533-03	VDX 8770-8 I/O Slot chassis with six (6) Switch Fabric Modules (BR-VDX8770-SFM-1), one (1) Management Module (BR-VDX8770-MM-1), four (4) exhaust Fan and three (3) 3000W DC Power supply unit. Additional Management modules to be ordered separately. Power cord ordered separately.
SKU: XBR-000195 P/N: 80-1002006-02	FIPS Kit containing tamper evident labels to be affixed to the module per, section 11, Appendix A: Tamper Evident Seal Application Procedures, in this document. All SKUs listed above utilize this kit to satisfy the physical security requirements

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

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 6 - Components for the VDX 8770

SKU / Part Number	Description
SKU: XBR-BLNK-PSU P/N: 80-1006430-01	Field Replaceable Unit - Blank Panel for Power Supply Unit (PSU) Slots
SKU: BR-VDX8770-SFM-1 P/N: 80-1006295-01	Field Replaceable Unit - Switch Fabric Module (SFM)
SKU: BR-VDX8770-MM-1 P/N: 80-1006294-02	Field Replaceable Unit - Management Module (MM)
SKU: BR-VDX8770-12X40G-QSFP-1 P/N: 80-1006293-02	Field Replaceable Unit – twelve (12) 40GE QSFP Line Card. No Optics
SKU: BR-VDX8770-48X10G-SFPP-1 P/N: 80-1006048-02	Field Replaceable Unit – eighty-four (48) 1/10G SFP+ Line Card, No Optics
SKU XBR-BLNK-FULL P/N 80-1006431-01	Field Replaceable Unit - Filler Panel for Line Card Slot
SKU XBR-BLNK-HALF P/N 80-1006429-01	Field Replaceable Unit - Half-Slot Filler Panel for Switch Fabric Module Slot or Management Module Slot

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

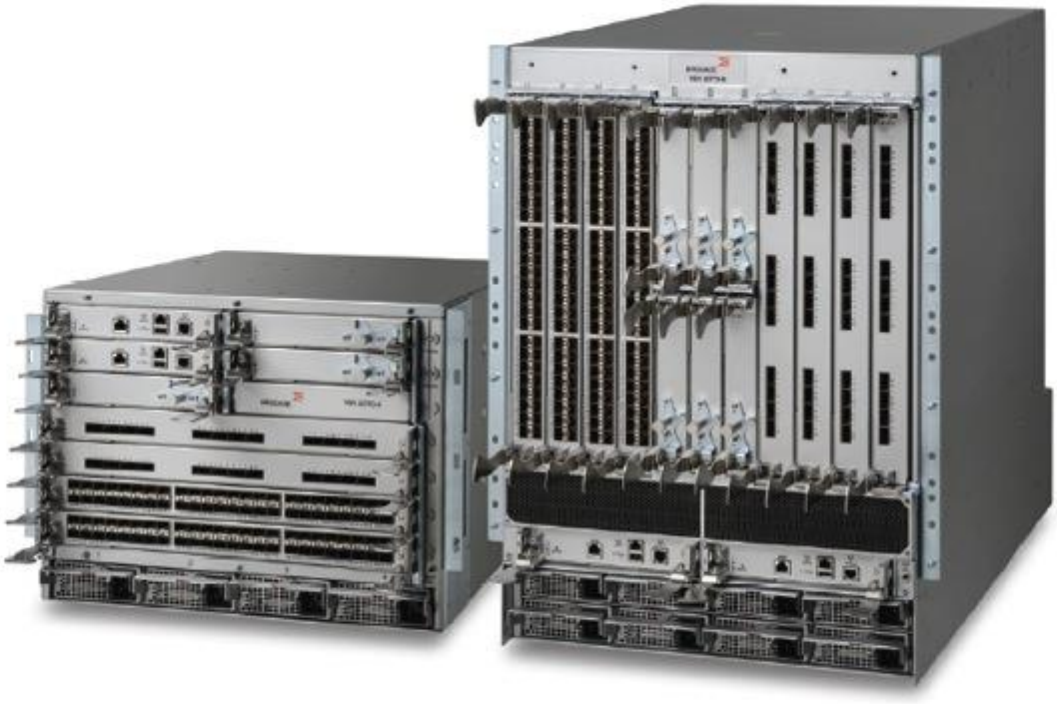
Table 7 - VDX 8770 Validated Configurations

Approved Configuration Variations	Product Description
VDX 8770-4 (AC Power)	VDX 8770-4 I/O Slot chassis (BR-VDX8770-4-BND-AC) containing: three (3) Switch Fabric Modules (BR-VDX8770-SFM-1), one (1) Management Module (BR-VDX8770-MM-1), two (2) exhaust Fan and two (2) 3000W AC Power supply unit. Additional components from Table 6 above may be added.
VDX 8770-4 (DC Power)	VDX 8770-4 I/O Slot chassis (BR-VDX8770-4-BND-DC) containing: three (3) Switch Fabric Modules (BR-VDX8770-SFM-1), one (1) Management Module (BR-VDX8770-MM-1), two (2) exhaust Fan and two (2) 3000W DC Power supply unit. Additional components from Table 6 above may be added.
VDX 8770-8 (AC Power)	VDX 8770-8 I/O Slot chassis (BR-VDX8770-8-BND-AC) containing: six (6) Switch Fabric Modules (BR-VDX8770-SFM-1), one (1) Management Modules (BR-VDX8770-MM-1), four (4) exhaust Fan and three (3) 3000W AC Power supply unit. Additional Management Module (BR-VDX8770-MM-1) shall be inserted for this configuration. Additional components from Table 6 above may be added.
VDX 8770-8 (DC Power)	VDX 8770-8 I/O Slot chassis (BR-VDX8770-8-BND-DC) containing six (6) Switch Fabric Modules (BR-VDX8770-SFM-1), one (1) Management Modules (BR-VDX8770-MM-1), four (4) exhaust Fan and three (3) 3000W DC Power supply unit. Additional Management Module (BR-VDX8770-MM-1) shall be inserted for this configuration. Additional components from Table 6 above may be added.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

Figure 7 - VDX 8770-4 and VDX 8770-8



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 6 - Components for the VDX 8770. There are no filler panels for the fans since all fans must be installed on the chassis.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

2 Security Level Definitions

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

Table 8 - 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

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

3 Modes of Operation

Module supports an Approved mode of operation and a non-Approved mode of operation. The initial state of the cryptographic module is the non-Approved mode of operation. The Crypto-Officer shall follow the procedures in section 3.1, FIPS Approved mode of operation, to initialize the module into the Approved mode of operation. The module cannot be configured into the non-Approved mode once the initialization procedures have been completed by the Crypto-Officer.

3.1 FIPS Approved mode of operation

The cryptographic module supports the following Approved algorithms in firmware

Table 9 - FIPS Approved Cryptographic Functions

Label	Cryptographic Function	Certificate Number
AES	Advanced Encryption Algorithm Modes: CBC Sizes: 128, 256 [NOTE: AES-192 is not used or called by any service in FIPS mode. ECB and CTR Modes are not used or called by any service in FIPS mode]	3544
Triple-DES	Triple Data Encryption Algorithm Modes: Three-key CBC	1985
SHS	Secure Hash Algorithm Message Digests: SHA-1, SHA-256, SHA-512 [NOTE: SHA-224 and SHA-384 are not used or called by any service in FIPS mode]	2924
HMAC	Keyed-Hash Message Authentication code MACs: HMAC-SHA-1 (112-bit key), HMAC-SHA-256, HMAC-SHA-512 [NOTE: HMAC-SHA-224 and HMAC-SHA-384 are not used or called by any service in FIPS mode]	2264
RSA	Rivest Shamir Adleman Signature Algorithm FIPS 186-4 Key Generation: RSA 2048-bit RSASSA-PKCS1_V1_5 Signature Generation and Signature Verification: RSA 2048-bit with SHA-256 [NOTE: RSA 1024-bit and RSA 3072-bit is not used or called by any service in FIPS Mode]	1826

Label	Cryptographic Function	Certificate Number
ECDSA	Elliptic Curve Digital Signature Algorithm FIPS 186-4 PKG: P-256 FIPS 186-4 PKV: P-256 FIPS 186-4 SigVer: P-256 with SHA-256 [NOTE: P-384 and P-521 curves are not used or called by any service in FIPS Mode]	722
DRBG	SP800-90A Deterministic Random Bit Generator Mode: AES-256 CTR_DRBG (Prediction Resistance Enabled)	901
CVL	SP800-135 KDF (TLS v1.0/1.1 and v1.2)**	601
CVL	SP800-135 KDF (SSHv2)**	601
CVL	SP800-56A ECC CDH Primitive Curves: P-256, P-384, P-521	600

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
- SNMPv3 (WARNING: blocked during configuration of the module into FIPS 140-2 mode as per section 3.1; the protocol SNMPv3 “shall not” be used when operated in FIPS 140-2 mode; any keys derived via SNMPv3 “shall” not be used in FIPS 140-2 mode; the use of SNMPv3 is an explicit violation of this Security Policy; any such use of SNMPv3 deems the cryptographic module completely unfit for service to protect sensitive unclassified data in perpetuity)

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)
- EC Diffie-Hellman (CVL Cert. #600, key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength)
- HMAC-MD5 – Used to support RADIUS for operator authentication only (HMAC-MD5 is not exposed to the operator)
- MD5 – Used in the TLS v1.0 KDF in FIPS mode as per SP800-135 (MD5 is not exposed to the operator)
- MD5 – Used for password hash (Note: The use of MD5 does not provide cryptographic protection, and Is considered as plaintext)
- Non-deterministic random number generator for seeding SP800-90A DRBG

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

1. Crypto-Officer must Apply tamper labels as specified in Security Policy, section 11, Appendix A: Tamper Evident Seal Application Procedures

NOTE: The tamper evident seals shall be installed for the module to operate in a FIPS Approved mode of operation.

2. Login to the switch as Crypto-Officer
3. Enable **fips selftests** using the following commands:
   sw0#unhide fips
   sw0#fips selftests
4. Enter **fips zeroize** command to zeroize all the existing security configurations and parameters:
   sw0#fips zeroize

5. After the module successfully reboots and performs all Power-Up Self-tests successfully, login as Crypto-Officer to configure the system into a FIPS 140-2 Approved mode of Operation.
6. Enter the **cipherset ldap** command to configure TLS 1.0 and TLS 1.2 ciphers for LDAP authentication:
   sw0#cipherset ldap
7. Enter the **cipherset radius** command to configure TLS 1.0 and TLS 1.2 ciphers for RADIUS authentication:
   sw0#cipherset radius
8. Enter the **cipherset ssh sha256** command to configure SHA2 hash value for SSH server:
   sw0#cipherset ssh sha256

9. Enter the local rbridge-id specific configuration mode
   sw0(config)# rbridge-id-1

10. Enter the **ssh server key-exchange** command to configure SSH server key exchange protocol:
    sw0(config-rbridge-id-1)# ssh server key-exchange ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256

11. Enter the **ssh client key-exchange** command to configure SSH client key exchange protocol:
    sw0(config-rbridge-id-1)# ssh client key-exchange ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256

12. Enter the **ssh server cipher** command to configure SSH server ciphers:
    sw0(config-rbridge-id-1)# ssh server cipher aes128-cbc,aes256-cbc

13. Enter the **ssh client cipher** command to configure SSH client ciphers:
    sw0(config-rbridge-id-1)# ssh client cipher aes128-cbc,aes256-cbc

14. Enter the **ssh server mac** command to configure SSH server MACs:
    sw0(config-rbridge-id-1)# ssh server mac hmac-sha1,hmac-sha2-256,hmac-sha2-512

15. Enter the **ssh client mac** command to configure SSH client MACs:
    sw0(config-rbridge-id-1)# ssh client mac hmac-sha1,hmac-sha2-256,hmac-sha2-512

16. Enter the following commands to restart the SSH server, for the configured algorithms to take effect:
    sw0(config-rbridge-id-1)# ssh server shutdown
    sw0(config-rbridge-id-1)# no ssh server shutdown

17. Use IP ACLs to block Telnet, HTTP, HTTPS, SNMP and Brocade internal ports 7110, 7710, 8008, 9110, and 9710 for IPv4 and IPv6. If SSH access is required, enter **seq permit** commands to allow access on port 22. If remote access is required, such as through SCP or LDAP, enter **seq permit** commands to allow UDP and TCP traffic on ports 1024 through 65535.

    Configure IP ACLs using **ip access-list** command and use **ip access-group** command to apply the rules to the management interface:

    ```
    device(config)# ip access-list extended <User defined name (i.e.FIPS-ACL4)>
    device(config-ip-ext)# seq 1 deny tcp any any eq 23
    device(config-ip-ext)#seq 2 deny tcp any any eq 80
    device(config-ip-ext)#seq 3 deny tcp any any eq 443
    device(config-ip-ext)#seq 4 deny tcp any any eq 7110
    device(config-ip-ext)#seq 5 deny tcp any any eq 7710
    device(config-ip-ext)#seq 6 deny tcp any any eq 8008
    device(config-ip-ext)#seq 7 deny tcp any any eq 9110
    device(config-ip-ext)#seq 8 deny tcp any any eq 9710
    device(config-ip-ext)#seq 9 deny udp any any eq 161
    device(config-ip-ext)#seq 10 permit udp any any eq 123
    device(config-ip-ext)#seq 11 permit tcp any any range 1024 65535
    device(config-ip-ext)#seq 12 permit udp any any range 1024 65535
    device(config-ip-ext)#seq 13 permit tcp any any eq 22
    device(config-ip-ext)#seq 14 permit tcp any any eq 830

    device(config-ip-ext)#exit
    device(config)# interface tengigabitethernetManagement  <ID for Management Interface (i.e.
    1/0/49)>
    device(conf-if-fo-1/0/49)# ip access-group <User defined name (i.e.FIPS-ACL4)> in

    device(config)# ipv6 access-list extended <User defined name (i.e.FIPS-ACL6)>
    device(config-ip-ext)# seq 1 deny tcp any any eq 23
    device(config-ip-ext)#seq 2 deny tcp any any eq 80
    device(config-ip-ext)#seq 3 deny tcp any any eq 443
    device(config-ip-ext)#seq 4 deny tcp any any eq 7110
    device(config-ip-ext)#seq 5 deny tcp any any eq 7710
    device(config-ip-ext)#seq 6 deny tcp any any eq 8008
    device(config-ip-ext)#seq 7 deny tcp any any eq 9110
    device(config-ip-ext)#seq 8 deny tcp any any eq 9710
    device(config-ip-ext)#seq 9 deny udp any any eq 161
    device(config-ip-ext)#seq 10 permit udp any any eq 123
    device(config-ip-ext)#seq 11 permit tcp any any range 1024 65535
    device(config-ip-ext)#seq 12 permit udp any any range 1024 65535
    device(config-ip-ext)#seq 13 permit tcp any any eq 22
    device(config-ip-ext)#seq 14 permit tcp any any eq 830

    device(config-ip-ext)#exit
    device(config)# interface tengigabitethernetManagement  <ID for Management Interface (i.e.
    1/0/49)>
    device(conf-if-fo-1/0/49)# ipv6 access-group <User defined name (i.e.FIPS-ACL6)>  in
    ```

    NOTE
    Do not use FTP mode for the operations such as copying startup or running configuration, copy support, and firmware download.

    NOTE
    Do not configure TACACS+ protocol for authentication.

18. Enter the following command to remove any tacacs+ server configuration

    ```
    sw0(config)# no tacacs-server <host>
    ```

19. Depending on the desired AAA Authentication method, perform one of the steps below:

    I. Authentication mode is configured to local authentication by default.

    II. Configure PEAP MS-CHAP V2 for RADIUS authentication:

    a) Enter the **radius-server host** ip-address **protocol peap-mschap** [**port** portnum] [**key** shared-key] [**timeout** secs] [**retransmit** num] command in global configuration mode to configure RADIUS server:

    ```
    device(config)# radius-server host 10.24.65.6 protocol peap-mschap key sharedsecret
    ```

    b) Enter the **aaa authentication login radius local-auth-fallback** command:

    ```
    device(config)# aaa authentication login radius local-auth-fallback.
    ```

    Note: The RADIUS protocol relies on the strength of TLSv1.0 and TLSv1.2.

    III. Configure LDAP authentication:

    a) Enter the **certutil import ldapca directory** *ca-certificate-directory* **file** *filename* **protocol SCP host** *remote-ip* **user** *user-account* **password** *password* command in privileged EXEC mode to import LDAP CA certificate:

    ```
    device# certutil import ldapca directory /usr/ldapcacert file cacert.pem protocol SCP host 10.23.24.56 user admin password *****
    ```

    The CA certificate imported must be RSA2048 with SHA256 encryption.

    b) Enter the **ldap-server host** *ip-address* **basedn** *domain-name* [**port** portnum] [**retransmit** *num*] command in global configuration mode to configure the LDAP server.

    ```
    device(config)# ldap-server host padl12r2.la12security.xyz.com basedn la12security.xyz.com.
    ```

    c) Enter the **ip dns** command to configure the DNS domain and server.

    ```
    device(config)# ip dns domain-name la12security.xyz.com
    device(config)# ip dns name-server 10.38.37.183
    ```

    d) Enter the **aaa authentication login ldap local-auth-fallback** command.

    ```
    device(config)# aaa authentication login ldap local-auth-fallback.
    ```

20. If required to set up a syslog server, follow the steps below to enable secure logging:

    a) Enter the **certutil import syslogca directory** *ca-certificate-directory* **file** *filename* **protocol SCP host** *remote-ip* **user** *user-account* **password** *password* command in privileged EXEC mode to import Syslog CA certificate.

    ```
    device# certutil import syslogca directory /usr/syslogcacert file cacert.pem protocol SCP host 10.23.24.56 user admin password *****.
    ```

    The CA certificate imported must be RSA2048 with SHA256 encryption.

    b) Enter the **logging syslog-server host** *ip-address* **use-vrf** *vrf-name* **secure** command in global configuration mode to configure the Syslog server.

21. Enter the **certutil import sshkey directory** *pubkey-directory* **file** *filename* **protocol SCP host** *remote-ip* **login** *login-id* **password** *password* **user** user-account command in privileged EXEC mode to import SSH public key, if required:

    ```
    device# certutil import sshkey directory /usr/sshkeys file id_rsa.pub protocol SCP host 10.23.24.56 user admin login remoteuser password *****.
    ```

To support passwordless SSH authentication, externally generated RSA key pairs must be RSA2048 only.

22. Configure ntp server using commands in global configuration mode, if required:

    a) Enter the **ntp authentication key** *key-id* **sha1** *key-string* to configure NTP authentication key of type SHA1.

    ```
    device(config)# ntp authentication key 1 sha1 ntpsecret
    ```

    b)Enter the **ntp server** *ip-address* **key** *key-id* **secure** command to configure the Syslog server.

    ```
    device(config)# ntp server 10.20.8.1 key 1
    ```

23. Configure VDX 6740 and VDX 6740T to disable AG mode using the following command in local rbridge-id specific configuration mode.

    ```
    device(config-rbridge-id-1)# ag
    device(config-rbridge-id-1-ag)# no enable
    ```

24. Vcenter, dot1x(802.1x) and OSPF features are not FIPS compliant.

    a) If dot1x is enabled, execute the following CLI in config mode to disable dot1x globally:

    ```
    no dot1x enable
    ```

    b)If vcenter is configured, remove the configuration using the following CLI:

    ```
    no vcenter<name>
    ```

25. Passwords of the default accounts (admin and user) must be changed to maintain FIPS 140-2 compliance:

    ```
    sw0#username admin password <enter password>
    sw0#username user password <enter password>
    ```

26. Disable telnet service with the following command:

    ```
    sw0(config-rbridge-id-1)#telnet server shutdown
    ```

27. Disable boot prom access using the following commands:

    ```
    sw0#unhide fips
    sw0#prom-access disable
    ```

28. Enter the **copy running-config startup-config** to save all the settings to the startup configuration file.

    ```
    sw0#copy running-config startup-config
    ```

By following the procedures above, the following will be configured:

TLS 1.2 Ciphers:

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS 1.0 Ciphers:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Note: For more information, please refer to additional Brocade manuals on MyBrocade website. To access them online, go to the MyBrocade website at http://my.brocade.com.

3.2 Non-Approved Mode of Operation

In non-Approved mode, an operator will have no access to CSPs used within the Approved mode. When switching from the non-Approved mode of operation to the Approved-mode, the operator is required to perform zeroization of the module's plaintext CSPs as indicated in the procedure in section 3.1, above.

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 10 - Non-FIPS 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); BLOWFISH; BLOWFISH-CBC; BLOWFISH-CFB; BLOWFISH-ECB; BLOWFISH-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; DES-EDE3; DES-EDE3-CFB; DES-EDE3-OFB; DES-OFB; DES3; DESX;
		RC2; RC2-40- CBC; RC2-64-CBC; RC2-CBC; RC2-CFB; RC2-ECB; RC2-OFB; RC4; RC4-40

Message Digests for SSL and TLS	Crypto-Officer	SHA-384 (non-compliant); SHA-512 (non-compliant); MD2; MD4; MD5; RMD160
Message authentication algorithms and ciphers for configuring SSH	Crypto-Officer	Ciphers: AES-128-CTR (non-compliant); AES-192-CTR (non-compliant); AES-256-CTR (non-compliant); AES-128-GCM (non-compliant); AES-192-GCM (non-compliant); AES-256-GCM (non-compliant); Triple-DES-CBC (non-compliant); AES-192-CBC (non-compliant); ARCFOUR128; ARCFOUR256; BLOWFISH-CBC; CAST128-CBC Macs: HMAC-MD5; UMAC-64; HMAC-RIPEMD160; HMAC-SHA-1-96 (non-compliant); HMAC-MD5-96 Curves: DIFFIE-HELLMAN-GROUP-EXCHANGE-SHA-1; DIFFIE-HELLMAN-GROUP14-SHA-1; DIFFIE-HELLMAN-GROUP1-SHA-1

Crypto Function/Service	*User Role Change*	*Additional Details*
SNMP	Crypto-Officer	Simple Network Management Protocol. SNMPv1 (Plaintext; no cryptography), SNMPv2c and SNMPv3 in noAuthNoPriv, authNoPriv mode SNMPv3 in authPriv mode MD5 Modes: Not Applicable Key sizes: Not Applicable DES Modes: CBC Key sizes: 56-bits AES (non-compliant) Modes: CFB (non-compliant) Key sizes: 128-bits SHA-1 (non-compliant) Modes: Not Applicable Key sizes: Not Applicable SP800-135 SNMPv3 KDF (non-compliant) Modes: Not Applicable Key sizes: Not Applicable
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	Crypto-Officer	N/A – No algorithms (plaintext)
FTP	Crypto-Officer	Config Upload; Config Download; Support Save; FW Download, autoftp
FCSP	Crypto-Officer	DHCHAP with Diffie-Hellman Group 0-4 Diffie-Hellman key sizes supported: 00 - DH Null option 01 - 1024 bit key 02 - 1280 bit key 03 - 1536 bit key 04 - 2048 bit key Hashes supported: MD5; SHA-1 (non-compliant)
RSA	Crypto-Officer	RSA key size 1024 bits for SSH and TLS
Diffie-Hellman	Crypto-Officer	DH key size 1024 bits for SSH

4 Ports and Interfaces

Each module provides Networking ports, USB ports, Management Ethernet port, Serial port, Power Supply connectors and LEDs. This section describes the physical ports and the interfaces they provide for Data input, Data output, Control input, and Status output.

Table 11 below shows the correspondence between the physical interfaces of the modules and logical interfaces defined in FIPS 140-2.

Table 11 - Physical/Logical Interface Correspondence

Physical Interface	Logical Interface
Networking ports	Data input
USB port	
Networking ports	Data output
USB port	
Management Ethernet port	Control input
Networking ports	
Serial port	
Management Ethernet port	Status output
Serial port	
Networking ports	
USB port	
LED	
Power Supply connector(s)	Power

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

4.1 Brocade VDX 6740 & Brocade VDX 6740T

The “Brocade VDX 6740” column in Table 12 applies to the following SKUs:

- VDX 6740-24-F, VDX 6740-24-R, VDX 6740-48-F, VDX 6740-48-R, VDX 6740-64-F and VDX 6740-64-R

The “Brocade VDX 6740T” column in Table 12 applies to the following SKUs:

- VDX 6740T-24-F, VDX 6740T-24-R, VDX 6740T-48-F, VDX 6740T-48-R, VDX 6740T-64-F, VDX 6740T-64-R, VDX6740T-56-1G-R and VDX6740T-56-1G-F

Table 12 – Physical Interface Descriptions for VDX 6740 and VDX 6740T.

Physical Interface	Brocade VDX 6740	Brocade VDX 6740T
Networking ports	(QTY. 48) 1x10 GbE SFP+ ports (QTY. 4) 40 GbE QSFP ports	(QTY.48) 10 GbE BaseT ports (QTY. 4) 40 GbE QSFP ports
Management Ethernet port	(QTY. 1) RJ-45 10/100/1000 Ethernet out-of-band management port	(QTY. 1) RJ-45 10/100/1000 Ethernet out-of-band management port
Serial port	(QTY. 1) RJ-45 used for console	(QTY. 1) RJ-45 used for console
USB port	(QTY. 1) Used for data and firmware downloads with Brocade USB flash device	(QTY. 1) Used for data and firmware downloads with Brocade USB flash device
LED	(QTY. 1) System Power LED (QTY. 1) System Status LED (QTY. 2) Power Supply and Fan LEDs - on non-port side (One LED per Power Supply and Fan assembly) (QTY. 48) port LEDs	(QTY. 1) System Power LED (QTY. 1) System Status LED (QTY. 2) Power Supply LEDs - on non-port side (One LED per Power Supply) (QTY. 5) Fan LEDs - on non-port side (One LED per Fan) (QTY. 48) port LEDs
Power Supply connector(s)	(QTY. 2) Power connectors	(QTY. 2) Power connectors

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

4.2 Brocade VDX 6940

The “Brocade VDX 6940-36Q” column in Table 13 applies to the following SKUs:

- BR-VDX6940-24Q-AC-F, BR-VDX6940-24Q-AC-R,
  BR-VDX6940-36Q-AC-F and BR-VDX6940-36Q-AC-R

The “Brocade VDX 6940-144S” column in Table 13 applies to the following SKUs:

- BR-VDX6940-64S-AC-F, BR-VDX6940-64S-AC-R,
  BR-VDX6940-96S-AC-F, BR-VDX6940-96S-AC-R,
  BR-VDX6940-144S-AC-F and BR-VDX6940-144S-AC-R

Table 13 – Physical Interface Descriptions for VDX 6940-36Q and VDX 6940-144S

Physical Interface	Brocade VDX 6940-36Q	Brocade VDX 6940-144S
Networking ports	(QTY. 36) 40-GbE QSFP ports	(QTY. 96) 10-GbE SFP ports (QTY. 12) 40-GbE QSFP ports
Management Ethernet port	(QTY. 1) RJ-45 10/100/1000 Ethernet out-of-band management port	(QTY.1) RJ-45 10/100/1000 Ethernet out-of-band management port
Serial port	(QTY. 1) RJ-45 used for console	(QTY. 1) RJ-45 used for console
USB port	(QTY. 1) Used for data and firmware downloads with Brocade USB flash device	(QTY. 1) Used for data and firmware downloads with Brocade USB flash device
LEDs	(QTY. 1) System Power LED (QTY. 1) System Status LED (QTY. 5) Fan LEDs; One LED per Fan (QTY. 2) Power Supply LEDs; One LED per Power Supply - on non-port side (QTY. 146) port LEDs	(QTY. 1) System Power LED (QTY. 1) System Status LED (QTY. 4) Fan LEDs; One LED per Fan (QTY. 4) Power Supply LEDs; Two LEDs per Power Supply – on non-port side (QTY. 146) port LEDs
Power Supply connector(s)	(QTY. 2) Power connectors	(QTY. 2) Power connectors

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

4.3 Brocade VDX 8770

Table 14 – Physical Interface Descriptions for VDX 8770-4 and VDX 8770-8 interface cards

Line modules / interface cards for VDX 8770-4 and VDX 8770-4	Physical Interface / Networking ports	LEDs
BR-VDX8770-48X10G-SFPP-1	(QTY. 48) 10 GbE port	(QTY. 1) Card Power LED (QTY. 1) Card Status LED (QTY. 48) Port LEDs
BR-VDX8770-12X40G-QSFP-1	(QTY. 12) 40 GbE QSFP ports	(QTY. 1) Card Power LED (QTY. 1) Card Status LED (QTY. 12) Port LEDs

Table 15 – Physical Interface Description for VDX 8770-4 and VDX 8770-8 Management Module (MM) (half-slot) card

Management Module (MM) Physical Interface	Quantity and Description
Management Ethernet and Networking ports	(QTY. 1) RJ-45 10/100/1000 Ethernet (Management) ports
Serial port	(QTY. 1) RJ-45 used for console
USB port	(QTY. 1) Used for data and firmware downloads with Brocade USB flash device
LED	(QTY. 1) Power LED (QTY. 1) Status LED (QTY. 1) Active LED (QTY. 2) port LEDs
Service IP Port	(QTY. 1) RJ-45 10/100/1000 Ethernet port (Latent functionality i.e. performs no function; reserved for future use)

Table 16 – Physical Interface Description for VDX 8770-4 and VDX 8770-8 Switch Fabric Module (SFM) card

Management Module (MM) Physical Interface	Quantity and Description
LED	(QTY. 1) Power LED (QTY. 1) Status LED

Table 17 – Physical Interface Description for VDX 8770-4 and VDX 8770-8 Fan Assemblies and Power Supplies

Physical Interface	Quantity and Description VDX 8770-4	Quantity and Description VDX 8770-8
LED	(QTY.12) Power Supply LED; Three LEDs per Power Supply (QTY. 4) Fan LEDs; Two LEDs per Fan – on non-port side	(QTY. 24) Power Supply LEDs; Three LEDs per Power Supply (QTY. 8) Fan LEDs; Two LEDs per Fan – on non-port side
Power Supply connector(s)	(QTY. 4) Power connectors	(QTY. 8) Power connectors

5 Identification and Authentication Policy

5.1 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 18 - 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 (RSA 2048)
RADIUS: If RADIUS is configured, RADIUS server authenticates to the cryptographic module.	Role-based operator authentication	RADIUS Shared Secret

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

Table 19 - Strengths of Authentication Mechanism

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 1/2^112 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 10/2^112 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 20 - Service Descriptions

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

6 Access Control Policy

6.1 Roles and Services

Table 21 - Services Authorized for Roles

ROLE / SERVICE	User	Admin	Maximum Permissions	LDAP	RADIUS
CLI Management		X	X		
Clock Management (NTP)		X	X		
Debug & Diagnostics		X	X		
Display		X	X		
Ethernet		X	X		
FIPS		X	X		
Firmware Management	X	X	X		
LDAP		X	X	X	
License		X	X		
Login Session Management		X	X		
PKI	X	X	X		
Platform		X	X		
RADIUS		X	X		X
Switch Connection Policy		X	X		
System Monitor		X	X		
Terminal Configuration		X	X		
User Management		X	X		
vCenter		X	X		
VCS		X	X		
Zeroize		X	X		

6.2 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 on-demand by power-cycling the module.
  - Expected indicator for successful Self-test execution: "<Self-test Name>...successful"
  - If an error is encountered the error status output is: "<Self-test Name>...FAILED!"
- Show Status: This service is met through the various status outputs provided by the services specified above, as well as the LED interfaces.

6.3 Definition of Critical Security Parameters (CSPs)

This section briefly describes the CSPs contained within the module. For detailed information on these CSPs, please refer to section 12, Appendix B: Critical Security Parameters.

The following are CSPs contained in the module:
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

DRBG CSPs:

- DRBG Seed
- DRBG Value V
- DRBG Key
- DRBG Internal State

Operator Authentication/Passwords:

- Passwords
- RADIUS Secret
- NTP Password

6.4 Definition of Public Keys:

This section briefly describes the Public Keys contained within the module. For detailed information on these Public Keys, please refer to section 13, Appendix C: Public Keys.

The following are the public keys contained in the module:

SSHv2 and SCP Public Keys:

- DH Public Key (2048 bit modulus)
- SSHv2 DH Peer Public Key (2048 bit modulus)
- 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)

TLS Public Keys:

- TLS v1.0/1.1/1.2 Peer Public Key (RSA 2048)

FW Download Public Keys:

- Firmware Download Public Key (RSA 2048 SHA-256)

LDAP Public Keys:

- LDAP ROOT CA certificate (RSA 2048)

6.5 Definition of Service Categories:

Table 22 - Services and Command Line Instructions (CLI)

Services	CLIs
CLI Management	no delete configure dir exit help history quit rename abort do pwd unhide unhide fips prompt1 prompt2 rbridge-id

Services	CLIs
Clock Management (NTP)	Clock Ntp
Debug & Diagnostics	Debug diag ping l2traceroute traceroute top undebug
Display	Show
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
FIPS	fips selftests cipherset prom-access
Firmware Management	Firmware
LDAP	aaa
License	License Dpod
Login Session Management	tacacs-server ldap-server aaa logout banner ssh telnet

Services	CLIs
PKI	Certutil
Platform	reload chassis clear copy fastboot usb logging service switch-attributes support auditlog autoupload beacon cidrecov df ha oscmd power-off power-on linecard
RADIUS	aaa
Switch Connection Policy	secpolicy
System Monitor	system-monitor system-monitor-mail threshold-monitor
Terminal Configuration	send terminal end line
User Management	Username role password-attributes rule encryption-level unlock
vCenter	Vcenter Vnetwork
VCS	Vcs
Zeroize	fips zeroize

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

Services listed in Table 23 below are the only services which have access to CSPs and Public Keys within the module.

Legend:

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

Table 23 - CSP Access Rights within Roles & Services

CSPs / Public Keys Services	SSHv2 and SCP CSPs & Public Keys	TLS CSPs & Public Keys	DRBG CSPs	Operator Authentication/Passwords	FW Download Public Keys	LDAP Public Keys
CLI Management	RW	RW	N	RW	N	RW
Clock Management (NTP)	N	N	N	RW	N	N
FIPS	RW	RW	RW	N	N	RW
Firmware Management	R	N	N	N	R	N
LDAP	N	N	N	N	N	RW
Login Session Management	N	N	N	RW	N	R
User Management	N	N	N	RW	N	N
PKI	RW	RW	RW	N	N	N
RADIUS	N	N	N	RW	N	N
Zeroize	Z	Z	Z	Z	N	Z

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

7 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.

7.1 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)
            (2) Three Key Triple-DES CBC KAT (decrypt)
            (3) AES (128, 192, 256) CBC KAT (encrypt)
            (4) AES (128, 192, 256) CBC KAT (decrypt)
            (5) SP800-90A AES-256 CTR_DRBG KAT
            (6) SHA-1, 256, 384, 512 KAT
            (7) HMAC SHA-1, 224, 256, 384, 512 KAT
            (8) RSA 2048 SHA 256 Sign KAT
            (9) RSA 2048 SHA 256 Verify KAT
            (10) SP800-135 TLS v1.0 KDF KAT
            (11) SP800-135 TLS v1.2 KDF KAT
            (12) SP800-135 SSHv2 KDF KAT
            (13) ECC CDH KAT
            (14) ECDSA KAT
            (15) Diffie-Hellman 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 (NDRNG)
        ii. Continuous Random Number Generator (RNG) test – performed on SP800-90A DRBG
        iii. RSA 2048 SHA- 256 Pairwise Consistency Test (Sign and Verify)
        iv. RSA 2048 Pair wise Consistency Test (Encrypt/Decrypt)
        v. ECDSA Pairwise Consistency test (Sign/Verify)
        vi. Firmware Load Test (RSA 2048 SHA-256 Signature Verification)
        vii. Bypass Test: N/A
        viii. 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 self-tests 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. FCSP is only supported in the non-FIPS Approved mode of operation.

8 Physical Security Policy

8.1 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.

8.2 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 24 - Inspection/Testing of Physical Security Mechanisms

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

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

9 Mitigation of Other Attacks Policy

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

Table 25 - Mitigation of Other Attacks

Other Attacks	Mitigation mechanism	Specific Limitations
N/A	N/A	N/A

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

10 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
DRBG	Deterministic Random Bit Generator
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
SNMPv3	Simple Network Management Protocol Version 3
SSHv2	Secure Shell Protocol
TLS	Transport Layer Security Protocol

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

11 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.

11.1 VDX 6740-24, VDX 6740-48 and VDX 6740-64

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. Figures shown in this section provides details on how to position each tamper evident label.

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 8 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 9 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 10 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 11 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 12 for details on how to position each seal.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

Figure 8 - VDX 6740-24, VDX 6740-48 and VDX 6740-64 bottom port side seal locations

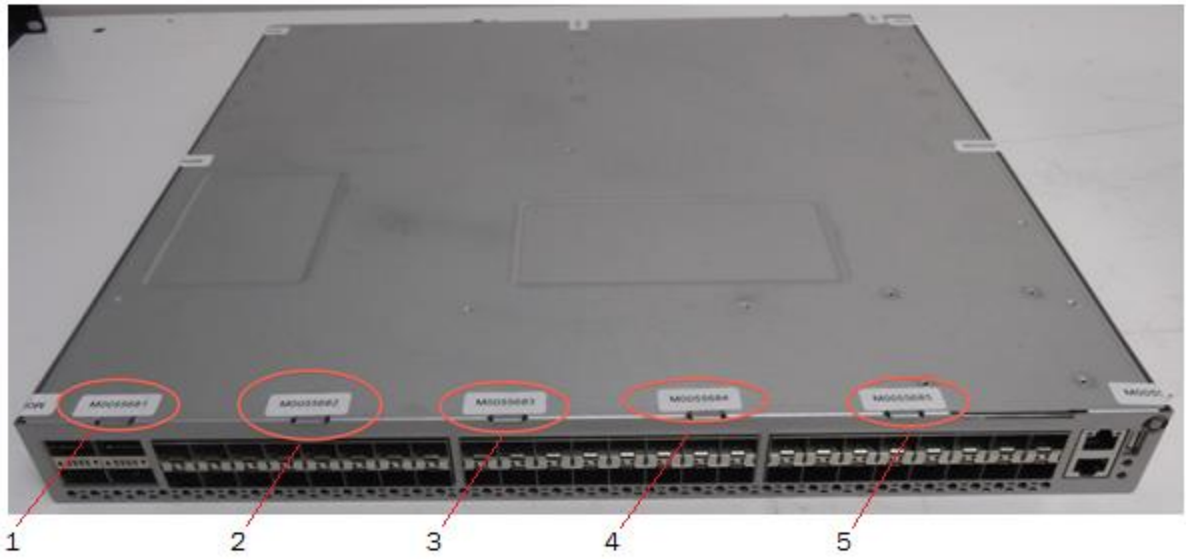
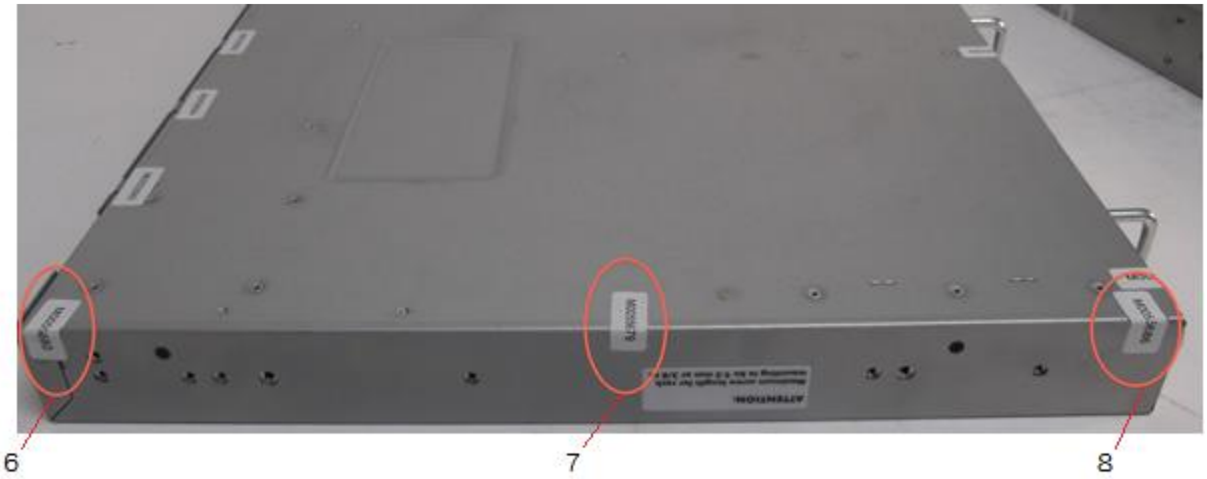


Figure 9 - VDX 6740-24, VDX 6740-48 and VDX 6740-64 bottom left side seal locations



REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

Figure 10 - VDX 6740-24, VDX 6740-48 and VDX 6740-64 bottom right side seal locations

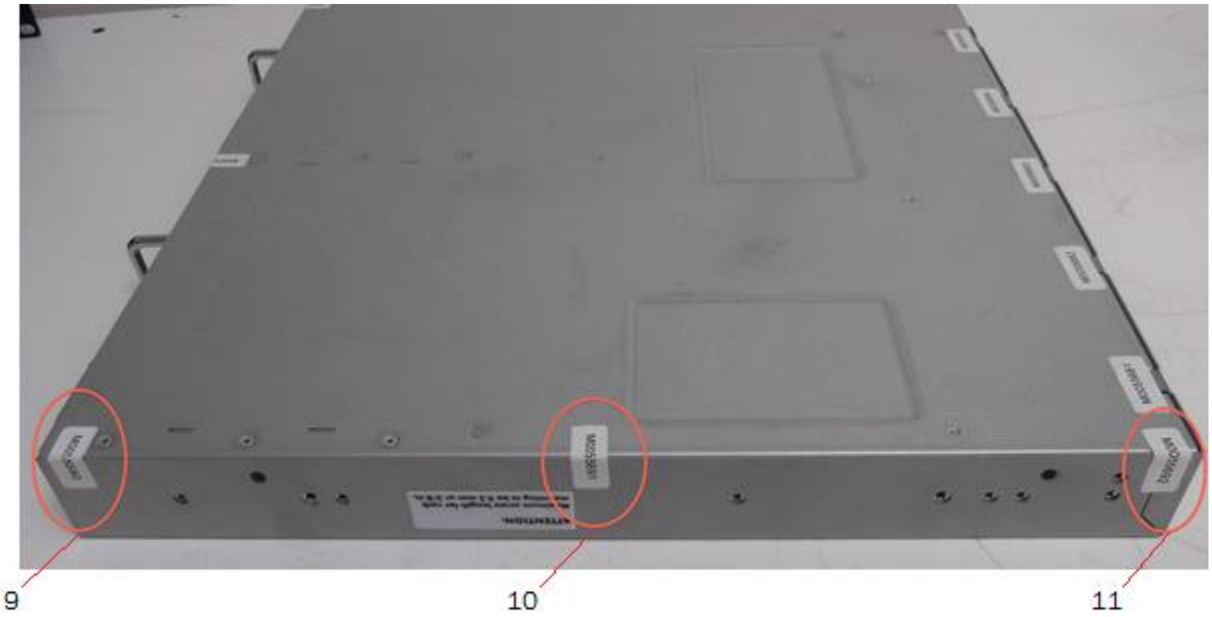
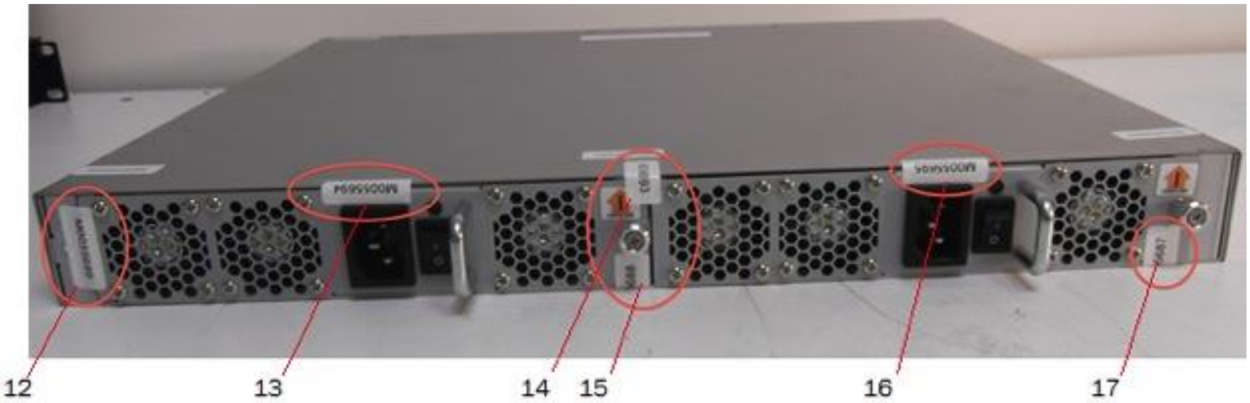


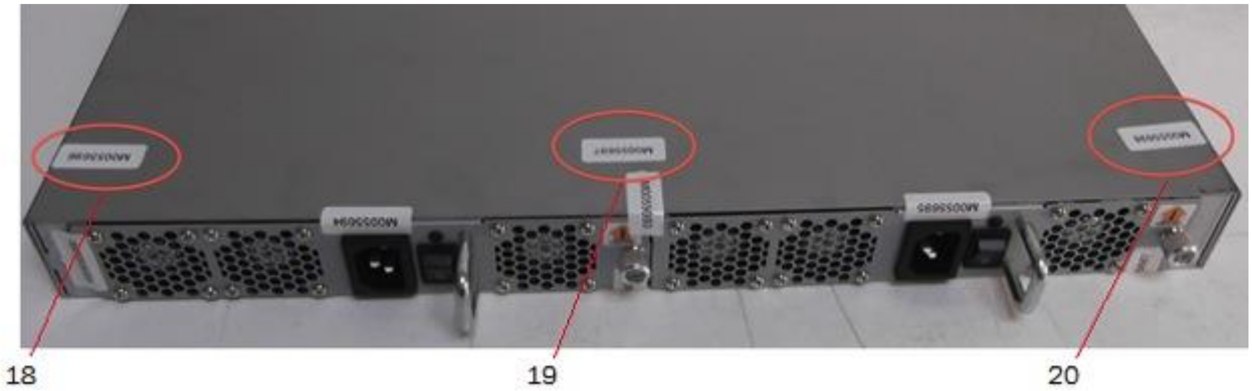
Figure 11 - VDX 6740-24, VDX 6740-48 and VDX 6740-64 top non-port side fan and power supply seal locations



REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

Figure 12 - VDX 6740-24, VDX 6740-48 and VDX 6740-64 top non-port side top cover seal locations



REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

11.2 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 figures in this section for details on how to position each tamper evident label.

Figure 13 - VDX 6740T-24, VDX 6740T-48, VDX 6740T-64 and VDX 6740T-56-1G bottom/front seal locations

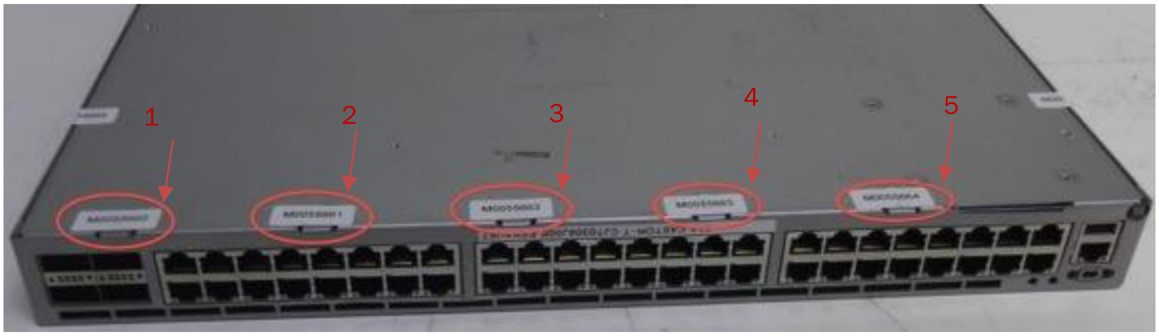
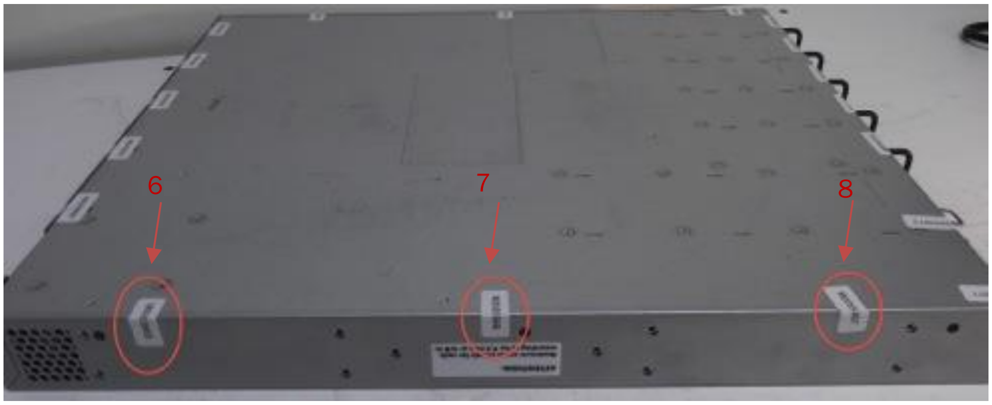


Figure 14 - VDX 6740T-24, VDX 6740T-48, VDX 6740T-64 and VDX 6740T-56-1G bottom left side seal locations



REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

Figure 15 - VDX 6740T-24, VDX 6740T-48, VDX 6740T-64 and VDX 6740T-56-1G bottom right side seal locations

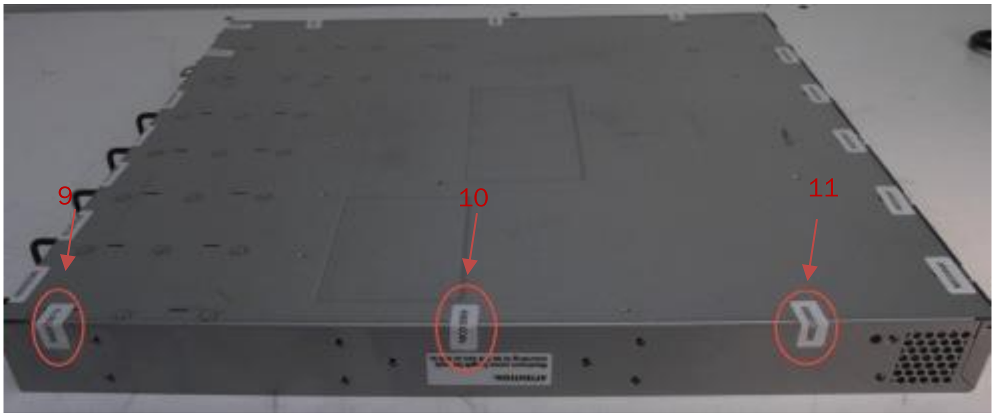


Figure 16 - VDX 6740T-24, VDX 6740T-48, VDX 6740T-64 and VDX 6740T-56-1G bottom back side seal locations

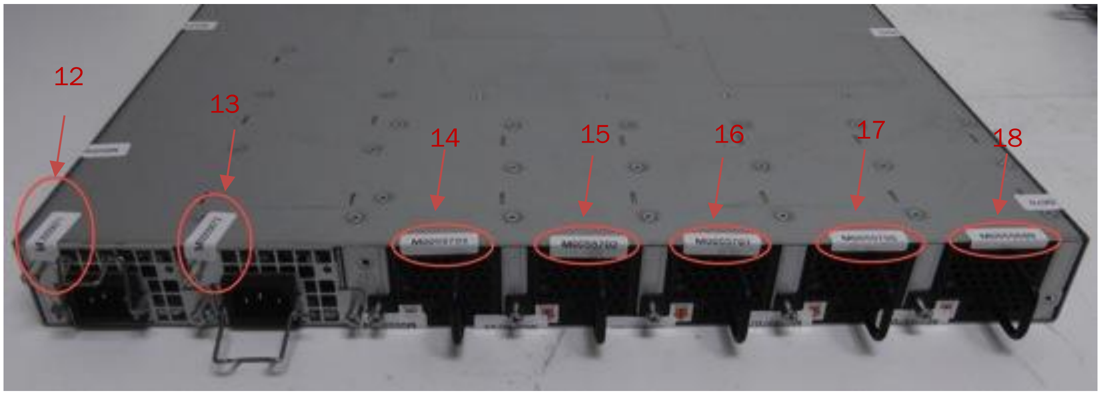
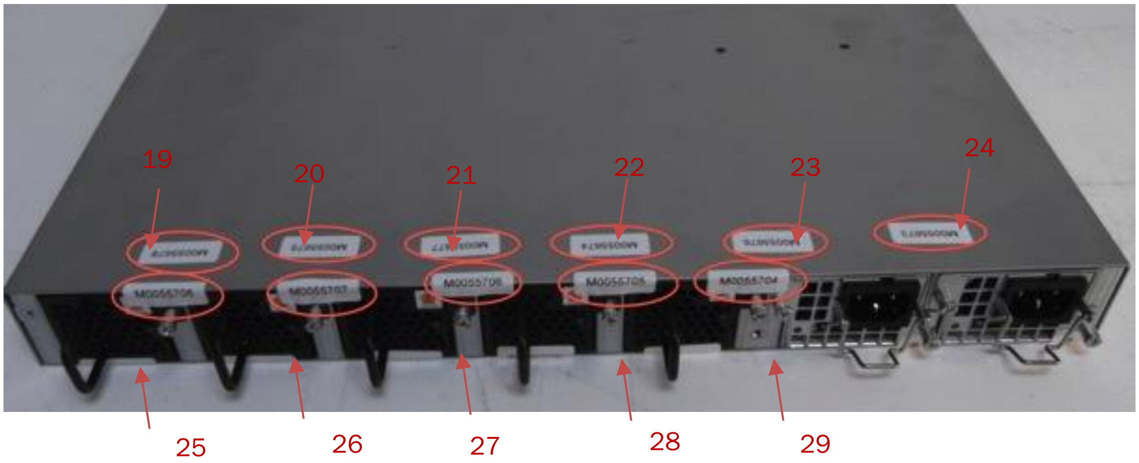


Figure 17 - VDX 6740T-24, VDX 6740T-48, VDX 6740T-64 and VDX 6740T-56-1G top back side seal locations



11.3 VDX 6940

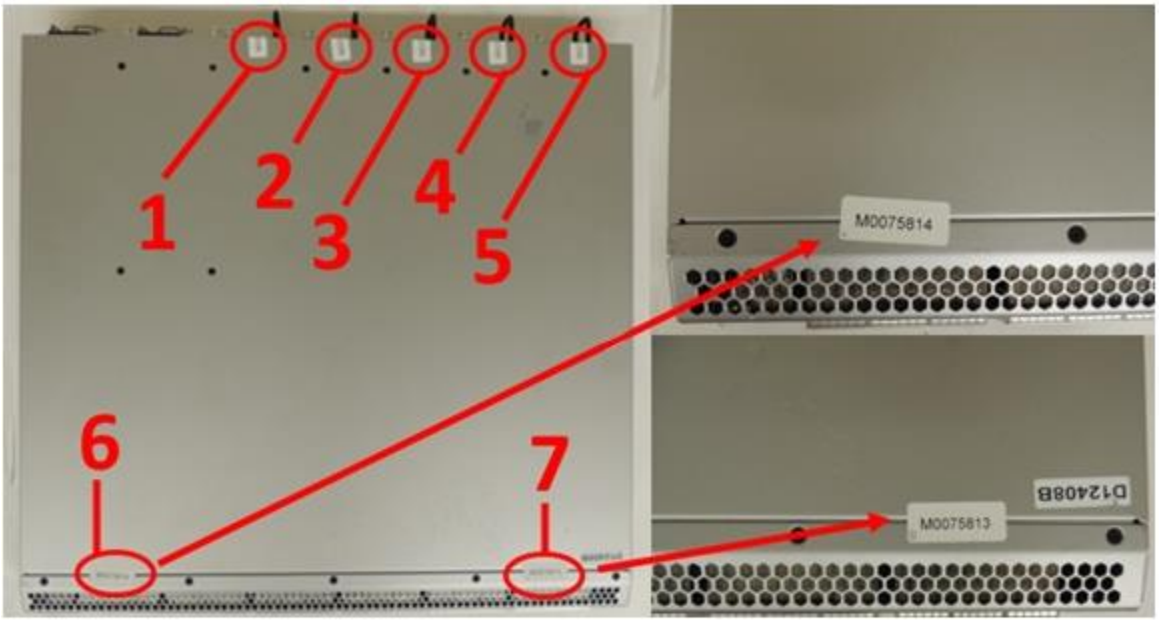
11.3.1 VDX 6940-24Q, VDX 6940-36Q

NOTE: THE BROCADE VDX6940-24Q USES THE SAME HARDWARE AS THE VDX 6940-36Q BUT USES A DIFFERENT SOFTWARE LICENSE. SEAL PLACEMENT LOCATIONS AND PROCEDURES FOR THE VDX6940-24Q ARE THE SAME AS THOSE FOR THE VDX6940-36Q (SHOWN).

The Brocade VDX 6940-36Q requires a total of nine (9) seals. See figures in this section for details on how to position each seal.

1. **Top:** Seven (7) tamper evident seals are required to complete this step of the procedure.
   Affix a seal, which wrap from the top to the rear of the unit, at seal location 1, 2, 3, 4, and 5. The purpose of these seals is to secure the removable fans to the unit. Affix a seal at location 6 and 7 which bridge the gap between the top front of the unit and the removable top cover. The purpose of these labels is to secure the top removable cover to the unit. See Figure 18 for correct seal orientation and positioning.

Figure 18 - VDX 6940-36Q - Top view with tamper evident seals



REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

2. **Rear:** Two (2) tamper evident seals are required to complete this step of the procedure. Affix a seal, which wrap from the rear to the bottom of the unit at seal location 8 and 9. The purpose of these seals is to secure the removable power supplies to the unit. See Figure 19 and Figure 20 for correct seal orientation and positioning.

Figure 19 - VDX 6940-36Q - Rear view with tamper evident seals

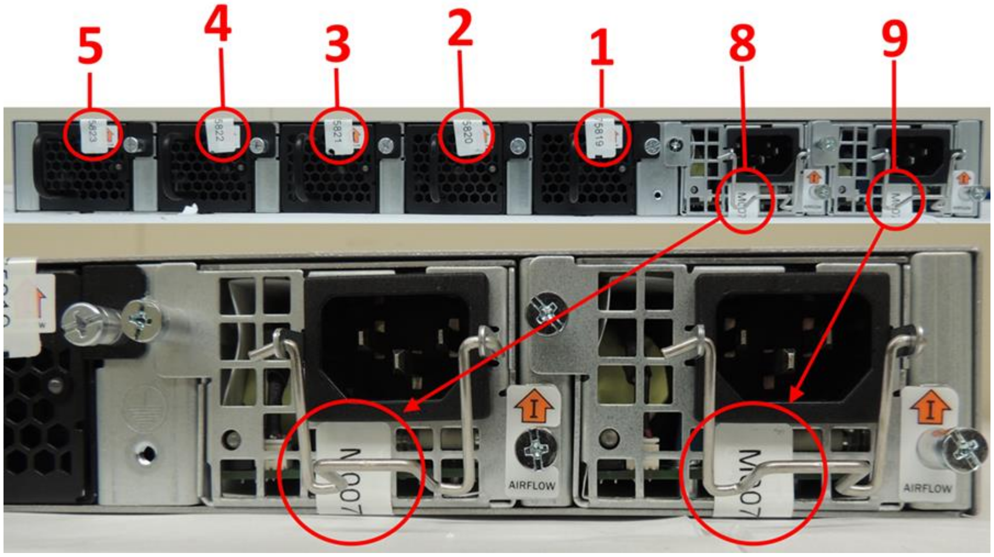
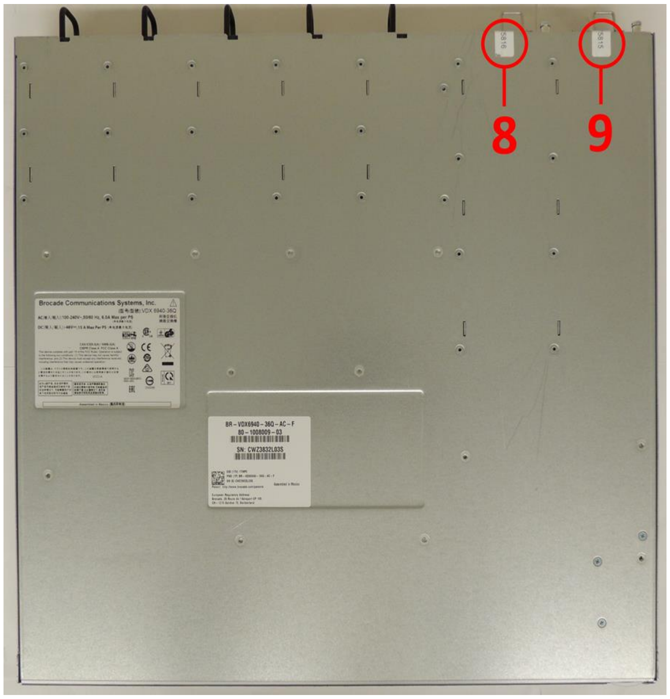


Figure 20 - VDX 6940-36Q - Bottom view with tamper evident seals



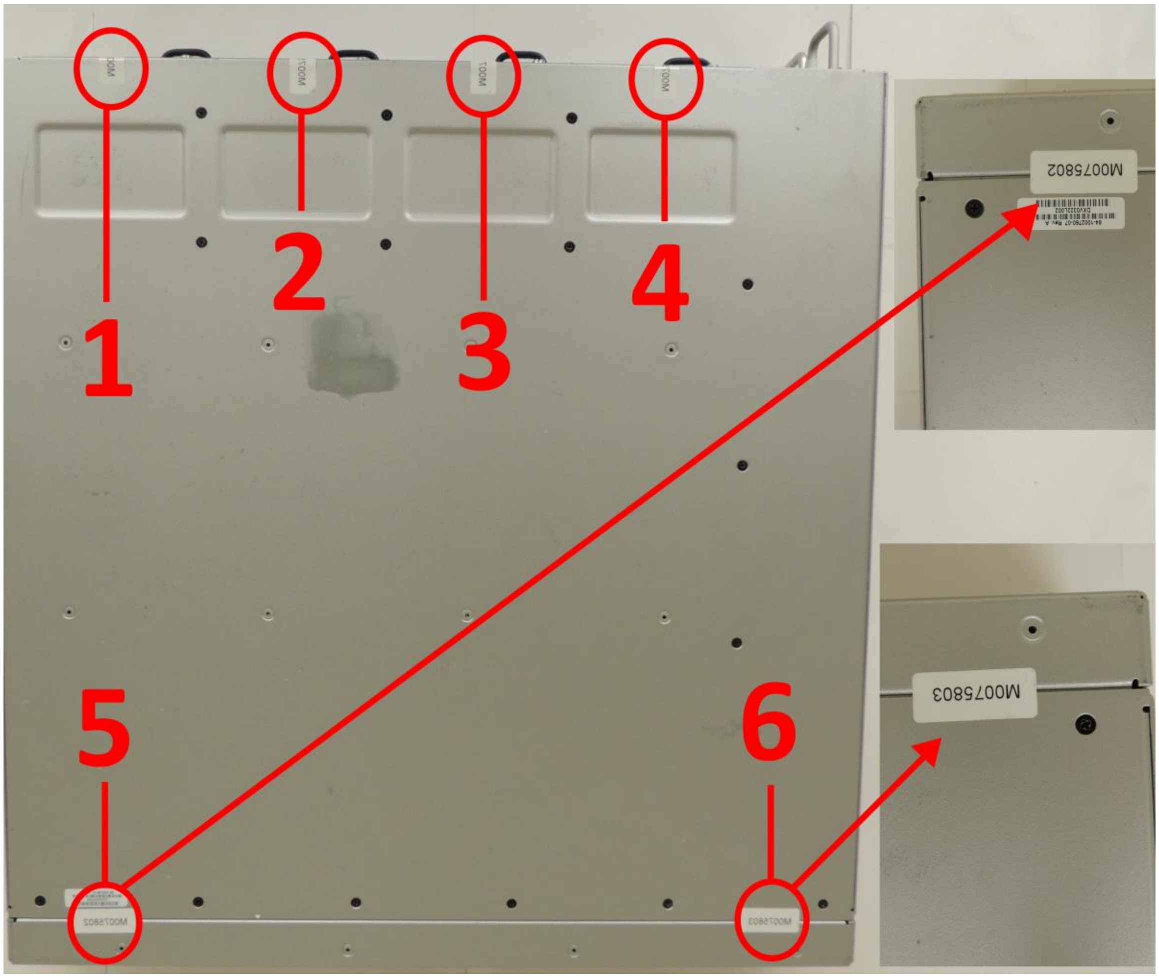
11.3.2 VDX6940-64S, VDX6940-96S, and VDX 6940-144S

NOTE: THE BROCADE VDX6940-64S AND VDX6940-96S USE THE SAME HARDWARE AS THE VDX 6940-144S BUT USE A DIF-FERENT SOFTWARE LICENSE. SEAL PLACEMENT LOCATIONS AND PROCEDURES FOR THE VDX6940-64S AND VDX6940-96S ARE THE SAME AS THOSE FOR THE VDX6940-144S (SHOWN).

The Brocade VDX 6940-144S requires a total of eight (8) seals. See figures in this section for details on how to position each seal.

1. **Top:** Six (6) tamper evident seals are required to complete this step of the procedure.
   Affix a seal, which wrap from the top to the rear of the unit at seal location 1, 2, 3, and 4. The purpose of these seals is to secure the removable fans to the unit. Affix a seal at location 5 and 6 which bridge the gap between the top front of the unit and the removable top cover. The purpose of these labels is to secure the top removable cover to the unit. See Figure 21 for correct seal orientation and positioning.

Figure 21 - VDX 6940-144S - Top view with tamper evident seals



2. **Rear:** Two (2) tamper evident seals are required to complete this step of the procedure.
   Affix a seal, which wrap from the rear of the unit to the left side of the unit, at seal location 7 and 8. The purpose of these seals is to secure the removable power supplies to the unit. See Figure 22 and Figure 23 for correct seal orientation and positioning.

Figure 22 - VDX 6940-144S - Rear view with tamper evident seals

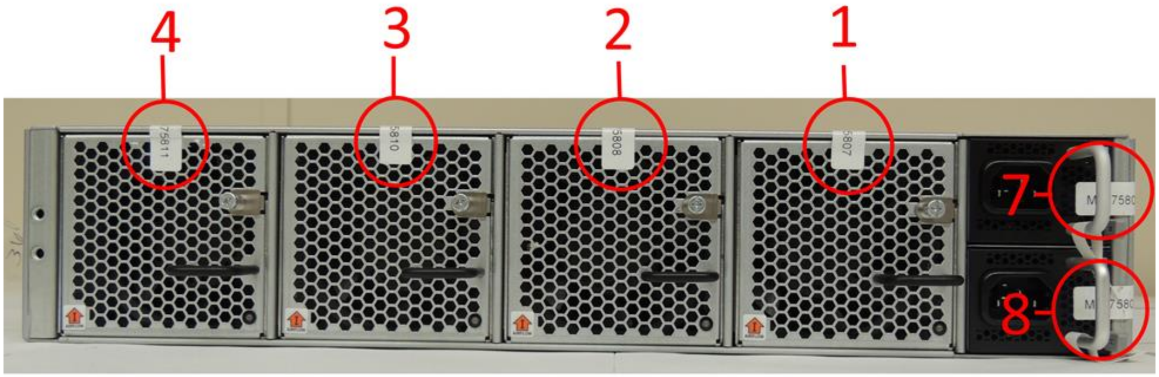
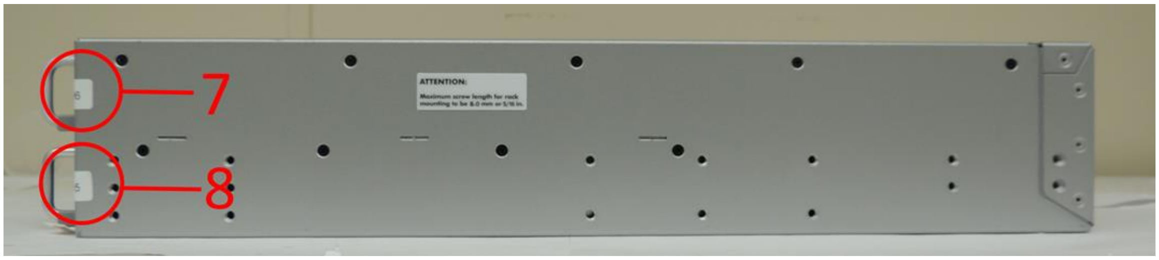


Figure 23 - VDX 6940-144S - Left view with tamper evident seals


7
8
ATTENTION:
Maximum screw length for rack mounting to be 8.0 mm or 5/16 in.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

11.4 VDX 8770

11.4.1 VDX 8770-8

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 for the VDX 8770-8. See figures in this section for details on how to position each tamper evident label.

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

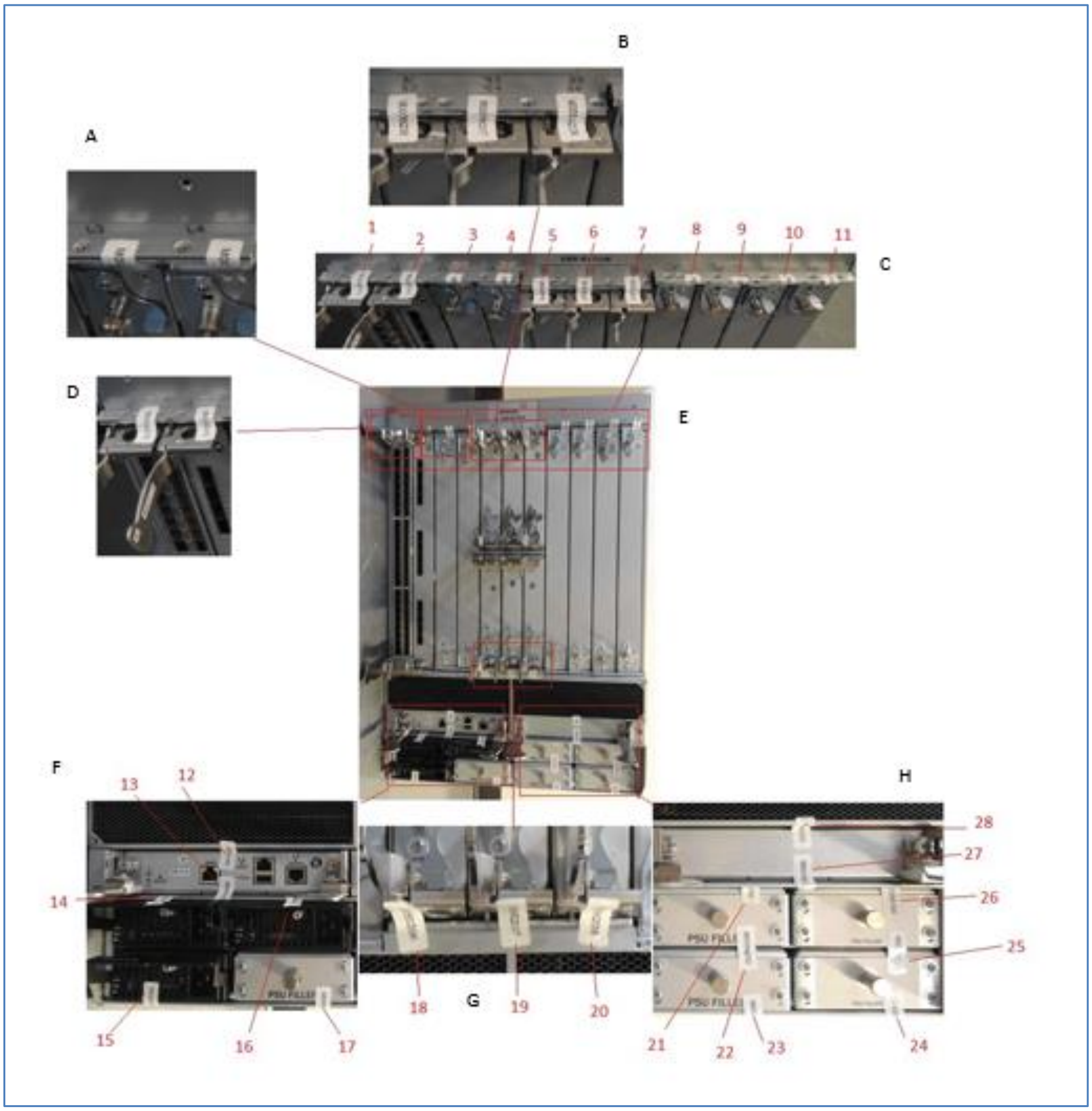
Twenty-eight (28) tamper evident seals are required to complete steps 1 to 6 on the port side as illustrated in Figure 24. Unused slots must be filled with the module or filler panel appropriate for that slot to maintain adequate cooling.

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 Figure 24 A, C, D and E 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 24 B and E 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 24 E and G 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 24 E, F and H for details on how to position each seal.
5. For VDX 8770-8 with AC power supply Units (PSU) see Figure 24 E and F for details on how to position seals 14-17. Four (4) seals are required to complete this step.
6. See Figure 24 E and H for details on how to position seals 21-26. Six (6) seals are required to complete this step.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

Figure 24 - VDX 8770-8 AC PSU port side seal locations



REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

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

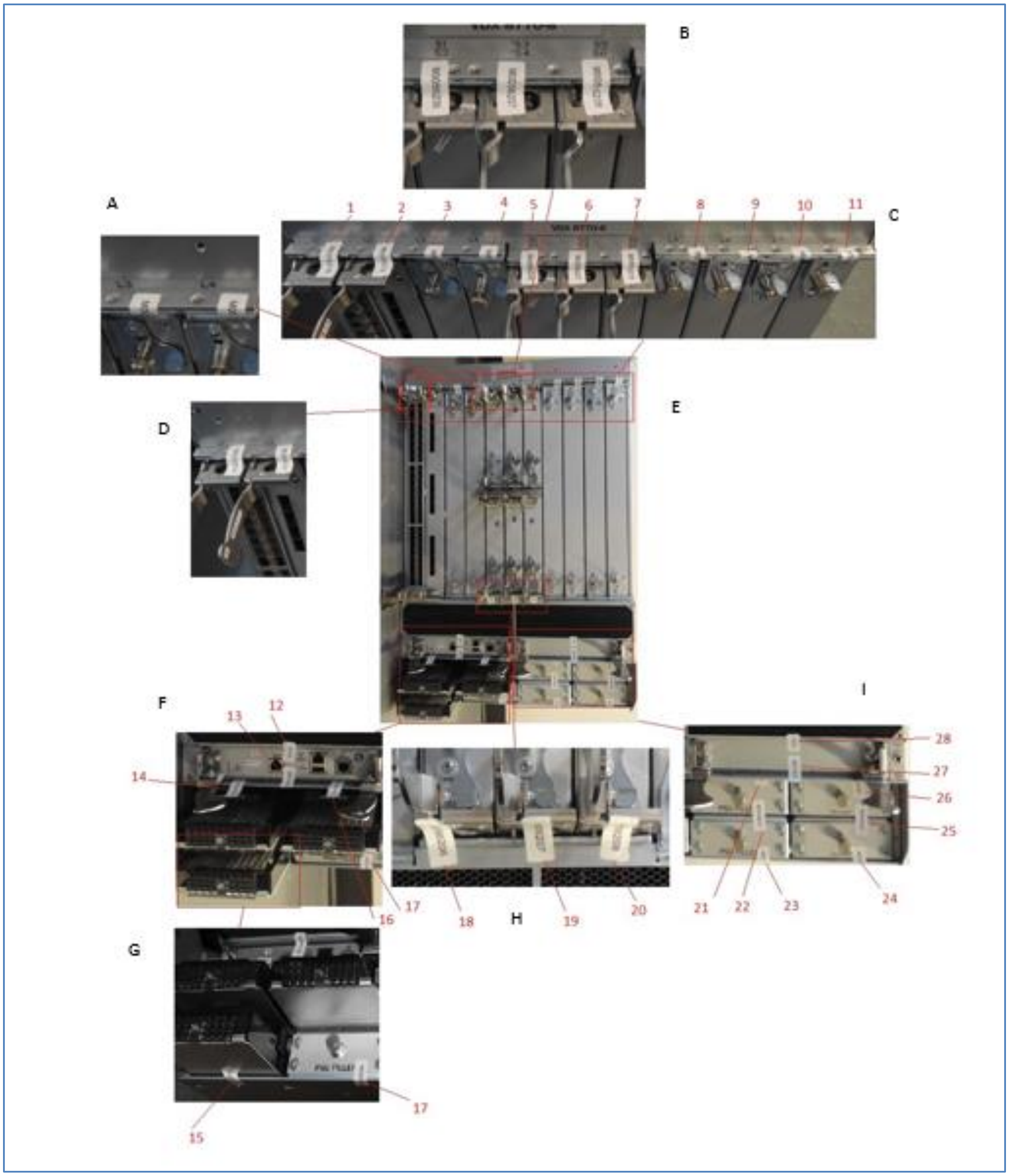
Twenty-eight (28) tamper evident seals are required to complete steps 1 to 6 on the port side as illustrated in Figure 25. Unused slots must be filled with the module or filler panel appropriate for that slot to maintain adequate cooling.

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 Figure 25 A, C, D and E 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 25 B and E 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 25 E and H 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 25 E, F and I for details on how to position each seal.
5. For VDX 8770-8 with DC power supply Units (PSU) refer to Figure 25 E, F and G for details on how to position seals 14-17. Four (4) seals are needed to complete this step.
6. See Figure 25 E and I on how to position seals 21-26. Six (6) seals are required to complete this step.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

Figure 25 - VDX 8770-8 DC PSU Port Side seal locations



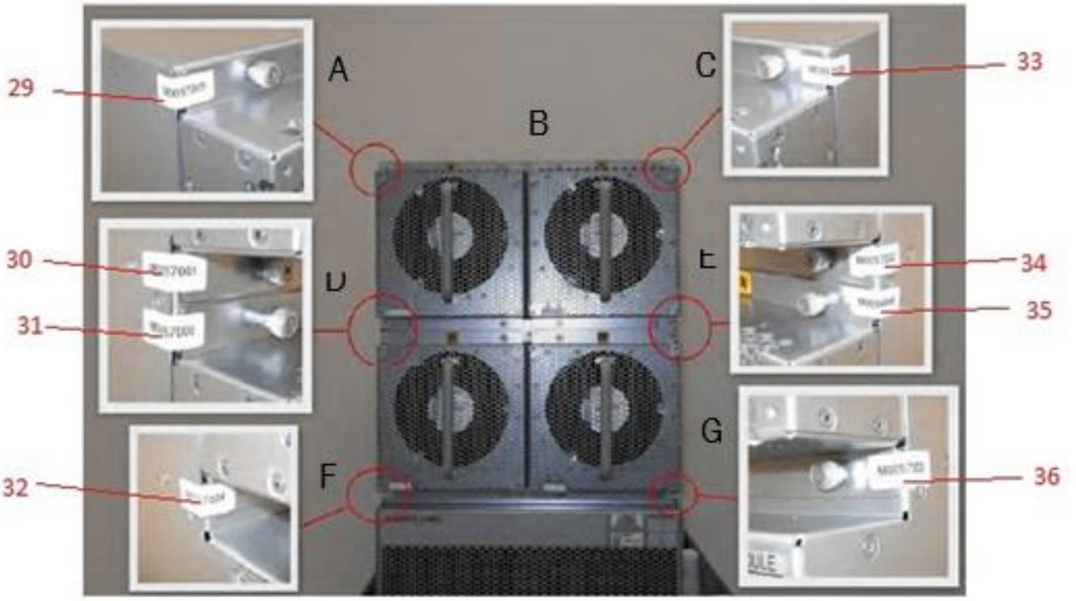
REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

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 26. All fan slots must be filled with a FAN FRU or FAN FRU filler panel to maintain adequate cooling.

Figure 26 - 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 26 A-G for details on how to position each seal.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

11.4.2 VDX 8770-4

Twenty-three (23) tamper evident seals are required to complete the physical security requirements for the VDX 8770-4. See figures in this section for details on how to position each tamper evident label..

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 27. 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 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 27 A and C 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 27 B and C 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 27 C and D for details on how to position each seal.
4. The VDX 8770-4 accepts both AC and DC power supply unit. Depending on the type of installed power supply unit 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 27 F 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 28 and Figure 27 F 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 26 A and C. The lower left FIPS bracket is shown in Figure 26 E and C. Two (2) seals are required to complete this step. See Figure 27 A and E for details on how to position each seal.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

Next page →

Figure 27 - VDX 8770-4 port side seal locations

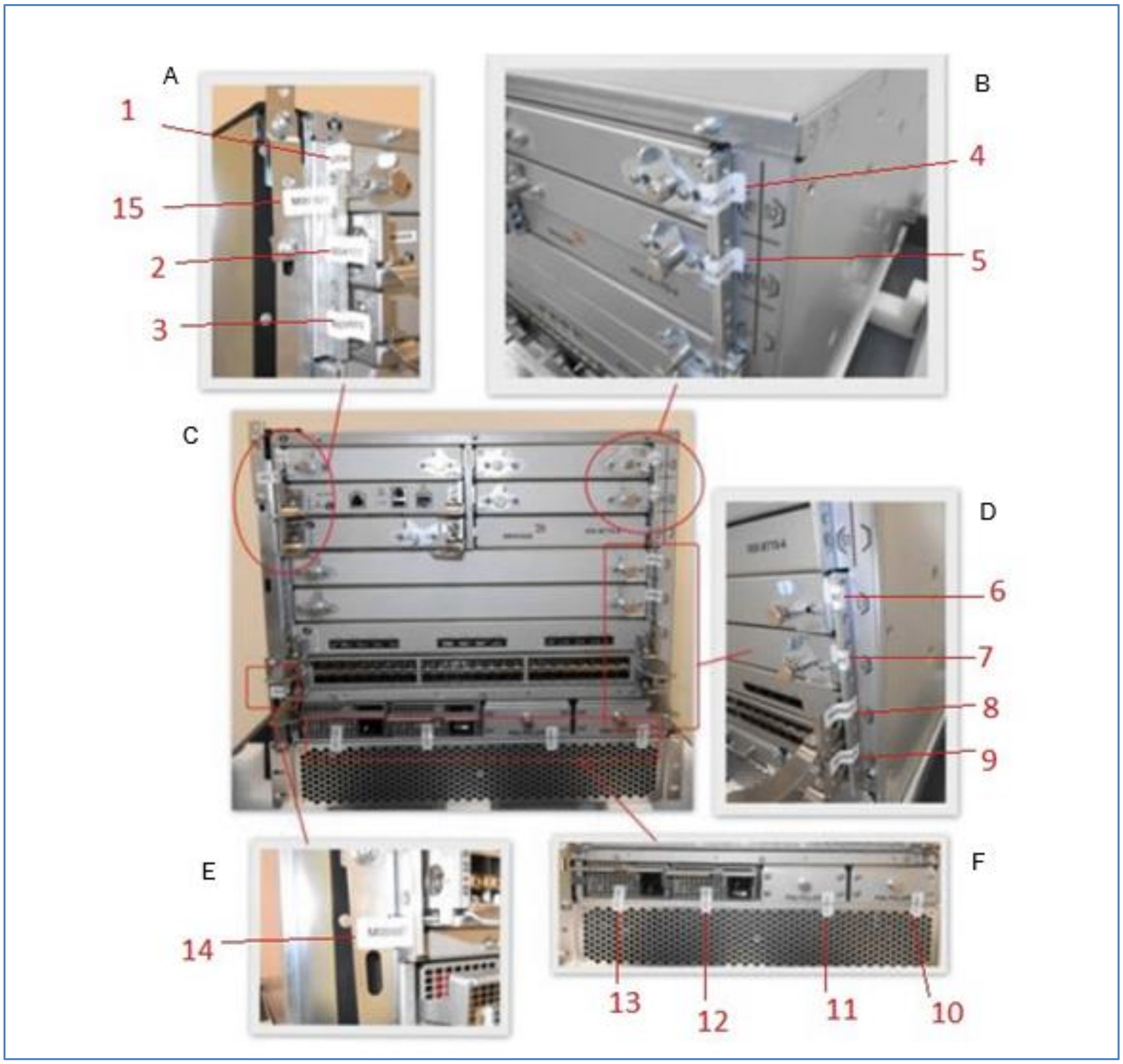
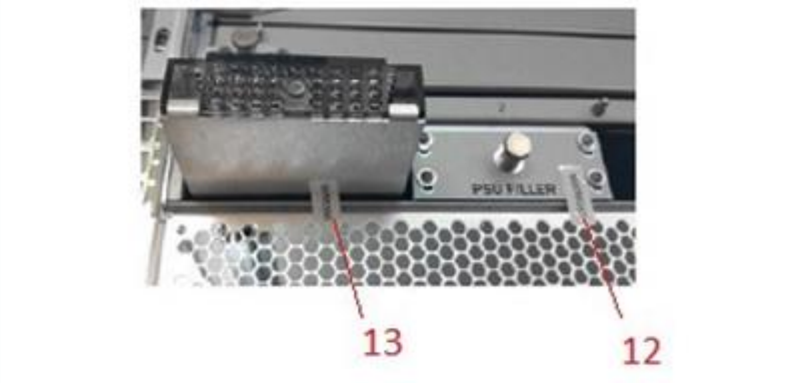


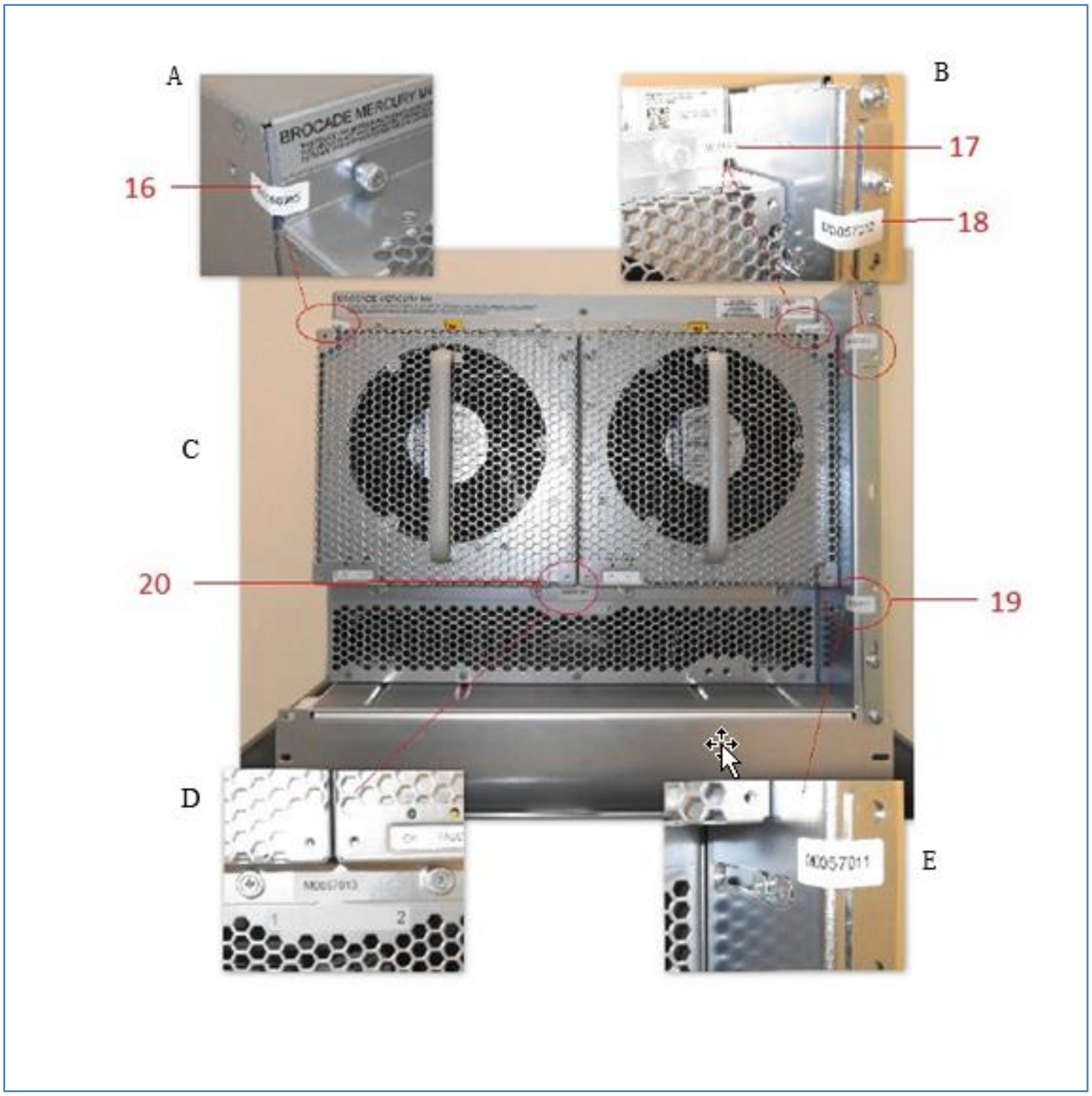
Figure 28 - VDX 8770-4 DC PSU seal locations



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 29. All fan slots must be filled with a FAN FRU or FAN FRU filler panel to maintain adequate cooling.

Figure 29 - VDX 8770-4 Non-port side seal locations



REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

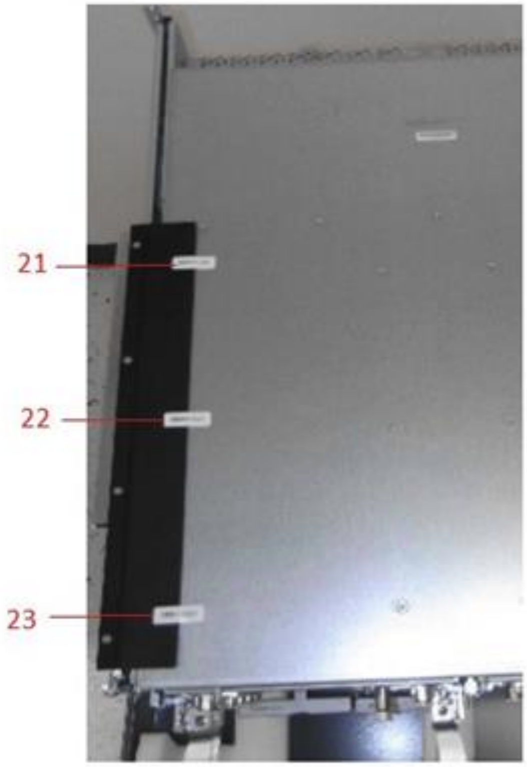
Next page →

1. Apply one (1) seal 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 29 A, B and C for details on how to position each seal.
2. Apply one (1) seal 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 29 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 29. The lower right FIPS bracket is shown in Figure 29. Two (2) seals are required to complete this step. See Figure 29 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 30. Relative to the port side of the VDX 8770-4 chassis the air duct is secured to the left side of the chassis.

Figure 30 - 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 30 for details on how to position each seal.

12 Appendix B: Critical Security Parameters

The module supports the following CSPs:

12.1 SSHv2 and SCP CSPs

1. DH Private Keys (256 bits) for use with 2048 bit modulus
- Description: Used in 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 SP800-90A DRBG; 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
- Description: AES (AES-128-CBC, AES-256-CBC) 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, 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: Plaintext in RAM
- 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
- Storage: Plaintext in RAM
- 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: Plaintext in RAM and Compact Flash
- Entry: N/A
- Output: N/A
- Destruction: "fips zeroize" command

7. Value of K during SSHv2 256 ECDSA session
- Description: ECDSA K Value
- Generation: SP800-90A DRBG, as per FIPS 186-4
- Storage: Plaintext in RAM
- 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.
- Storage: Plaintext in RAM
- 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.
- Storage: Plaintext in RAM
- 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: Plaintext in RAM and Compact Flash
- Entry: N/A
- Output: N/A
- Destruction: "fips zeroize" command

12.2 TLS CSPs

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 TLS 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 Keys 128, 256 bit AES CBC, Triple-DES 3 key CBC
- Description: Triple-DES 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

15. TLS Authentication Key for HMAC-SHA-1, HMAC-SHA-256
- Description: HMAC-SHA-1 and 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

12.3 DRBG CSPs

16. DRBG Seed
- Description: Seeding material for the SP800-90A DRBG (CTR_DRBG AES-256)
- Type: DRBG Seed material
- Generation: Internally generated using the NDRNG
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: "fips zeroize" command

17. DRBG Value V
- Description: Internal State of SP800-90A DRBG (CTR_DRBG AES-256)
- 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" command

18. DRBG Key
- Description: Internal State of SP800-90A DRBG (CTR_DRBG AES-256)
- 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" command

19. DRBG Internal State
- Description: Internal State of SP800-90A DRBG (CTR_DRBG AES-256)
- 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" command

12.4 Operator Authentication/Passwords

20. Passwords
- Description: Password used to authenticate operators (8 to 40 characters)
- Generation: N/A
- Storage: Plaintext in RAM and Compact Flash
- Entry: Encrypted/Authenticated over SSHv2 session
- Output: Encrypted/Authenticated over SSHv2 session
- Destruction: "fips zeroize" command

21. RADIUS Secret
- Description: Used to authenticate the RADIUS Server (8 to 40 characters)
- Generation: N/A
- Storage: Plaintext in RAM and Compact Flash
- Entry: Encrypted/Authenticated over SSHv2 session
- Output: Encrypted/Authenticated over SSHv2 session
- Destruction: "fips zeroize" command

22. NTP Password
- Description: Used to authenticate the NTP client with the server (0-15 characters)
- Generation: N/A
- Storage: Plaintext in RAM and Compact Flash
- Entry: Encrypted/Authenticated over SSHv2 session
- Output: Encrypted/Authenticated over SSHv2 session
- Destruction: "fips zeroize" command

13 Appendix C: Public Keys

The module supports the following Public Keys:

13.1 SSHv2 and SCP Public Keys

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

3. SSHv2 RSA 2048 bit Peer Public Key
-Description: Used to authenticate SSHv2 session Client
-Generation: N/A
-Storage: Plaintext in Compact Flash
-Entry: Plaintext; Imported into the module
-Output: N/A

4. 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: N/A
-Output: N/A

5. 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

6. SSHv2 ECDSA Peer Public Key (P-256)
- Description: Used to authenticate SSHv2 server to Client
- Generation: N/A
- Storage: Plaintext in Compact Flash
- Entry: Plaintext; Imported into the module
- Output: N/A

7. 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 SP800-90A DRBG; 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

13.2 TLS Public Keys

8. TLS v1.0/1.1/1.2 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

13.3 FW Download Public Keys

9. 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 RAM and Compact Flash
- Entry: Plaintext through firmwarekeyupdate cmd or through FW Update cmd.
- Output: Plaintext through firmwarekeyshow cmd.

13.4 LDAP Public Keys

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

14 Appendix D: Components Excluded from FIPS 140-2 Requirements

The following SKUs do not have any security relevance and have been excluded from FIPS 140-2 requirements:

Table 26 - VDX 6740 AC fan/power supply assembly options

SKU / MFG Part Number	Description
SKU: XBR-250WPSAC-F / P/N: 80-1004576-03	Brocade VDX 6740 AC fan/power supply assembly FRU, non-port side exhaust airflow
SKU: XBR-250WPSAC-R / P/N: 80-1004577-03	Brocade VDX 6740 AC fan/power supply assembly FRU, port side exhaust airflow

Table 27 - VDX 6740 and VDX 6740T Software Licenses

SKU / MFG Part Number	Description
SKU: SW-VDX-24POD10G / P/N: 80-1007513-01	Software license, 24 Ports 10G POD
SKU: SW-VDX-4POD40G / P/N: 80-1007524-01	Software license, 4 Ports 40G POD (equivalent to 40 G ports)

Table 28 – AC Power Supply Units (PSU) and Fan for Validated VDX 6740T Configuration

SKU / Part Number	Description
SKU: XBR-500WPSAC-01-F / P/N: 80-1007650-01	Brocade VDX 6740T AC Power Supply with Non Port side exhaust airflow.
SKU: XBR-500WPSAC-01-R / P/N: 80-1007651-01	Brocade VDX 6740T AC Power Supply with Port side exhaust airflow.
SKU: XBR-AC-FAN-F / P/N: 80-1007638-01	Brocade VDX 6740T AC Fan with Non port side exhaust airflow.
SKU: XBR-AC-FAN-R / P/N: 80-1007639-01	Brocade VDX 6740T AC Fan with Port side exhaust airflow.

Table 29 - VDX 6940 Software Licenses

SKU / Part Number	Description
SKU: SW-VDX-32-10GPOD P/N: 80-1008546-01	Factory installed software license - thirty-two (32) 10GbE Ports On Demand (POD) software license (used for VDX 6940-96S and VDX 6940-144S)
SKU: SW-VDX-12-40GPOD P/N: 80-1008547-01	Factory installed software license - twelve (12) 40GbE Ports On Demand (POD) software license (used for VDX 6940-36Q and VDX 6940-144S)
SKU: BR-VDX6940-36Q-12X40G-POD P/N: 80-1008512-01	Software License only – 12x40GbE Ports On Demand(POD) license for the VDX 6940-24Q models
SKU: BR-VDX6940-144S-16-10GPOD P/N: 80-1008544-01	Software License only – 16x10GbE Ports On Demand(POD) LICENSE FOR VDX6940-144S
SKU: BR-VDX6940-144S-6X40G-POD P/N: 80-1008545-01	Software License only – 6x40GbE or 2x100GbE Ports On Demand(POD) LICENSE FOR VDX6940-144S

Table 30 – Fan and AC Power Supply Units (PSU) for Validated VDX 6940 Configuration

SKU	Description
SKU: XBR-500WPSAC-01-F / P/N: 80-1007650-01	Brocade VDX 6940-24Q and Brocade VDX 6940-36Q, AC Power Supply with Non-port side exhaust airflow.
SKU: XBR-500WPSAC-01-R / P/N: 80-1007651-01	Brocade VDX 6940-24Q and Brocade VDX 6940-36Q, AC Power Supply with Port side exhaust airflow.
SKU: XBR-FAN-40-01-F / P/N: 80-1008448-01	Brocade VDX 6940-24Q and Brocade VDX 6940-36Q, AC Fan with Non-port side exhaust airflow.
SKU: XBR-FAN-40-01-R / P/N: 80-1008447-01	Brocade VDX 6940-24Q and Brocade VDX 6940-36Q, AC Fan with Port side exhaust airflow.
SKU: XBR-1100WPSAC-F / P/N: 80-1007262-01	Brocade VDX 6940-64S, Brocade VDX 6940-96S and Brocade VDX 6940-144S, AC Power Supply with Non-port side exhaust airflow.
SKU: XBR-1100WPSAC-R / P/N: 80-1007263-01	Brocade VDX 6940-64S, Brocade VDX 6940-96S and Brocade VDX 6940-144S, AC Power Supply with Port side exhaust airflow.
SKU: XBR-FAN-80-01-F / P/N: 80-1008542-01	Brocade VDX 6940-64S, Brocade VDX 6940-96S and Brocade VDX 6940-144S, AC Fan with Non-port side exhaust airflow.
SKU: XBR-FAN-80-01-R / P/N: 80-1008543-01	Brocade VDX 6940-64S, Brocade VDX 6940-96S and Brocade VDX 6940-144S, AC Fan with Port side exhaust airflow.

Table 31 – Other components for the VDX 8770

SKU / Part Number	Description
SKU: XBR-ACPWR-3000 P/N: 80-1006540-01	Field Replaceable Unit - Power Supply Unit (PSU)– AC
SKU: XBR-DCPWR-3000 P/N: 80-1006539-02	Field Replaceable Unit - Power Supply Unit (PSU) – DC
SKU: XBR-FAN-FRU P/N: 80-1006080-01	Field Replaceable Unit - Fan Module (FAN)