Brocade® MLXe® Series Ethernet Routers, Brocade® NetIron® CER 2000 Series Ethernet Routers and Brocade NetIron® CES 2000 Series Ethernet Switches

FIPS 140-2 Non-Proprietary Security Policy

Document Version 1.0

March 7, 2017

Brocade Communications

Revision History

Revision History	Revision	Summary of changes
3/7/2017	1.0	Initial version

This Brocade Communications Systems, Inc. Security Policy for Brocade® MLXe® NetIron® Ethernet Routers, Brocade® NetIron® CER 2000 series Ethernet Routers and Brocade CES 2000 series Routers 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:

1 Introduction 12
2 Overview 13
2.1 Brocade MLXe 13
2.2 Brocade CER 2000 series /CES 2000 series 13
2.3 Tamper Evident Seal Application requirement 14
2.4 Differences in features and services across NetIron Hardware family 14
2.4.1 Physical Form Factor, Support for Interface Line Cards and Port Counts 14
2.4.2 IPSec, MACsec and HTTPS service support comparison 15
2.4.3 Power Supply support 16
2.4.4 Physical Layer interface for ports CER 2000 series / CES 2000 series 17
2.5 Block Diagram 18
3 Brocade MLXe series 19
3.1 MLXe bundled SKUs 19
3.2 MLXe Management cards SKUs 20
3.3 MLXe Interface cards SKUs 21
3.4 MLXe Switch Fabric Modules SKUs 22
3.5 MLXe Power Supply SKUs 23
3.6 MLXe Exhaust Fan SKUs 23
3.7 MLXe Chassis Slots Blank Filler Panel SKUs 24
3.8 Validated MLXe configuration 25
3.9 MLXe-4 images 26
3.10 MLXe-8 images 27
3.11 MLXe-16 images 28
3.12 MLXe-32 images 30
4 Brocade CER 2000 series 32
4.1 Brocade CER 2000 images 33
5 Brocade CES 2000 series 34
5.1 Brocade CES 2000 35
6 Ports and Interfaces 36
6.1 Brocade MLXe series 37
6.1.1 MLXe MR2 Management Modules (Management cards) 37
6.1.2 BR-MLX-10GX20-M, BR-MLX-10GX20-X2, BR-MLX-1GX20-U10G-M and BR-MLX-1GX20-U10G-X2 line cards 37
6.1.3 BR-MLX-10GX4-IPSEC-M interface line card 38
6.1.4 MLXe Status LED 38
6.2 Brocade CER 2000 series/CES 2000 series 40

6.2.1 CER 2024C 40
6.2.2 CER 2024F 40
6.2.3 CES 2024C 40
6.2.4 CES 2024F 40
6.2.5 CER 2000 series / CES 2000 series Status LED 41
6.3 Modes of Operation 42
6.4 Module Validation Level 42
7 Roles 43
8 Services 44
8.1 User Role Services 47
8.1.1 SSHv2 47
8.1.2 HTTPS 48
8.1.3 SNMP 48
8.1.4 Console 49
8.1.5 NTP 49
8.2 Port Configuration Administrator Role Services 50
8.2.1 SSHv2 50
8.2.2 HTTPS 50
8.2.3 SNMP 50
8.2.4 Console 50
8.2.5 NTP 50
8.3 Crypto-officer Role Services 51
8.3.1 SSHv2 51
8.3.2 SCP 51
8.3.3 HTTPS 51
8.3.4 SNMP 51
8.3.5 Console 51
8.3.6 NTP 52
8.4 MACsec Peer Role Services 52
8.4.1 MACsec 52
8.5 IKEv2/IPsec Peer Role Services 52
8.5.1 IKEv2/IPsec Negotiation – IPsec Traffic 52
8.6 Non-Approved Mode Services 53
8.6.1 Non-Approved Algorithms 56
9 Algorithm certificates 57
9.1 Algorithm certificates in MLXe 57
9.2 Algorithm certificates in CER 2000 series / CES 2000 series 61
9.3 non-Approved but allowed cryptographic methods 61

10 Policies 62
10.1 Security Rules 62
10.1.1 Cryptographic Module Operational Rules 65
10.2 Authentication 66
10.2.1 Line Authentication Method 66
10.2.2 Enable Authentication Method 66
10.2.3 Local Authentication Method 66
10.2.4 RADIUS Authentication Method 67
10.2.5 TACACS+ Authentication Method 67
10.2.6 Strength of Authentication 68
10.2.6.1 MACsec Peer Role (only applicable to MLXe) 68
10.2.6.2 IKEv2/IPsec Peer Role (only applicable to MLXe) 68
10.2.6.3 All other roles 68
10.3 Access Control and Critical Security Parameters (CSPs) 70
10.3.1 CSP Zeroization 78
10.4 Physical Security 79
11 Crypto-officer Guidance 80
11.1 FIPS Approved Mode Status 80
11.2 FIPS Approved Mode 82
11.2.1 Invoking FIPS Approved Mode 82
11.2.1.1 Invoking FIPS Approved Mode for Brocade MLXe Series Devices 82
11.2.1.2 Invoking FIPS Approved Mode for Brocade CER 2000 series and CES 2000 series Devices 83
11.2.2 Negating FIPS Approved Mode 84
11.2.2.1 Negating FIPS Approved Mode for Brocade MLXe Series Devices 84
11.2.2.2 Negating FIPS Approved Mode for Brocade CER 2000 Series and CES 2000 Series Devices 84
12 Mitigation of other attacks 85
13 Glossary 86
14 Appendix A: Tamper Evident Seal Application Procedure 87
14.1 Brocade MLXe devices 87
14.1.1 MLXe-4 device 87
14.1.2 MLXe-8 device 89
14.1.3 MLXe-16 device 91
14.1.4 MLXe-32 device 93
14.1 Brocade CER 2000 series 104
14.1.1 CER 2024C-4X-RT devices 104
14.1.2 CER 2024F-4X-RT devices 107
14.2 Brocade CES 2000 series devices 110
14.2.1 CES 2024C-4X devices 110

14.2.2 CES 2024F-4X devices ... 112
15 Appendix B: Critical Security Parameters ... 115
15.1 Authentication Key ... 115
15.2 KDF ... 117
15.3 Line card (LP) DRBG ... 120
15.4 Management card (MP) DRBG ... 121
15.5 Private Keys ... 122
15.6 Public Keys ... 126
15.7 Session Keys ... 131
15.8 Shared Secret ... 133

Table of tables:

Table 1 - Overview – NetIron devices – The Physical Form Factor comparison 14
Table 2 - Overview – NetIron devices – Support for IPSec, MACsec and HTTPS features 15
Table 3 - Overview –MLXe product interface line card support for IPSec and MACsec features 15
Table 4 - Overview – Power Supply support for MLXe products 16
Table 5 - Overview – Power Supply support for CER 2000 series and CES 2000 series products 16
Table 6 - Overview – Port Physical Layer interface for CER 2000 series and CES 2000 series products 17
Table 7 - MLXe Series Firmware Version 19
Table 8 - MLXe Series (bundled SKU) Part Numbers 19
Table 9 - MLXe Management Card Part Numbers for MLXe-4, MLXe-8 and MLXe-16 20
Table 10 - MLXe Management Card Part Numbers for MLXe-32 20
Table 11 - MLXe Interface Line Card Part Numbers for all MLXe products (MLXe-4, MLXe-8, MLXe-16 and MLXe-32) 21
Table 12 - MLXe Switch Fabric Module Part Number for MLXe-4 22
Table 13 - MLXe Switch Fabric Module Part Number for MLXe-8 and MLXe-16 22
Table 14 - MLXe Switch Fabric Module Part Number for MLXe-32 22
Table 15 - MLXe Power Supply Module Part Numbers for MLXe-4, MLXe-8 and MLXe-16 23
Table 16 - MLXe Power Supply Module Part Numbers for MLXe-32 23
Table 17 - MLXe Fan Module Part Number for MLXe-4 23
Table 18 - MLXe Fan Module Part Number for MLXe-8 23
Table 19 - MLXe Fan Module Part Number for MLXe-16 23
Table 20 - MLXe Fan Module Part Number for MLXe-32 23
Table 21 - MLXe Switch Fabric Module Blank Filler Panel Part Numbers for MLXe-4 24
Table 22 - MLXe Switch Fabric Module Blank Filler Panel Part Number for MLXe-8, MLXe-16 and MLXe-32 24
Table 23 - MLXe Power Supply Blank Filler Panel Part Numbers for MLXe-4 24
Table 24 - MLXe Power Supply Blank Filler Panel Part Numbers for MLXe-8, MLXe-16 and MLXe-32 24
Table 25 - MLXe Management card Blank Filler Panel Part Numbers for MLXe-4, MLXe-8, MLXe-16 and MLXe-32 ... 24
Table 26 - MLXe Interface card Blank Filler Panel Part Numbers for MLXe-4, MLXe-8, MLXe-16 and MLXe-32 24
Table 27 - Validated MLXe Configurations 25
Table 28 - CER 2000 series Firmware Version 32
Table 29 - CER 2000 series Part Numbers 32
Table 30 - CER 2000 series Power Supply Module Part Numbers 32
Table 31 - CER 2000 Software License 32
Table 32 - Validated CER 2000 series Configuration 32
Table 33 - CES 2000 series Firmware Version 34
Table 34 - CES 2000 series Part Numbers 34
Table 35 - CES 2000 series Power Supply Module Part Numbers 34

Table 36 - Validated CES 2000 series Configuration 34

Table 37 - Physical/Logical Interface Correspondence 36

Table 38 - Power and status LEDs for BR-MLX-10GX20-M, BR-MLX-10GX20-X2, BR-MLX-1GX20-U10G-M, BR-MLX-1GX20-U10G-X2 and BR-MLX-10GX4-IPSEC-M Interface Line cards 38

Table 39 - Power and fan status LEDs for the MR2 Management Module 39

Table 40 - Power and fan status LEDs for the CER 2000 series and CES 2000 series models 41

Table 41 - NetIron Security Levels 42

Table 42 - List of Roles supported in NetIron firmware 43

Table 43 - List of services in Approved mode of operation 45

Table 44 - FIPS Approved Cryptographic Functions 45

Table 45 - Non-Approved Cryptographic Functions Allowed in FIPS Approved Mode 46

Table 46 - Functions/Services, Roles in Non-Approved Mode Services 55

Table 47 - Algorithm Certificates for the MLXe Series 58

Table 48 - Algorithm Certificates for BR-MLX-10GX20-M, BR-MLX-10GX20-X2, BR-MLX-1GX20-U10G-M and BR-MLX-1GX20-U10G-X2 interface line cards 58

Table 49 - Algorithm Certificates for BR-MLX-10GX4-IPSEC-M interface line cards 60

Table 50 - Algorithm Certificates for CER 2000 series / CES 2000 series 61

Table 51 - Power-Up Self-Tests - Cryptographic Known Answer Tests (KAT) 63

Table 52 - Conditional Self-Tests 64

Table 53 - Access Control Policy and Critical Security Parameters (CSPs) 75

Table 54 - MACsec and IPSec Access Control Policy and Critical Security Parameters (CSPs) 77

Table 55 - Inspection of Physical Security Mechanisms 79

Table 56 - Sample output - MLXe in non-Approved mode 80

Table 57 - Sample output – CES/CER in non-Approved mode 80

Table 58 - Sample output - MLXe in FIPS Approved mode 81

Table 59 - Sample output – CES/CER in FIPS Approved mode 81

Table 60 - Mitigation of other attacks 85

Table 61 - Glossary 86

Table 62 - Acronyms used in appendix B 115

Table of figures:

Figure 1 - Block Diagram 18

Figure 2 – Brocade MLXe-4 26

Figure 3 – Brocade MLXe-4: Starting from left to right clockwise: Left side, Rear side, Bottom side, Top side, and Right side 26

Figure 4 – Brocade MLXe-8 front view 27

Figure 5 – Brocade MLXe-8: Starting from left to right clockwise: Left side, Rear side, Bottom side, Top side, and Right side 27

Figure 6 – Brocade MLXe-16 – front view 28

Figure 7 – Brocade MLXe-16: Starting from left to right clockwise: Left side, Rear side, Bottom side, Top side, and Right side 29

Figure 8 – Brocade MLXe-32 – front view 30

Figure 9 – Brocade MLXe-32: Starting from left to right clockwise: Front side, Left side, Rear side, Right side, Bottom side, and Top side 31

Figure 10 - BR-CER-2024F-4X-RT-AC with Base: BR-CER-2024F-4X-RT-AC and License: SW-CER-2024-RTUPG 33

Figure 11 - BR-CER-2024F-4X-RT-AC backside with Power supply RPS9 (AC Power Supply) 33

Figure 12 - BR-CER-2024C-4X-RT-AC with Base: BR-CER-2024C-4X-RT-AC and License: SW-CER-2024-RTUPG 33

Figure 13 - BR-CER-2024C-4X-RT-AC backside with Power supply RPS9 (AC Power Supply) 33

Figure 14 - Front view of BR-CES-2024C-4X-AC 35

Figure 15 - BR-CES-2024C-4X-AC backside with Power supply: RPS9 (AC Power supply) 35

Figure 16 - Front view of BR-CES-2024F-4X-AC 35

Figure 17 - BR-CES-2024F-4X-AC backside with Power supply: RPS9 (AC Power supply) 35

Figure 18 - Front view of Brocade MLXe-4 with security seals 87

Figure 19 - Rear view of Brocade MLXe-4 device with security seals 88

Figure 20 - Front view of Brocade MLXe-8 device with security seals 89

Figure 21 - Rear view of Brocade MLXe-8 device with security seals 90

Figure 22 - Front view of Brocade MLXe-16 device with security seals 91

Figure 23 - Rear view of Brocade MLXe-16 device with security seals 92

Figure 24 - Front overview of MLXe-32 Configuration 1 with tamper labels 94

Figure 25 - Front upper chassis of MLXe-32 Configuration 1 with tamper labels 95

Figure 26 - Front middle chassis (grill) of MLXe-32 Configuration 1 with tamper labels 95

Figure 27 - Front lower chassis of MLXe-32 Configuration 1 with tamper labels 96

Figure 28 - Front overview of MLXe-32 Configuration 2 with tamper labels 97

Figure 29 - Front overview of MLXe-32 Configuration 2 with tamper labels 98

Figure 30 - Front middle chassis (grill) of MLXe-32 Configuration 2 with tamper labels 98

Figure 31 - Front lower chassis of MLXe-32 Configuration 2 with tamper labels 99

Figure 32 - Label 31 example of MLXe-32 100

Figure 33 - Label 11 example of MLXe-32 100
Figure 34 - Back overview of MLXe-32 with tamper labels 101
Figure 35 - Back upper chassis of MLXe-32 with tamper labels 102
Figure 36 - Back lower chassis of MLXe-32 with tamper labels 103
Figure 37 - Top front view of Brocade CER 2024C-4X-RT device with security seals 104
Figure 38 - Right view of Brocade CER 2024C-4X-RT device with security seals 105
Figure 39 - Left side view of Brocade CER 2024C-4X-RT device with security seals 105
Figure 40 - Rear view of Brocade CER 2024C-4X-RT device with security seals 106
Figure 41 - Bottom view of Brocade CER 2024C-4X-RT device with security seals 106
Figure 42 - Top front view of Brocade CER 2024F-4X-RT device with security seals 107
Figure 43 - Right side view of Brocade CER 2024F-4X-RT device with security seals 108
Figure 44 - Left side view of Brocade CER 2024F-4X-RT device with security seals 108
Figure 45 - Rear view of Brocade CER 2024F-4X-RT device with security seals 108
Figure 46 - Bottom view of Brocade CER 2024F-4X-RT device with security seals 109
Figure 47 - Top front view of Brocade CES 2024C-4X device with security seals 110
Figure 48 - Right side view of Brocade CES 2024C-4X device with security seals 110
Figure 49 - Left side view of Brocade CES 2024C-4X device with security seals 111
Figure 50 - Rear view of Brocade CES 2024C-4X device with security seals 111
Figure 51 - Bottom view of Brocade CES 2024C-4X device with security seals 112
Figure 52 - Top front view of Brocade CES 2024F-4X device with security seals 113
Figure 53 - Right side view of Brocade CES 2024F-4X device with security seals 113
Figure 54 - Left side view of Brocade CES 2024F-4X device with security seals 113
Figure 55 - Rear side view of Brocade CES 2024F-4X device with security seals 114
Figure 56 - Bottom view of Brocade CES 2024F-4X device with security seals 114

1 Introduction

Brocade MLXe Series routers feature industry-leading 100 Gigabit Ethernet (GbE), 10 GbE, 40 GbE, and 1 GbE wire speed density; rich IPv4, IPv6, IPSec, Multi-VRF, MPLS, and Carrier Ethernet capabilities without compromising performance; and advanced Layer 2 switching with built in MACsec capability. Built upon Brocade's sixth-generation architecture and terabit- scale switch fabrics, the Brocade MLXe Series has a proven heritage with more than 13,000 routers deployed worldwide. Internet Service Providers (ISPs), transit networks, Content Delivery Networks (CDNs), hosting providers, and Internet Exchange Points (IXPs) rely on these routers to meet skyrocketing traffic requirements and reduce the cost per bit. By leveraging the Brocade MLXe Series, mission-critical data centers can support more traffic, achieve greater virtualization, and provide cloud services using less infrastructure—thereby simplifying operations and reducing costs. Moreover, the Brocade MLXe Series can reduce complexity in large campus networks by collapsing core and aggregation layers, as well as providing connectivity between sites using MPLS/VPLS. The IPsec supported interface card has built-in capability to negotiate IKEv2 sessions and establish IPSec tunnels to allow Virtual Private Networks (VPN) to be created within the network. The interface line cards supporting MACsec protocol allows users to setup secure MACsec tunnels at wire-speed.

The Brocade NetIron CER 2000 series is a family of compact 1U routers that are purpose-built for high-performance Ethernet edge routing, as well as providing connectivity between sites using MPLS/VPLS. These fixed-form routers can store a complete Internet table and support advanced MPLS features such as Traffic Engineering and VPLS. They are ideal for supporting a wide range of applications in Metro Ethernet, data center and campus networks. The NetIron CER 2000 series is available in 24-port 1 Gigabit Ethernet (GbE) copper and hybrid fiber configurations with two optional 10 GbE uplink ports. To help ensure high performance, all the ports are capable of forwarding IP and MPLS packets at wire speed without oversubscription. With less than 5 watts/Gbps of power consumption, service providers can push up to 136 Gbps of triple-play services through the NetIron CER 2000 series while reducing their carbon footprint.

The Brocade NetIron CES 2000 series is a family of compact 1U, multiservice edge/aggregation switches that combine powerful capabilities with high performance and availability. The switches provide a broad set of advanced Layer 2, IPv4, IPv6, and MPLS capabilities in the same device. As a result, they support a diverse set of applications in metro edge, service provider, mobile backhaul wholesale, data center, and large enterprise networks.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

2 Overview

Brocade routers provide high-performance routing to service providers, metro topologies, and Internet Exchange Points. Each router is a multi-chip standalone cryptographic module. Each device has an opaque enclosure with tamper detection tape for detecting any unauthorized physical access to the device. The Brocade NetIron family of products include both chassis and fixed-port devices.

2.1 Brocade MLXe

Brocade MLXe series devices are chassis devices. Each MLXe chassis contains slots for management cards (also known as management modules, see Table 9), Switch Fabric Module (SFM; see Table 12), and interface line cards (see, Table 11). The SFM pass data packets between the various line cards. The interface line cards forward data packets with or without any cryptographic operations. The same interface line cards can perform some cryptographic operations on the control packet and pass it to the management card for further processing. The management cards also are able to perform cryptographic operations on control packets and forward them to interface line cards.

The cryptographic boundary of a Brocade MLXe series device includes the following components:

- A MLXe chassis
- Two management cards (see Table 9);
  - One management card runs in active mode while the other is in standby mode.
- One or more Switch Fabric Modules (SFM, see Table 12)
- One or more interface line cards (also, referred to as interface modules; see, Table 11)
- The fan tray assemblies
  - The fan assemblies can be replaced in the field.
- The power supplies
  - The power supplies can be replaced in the field.
- NOTE: All unpopulated management card slot, switch fabric module slots and interface line card slots are covered by opaque filler panels, which are part of the cryptographic boundary.

2.2 Brocade CER 2000 series /CES 2000 series

The cryptographic boundary of a Brocade CER 2000 series / CES 2000 series device includes the following components:

- The outer perimeter of the metal chassis, including the removable cover and pre-installed fan assembly.
- The power supplies

NOTE: The CER 2000 series and CES 2000 series are fixed-port devices

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

2.3 Tamper Evident Seal Application requirement

For an MLXe, CER 2000 series and CES 2000 series to operate as a validated cryptographic module, the tamper evident seals supplied in Brocade XBR-000195 must be installed as defined in section, 14 - Appendix A: Tamper Evident Seal Application Procedure.

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

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

2.4 Differences in features and services across NetIron Hardware family

This section provides a top level overview of features and services unique to specific NetIron hardware platforms. Additional details about some of these services may be found in this document or other reference documents on myBrocade.com.

2.4.1 Physical Form Factor, Support for Interface Line Cards and Port Counts

Brocade MLXe product is a chassis based product. Configuration of this product can expand (limited to the number of slots available) depending on the number and specific interface line cards installed.

CER 2000 series is a fixed form factor device which provides fixed number of specific network traffic ports.

CES 2000 series is a fixed form factor device which provides fixed number of specific network traffic ports.

Product Family	Interface Line Card(s)	Number of ports
MLXe series	☑ Supports interface line cards	Total port count depends on the number of ports per interface line card and the number of interface line cards installed in the chassis.
CER 2000 series	No support for interface line cards.	Fixed number of ports. See, specific model description.
CES 2000 series	No support for interface line cards.	Fixed number of ports. See, specific model description.

Table 1 - Overview – NetIron devices – The Physical Form Factor comparison

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

2.4.2 IPSec, MACsec and HTTPS service support comparison

Tables below show the support for IPSec, MACsec, HTTPS Server services across NetIron product families.

Depending on the type of interface line cards installed and configured in an MLXe chassis, Brocade MLXe product supports all services mentioned in this section.

CER 2000 series models do not support any of the services mentioned in this section.

CES 2000 series models do not support any of the services mentioned in this section.

All other NetIron features and services, beyond IPSec, MACsec and HTTP Server, are supported on all NetIron products.

Product Family	Support for IPSec service	Support for MACsec service	Support for HTTPS Service
MLXe series	☑ Supports IPSec feature on the IPSec capable interface line cards	☑ Supports MACsec feature on the MACsec capable interface line cards	☑ Provides HTTPS Server support on the management cards
CER 2000 series	Does not support IPSec service	Does not support MACsec service	Does not support HTTPS service
CES 2000 series	Does not support IPSec service	Does not support MACsec service	Does not support HTTPS service

Table 2 - Overview – NetIron devices – Support for IPSec, MACsec and HTTPS features

Table below shows the specific MLXe interface line cards that support IPsec and MACsec features (see Table 11 for more information on MLXe interface Line Cards):

Product Family	Interface Line Card	Support for IPSec	Support for MACsec
MLXe series	**BR-MLX-10GX4-IPSEC-M**	☑ This interface line card supports IPsec feature	☑ This interface line card supports MACsec feature
	BR-MLX-10GX20-M	NOT APPLICABLE: This interface line card does not support IPSec feature	☑ This interface line card supports MACsec feature
	BR-MLX-1GX20-U10G-M	NOT APPLICABLE: This interface line card does not support IPSec feature	☑ This interface line card supports MACsec feature
	BR-MLX-10GX20-X2	NOT APPLICABLE: This interface line card does not support IPSec feature	☑ This interface line card supports MACsec feature
	BR-MLX-1GX20-U10G-X2	NOT APPLICABLE: This interface line card does not support IPSec feature	☑ This interface line card supports MACsec feature

Table 3 - Overview –MLXe product interface line card support for IPSec and MACsec features

2.4.3 Power Supply support

Tables below show the available power supply support for MLXe, CER 2000 series and CES 2000 series product families.

		MLXe Power Supplies			
Product Family		BR-MLXE-ACPWR-1800 power supply	BR-MLXE-DCPWR-1800 power supply	BR-MLXE-32-ACPWR-3000 power supply	BR-MLXE-32-DCPWR-3000 power supply
MLXe series	**MLXe-4**	AC	DC	N/A	
	MLXe-8				
	MLXe-16				
	MLXe-32	N/A		AC	DC

Table 4 - Overview – Power Supply support for MLXe products

	CER 2000 series and CES 2000 series Power Supplies	
Product Family	RPS9 power supply	RPS9DC power supply
CER 2000 series	AC	DC
CES 2000 series	AC	DC

Table 5 - Overview – Power Supply support for CER 2000 series and CES 2000 series products

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

2.4.4 Physical Layer interface for ports CER 2000 series / CES 2000 series

Table below shows the available variations for optical and electrical interface network ports (physical layer connection) for CER 2000 series and CES 2000 series product families.

	CER 2000 series Models				CES 2000 series Models			
Physical interface for Network ports	BR-CER-2024**C**-4X-RT-AC	BR-CER-2024**C**-4X-RT-DC	BR-CER-2024**F**-4X-RT-AC	BR-CER-2024**F**-4X-RT-DC	BR-CES-2024**C**-4X-AC	BR-CES-2024**C**-4X-DC	BR-CES-2024**F**-4X-AC	BR-CES-2024**F**-4X-DC
Optical (**fiber**)	*N/A*		☑ Provides Optical network interface ports		*N/A*		☑ Provides Optical network interface ports	
Electrical (**Copper**)	☑ Provides Electrical network interface ports		*N/A*		☑ Provides Electrical network interface ports		*N/A*	

Table 6 - Overview – Port Physical Layer interface for CER 2000 series and CES 2000 series products

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

2.5 Block Diagram

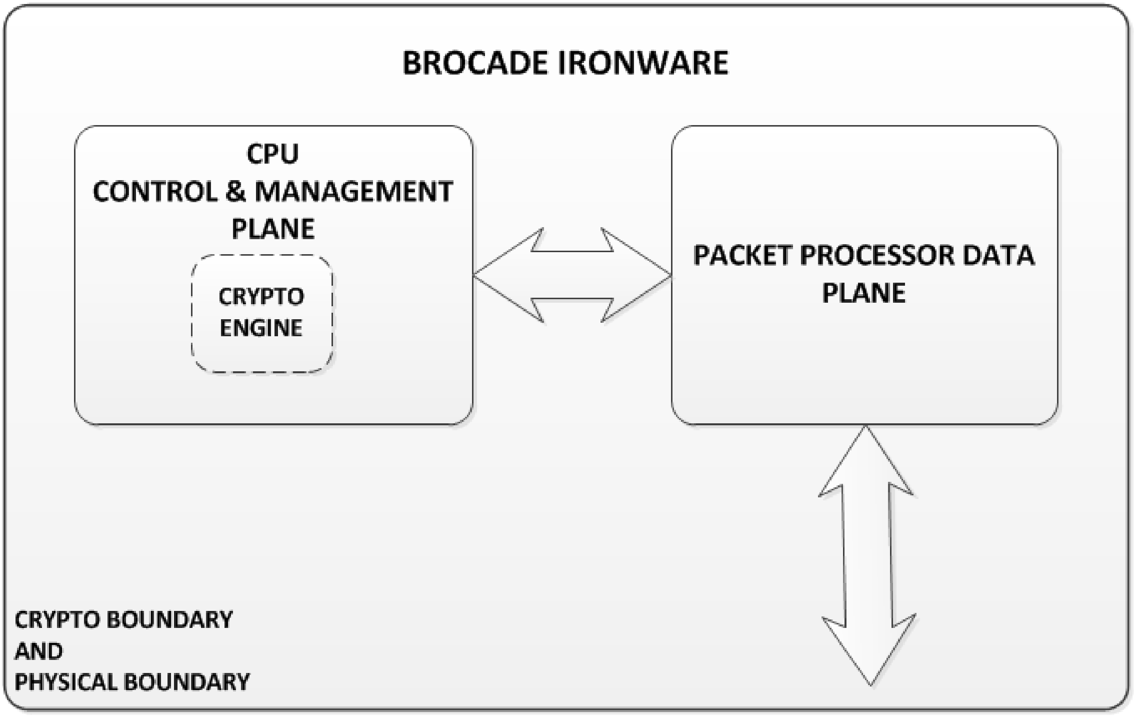

Figure 1 - Block Diagram

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

3 Brocade MLXe series

Table below identifies the firmware version for MLXe series:

Firmware
Multi-Service IronWare R05.9.00aa

Table 7 - MLXe Series Firmware Version

3.1 MLXe bundled SKUs

Table below lists all bundled SKUs which includes all the essential components to create an MLXe configuration. These bundled configurations then can be customized further using contents described in Table 8 through Table 21. Note that Table 27 describes the validated configurations.

SKU	MFG Part Number	Brief Description
BR-MLXE-4-MR2-X-AC	P/N: 80-1006874-03	Brocade MLXe-4, AC system with 1 MR2 (X) management card, 2 high speed switch fabric modules, 1 1800W AC power supply, 4 exhaust fan assembly kits and air filter. Power cord not included.
BR-MLXE-8-MR2-M-AC	P/N: 80-1007225-01	Brocade MLXe-8 AC system with 1 MR2 (M) management card, 2 high speed switch fabric modules, 2 1800W AC power supplies, 2 exhaust fan assembly kits and air filter. Power cord not included.
BR-MLXE-16-MR2-M-AC	P/N: 80-1006827-02	Brocade MLXe-16 AC system with 1 MR2 (M) management card, 3 high speed switch fabric modules, 4 1800W AC power supplies, 2 exhaust fan assembly kits and air filter. Power cord not included.
BR-MLXE-32-MR2-M-AC	P/N: 80-1007253-04	Brocade MLXe-32 AC system with 1 MR2 (M) management card, 7 high speed switch fabric modules, 4 3000W AC power supplies, 10 exhaust fan assembly kits and air filter. Power cord not included
BR-MLXE-32-MR2-X-AC	P/N: 80-1007255-04	Brocade MLXe-32 AC system with 1 XMR MR2 (X) management card, 7 high speed switch fabric modules, 4 3000W AC power supplies, 10 exhaust fan assembly kits and air filter. Power cord not included.

Table 8 - MLXe Series (bundled SKU) Part Numbers

NEXT PAGE →

3.2 MLXe Management cards SKUs

Table 9 and Table 10 below lists all management cards (BR-MLX-MR2-M/X and BR-MLX-32-MR2-M/X) used in MLXe series products. These management cards are grouped together based on two groups of:

1. MLXe-4, MLXe-8, MLXe-16 chassis and
2. MLXe-32 chassis

SKU	MFG Part Number	Brief Description
BR-MLX-MR2-M	P/N: 80-1005643-01	Brocade MLX system management (M) card, 4 GB SDRAM, 2 GB internal compact flash, external compact flash slot, EIA/TIA-232 and 10/100/1000 Ethernet ports for out-of-band management.
BR-MLX-MR2-X	P/N: 80-1005644-03	MLXe/XMR Gen2 management (X) card for 4-slot, 8-slot and 16-slot systems. Includes 4 GB RAM, 1 internal compact flash drive (2GB), 1 external compact flash slot with included 2GB card, RS-232 serial console port and 10/100/1000 Ethernet port for management.

Table 9 - MLXe Management Card Part Numbers for MLXe-4, MLXe-8 and MLXe-16

SKU	MFG Part Number	Brief Description
BR-MLX-32-MR2-M	P/N: 80-1005641-02	MLXe/MLX Gen2 management (M) card for 32-slot systems, 4 GB SDRAM, 2 GB internal compact flash, external compact flash slot, EIA/TIA-232 and 10/100/1000 Ethernet ports for out-of-band management.
BR-MLX-32-MR2-X	P/N: 80-1005642-03	MLXe/MLX Gen2 management (X) card for 32-slot systems. Includes 4 GB RAM, 1 internal compact flash drive (2GB), 1 external compact flash slot with included 2GB card, RS-232 serial console port and 10/100/1000 Ethernet port for management.

Table 10 - MLXe Management Card Part Numbers for MLXe-32

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

3.3 MLXe Interface cards SKUs

Table below lists all interface cards used in MLXe products (MLXe-4, MLXe-8, MLXe-16 and MLXe-32):

SKU	MFG Part Number	Brief Description
BR-MLX-10GX20-M	P/N:80-1007878-02	Brocade MLXe twenty (20)-port 10-GBE/1-GBE (M) combo interface line card with IPv4/IPv6/MPLS hardware support. Requires SFP+ and SFP optics. Supports 512K IPv4 routes in FIB. Requires high speed switch fabric modules
BR-MLX-10GX20-X2	P/N:80-1007911-02	Brocade MLXe twenty (20)-port 10-GBE/1-GBE (X2) combo interface line card with IPv4/IPv6/MPLS hardware support. Requires SFP+ and SFP optics. Supports simultaneous 2M IPv4 and 0.8M IPv6, or simultaneous 1.5M IPv4 and 1M IPv6 routes in FIB. Requires hSFM.
BR-MLX-1GX20-U10G-M	P/N: 80-1008426-01	Brocade MLXe twenty (20)-port 10-GBE/1-GBE (M) combo interface line card with IPv4/IPv6/MPLS hardware support. Requires SFP+ and SFP optics. Supports 512K IPv4 routes in FIB. Requires high speed switch fabric modules
BR-MLX-1GX20-U10G-X2	P/N: 80-1008427-02	Brocade MLXe twenty (20)-port 10-GBE/1-GBE (X2) combo interface line card with IPv4/IPv6/MPLS hardware support. Requires SFP+ and SFP optics. Supports simultaneous 2M IPv4 and 0.8M IPv6, or simultaneous 1.5M IPv4 and 1M IPv6 routes in FIB. Requires hSFM
BR-MLX-10GX4-IPSEC-M	P/N:80-1007879-02	MLX 4-port 10/1 GbE and 4-port 1 GbE (M) combo IP Security (IPSEC) interface line card with 512K IPv4 or 128K IPv6 routes in hardware. It requires MR2 management card and High Speed Switch Fabric module (hSFM).

Table 11 - MLXe Interface Line Card Part Numbers for all MLXe products (MLXe-4, MLXe-8, MLXe-16 and MLXe-32)

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

3.4 MLXe Switch Fabric Modules SKUs

Table below lists switch fabric modules used in MLXe-4 product:

SKU	MFG Part Number	Brief Description
NI-X-4-HSF	P/N: 80-1003891-02	MLXe/MLX/XMR high speed switch fabric module for 4-slot chassis

Table 12 - MLXe Switch Fabric Module Part Number for MLXe-4

Table below lists switch fabric module used in MLXe-8 and MLXe-16 products:

SKU	MFG Part Number	Brief Description
NI-X-16-8-HSF	P/N: 80-1002983-01	MLXe/MLX/XMR high speed switch fabric module for 8-slot and 16-slot chassis

Table 13 - MLXe Switch Fabric Module Part Number for MLXe-8 and MLXe-16

Table below lists switch fabric module used in MLXe-32 product:

SKU	MFG Part Number	Brief Description
NI-X-32-HSF	P/N: 80-1008686-01	MLXe high speed switch fabric module for 32-slot chassis

Table 14 - MLXe Switch Fabric Module Part Number for MLXe-32

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

3.5 MLXe Power Supply SKUs

Table below lists all power supplies used in MLXe-4, MLXe-8 and MLXe-16 products:

SKU	MFG Part Number	Brief Description
BR-MLXE-ACPWR-1800	P/N: 80-1003971-01	16-slot, 8-slot and 4-slot MLXe AC 1800W power supply

Table 15 - MLXe Power Supply Module Part Numbers for MLXe-4, MLXe-8 and MLXe-16

Table below lists all power supplies used MLXe-32 product:

SKU	MFG Part Number	Brief Description
BR-MLXE-32-ACPWR-3000	P/N: 80-1003969-02	32-slot MLXe AC 3000W power supply

Table 16 - MLXe Power Supply Module Part Numbers for MLXe-32

3.6 MLXe Exhaust Fan SKUs

Table below lists exhaust fan module used in MLXe-4:

SKU	MFG Part Number	Brief Description
BR-MLXE-4-FAN	P/N: 80-1004114-01	MLXe-4 exhaust fan assembly kit

Table 17 - MLXe Fan Module Part Number for MLXe-4

Table below lists exhaust fan module used in MLXe-8:

SKU	MFG Part Number	Brief Description
BR-MLXE-8-FAN	P/N: 80-1004113-01	MLXe-8 exhaust fan assembly kit

Table 18 - MLXe Fan Module Part Number for MLXe-8

Table below lists exhaust fan module used in MLXe-16:

SKU	MFG Part Number	Brief Description
BR-MLXE-16-FAN	P/N: 80-1004112-01	MLXe-16 exhaust fan assembly kit

Table 19 - MLXe Fan Module Part Number for MLXe-16

Table below lists exhaust fan module used in MLXe-32:

SKU	MFG Part Number	Brief Description
BR-MLXE-32-FAN	P/N: 80-1004469-01	MLXe-32 exhaust fan assembly kit

Table 20 - MLXe Fan Module Part Number for MLXe-32

NEXT PAGE →

3.7 MLXe Chassis Slots Blank Filler Panel SKUs

Switch Fabric Module slots

Table below lists switch fabric module slot blank filler panel unique to MLXe-4:

SKU	MFG Part Number	Brief Description
NI-X-SF1PNL	P/N: 80-1003009-01	NetIron XMR/MLX switch fabric module blank panel for 4-slot chassis

Table 21 - MLXe Switch Fabric Module Blank Filler Panel Part Numbers for MLXe-4

Table below lists switch fabric module slot blank filler panel used in MLXe-8, MLXe-16 and MLXe-32:

SKU	MFG Part Number	Brief Description
NI-X-SF3PNL	P/N: 80-1004757-02	NetIron XMR/MLX switch fabric module blank panel

Table 22 - MLXe Switch Fabric Module Blank Filler Panel Part Number for MLXe-8, MLXe-16 and MLXe-32

Power Supply slots

Table below lists power supply slot blank filler panel unique to MLXe-4:

SKU	MFG Part Number	Brief Description
NI-X-PWRPNL-A	P/N: 80-1003053-01	NetIron XMR/MLX power supply blank panel for 4-slot chassis

Table 23 - MLXe Power Supply Blank Filler Panel Part Numbers for MLXe-4

Table below lists power supply slot blank filler panel used in MLXe-8, MLXe-16 and MLXe-32:

SKU	MFG Part Number	Brief Description
NI-X-PWRPNL	P/N: 80-1003052-01	NetIron XMR/MLX power supply blank panel for 8-slot, 16-slot and 32-slot chassis

Table 24 - MLXe Power Supply Blank Filler Panel Part Numbers for MLXe-8, MLXe-16 and MLXe-32

Management card slots

Table below lists management card slot blank filler panel for all MLXe chassis (MLXe-8, MLXe-8, MLXe-16 and MLXe-32:

SKU	MFG Part Number	Brief Description
NI-X-MPNL	P/N: 80-1004760-02	NetIron XMR/MLX Series management card blank panel

Table 25 - MLXe Management card Blank Filler Panel Part Numbers for MLXe-4, MLXe-8, MLXe-16 and MLXe-32

Interface card slots

Table below lists interface card slot blank filler panel for all MLXe chassis (MLXe-8, MLXe-8, MLXe-16 and MLXe-32:

SKU	MFG Part Number	Brief Description
NI-X-IPNL	P/N: 80-1006511-02	NetIron XMR/MLX Series interface line card blank panel

Table 26 - MLXe Interface card Blank Filler Panel Part Numbers for MLXe-4, MLXe-8, MLXe-16 and MLXe-32

3.8 Validated MLXe configuration

Validated MLXe configurations are listed below.

Chassis Model	Module Descriptions	Modules (quantities)
MLXe-4 Configuration	Bundled SKU:	BR-MLXE-4-MR2-X-AC
	Management card(s):	BR-MLX-MR2-X (1)
	Interface line card(s):	BR-MLX-10GX20-X2 (1), and BR-MLX-1GX20-U10G-X2 (1), and BR-MLX-10GX4-IPSEC-M (1)
MLXe-8 Configuration	Bundled SKU:	BR-MLXE-8-MR2-M-AC
	Management card(s):	BR-MLX-MR2-M (1)
	Interface line card(s):	BR-MLX-10GX20-M (1), and BR-MLX-10GX4-IPSEC-M (1)
MLXe-16 Configuration	Bundle SKU:	BR-MLXE-16-MR2-M-AC
	Management card(s):	BR-MLX-MR2-M (1)
	Interface line card(s):	BR-MLX-10GX20-M (1), and BR-MLX-10GX4-IPSEC-M (2)
MLXe-32 Configuration 1	Bundle SKU:	BR-MLXE-32-MR2-M-AC (1)
	Management card(s):	BR-MLX-32-MR2-M (1)
	Interface line card(s):	BR-MLX-10GX20-M (1), and BR-MLX-1GX20-U10G-M (1), and BR-MLX-10GX4-IPSEC-M (1)
	Switch Fabric module:	NI-X-32-HSF (1)
MLXe-32 Configuration 2	Bundle SKU:	BR-MLXE-32-MR2-X-AC (1)
	Management card(s):	BR-MLX-32-MR2-X (1)
	Interface line card(s):	BR-MLX-10GX20-X2 (2), and BR-MLX-1GX20-U10G-X2 (2), and BR-MLX-10GX4-IPSEC-M (1)
	Switch Fabric module:	NI-X-32-HSF (1)

Table 27 - Validated MLXe Configurations

NEXT PAGE →

3.9 MLXe-4 images

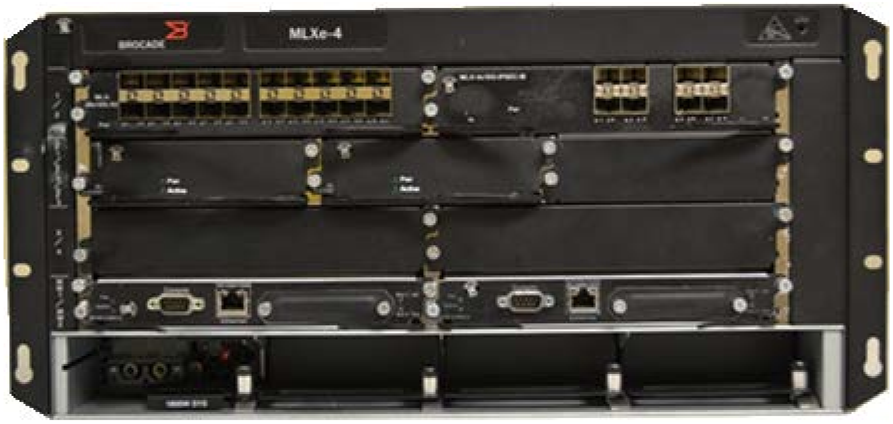

Figure 2 – Brocade MLXe-4

Note: Figure above displays a representation of the MLXe-4 cryptographic module. This is not the only possible configuration. Other possible configurations can be created by utilizing the validated configurations listed in Table 27.

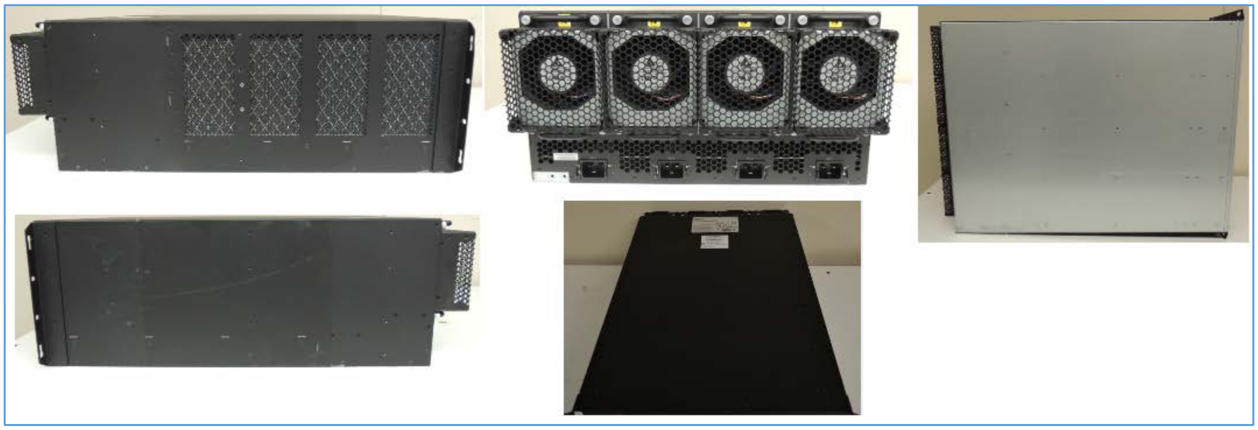

Figure 3 – Brocade MLXe-4: Starting from left to right clockwise: Left side, Rear side, Bottom side, Top side, and Right side

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

3.10 MLXe-8 images

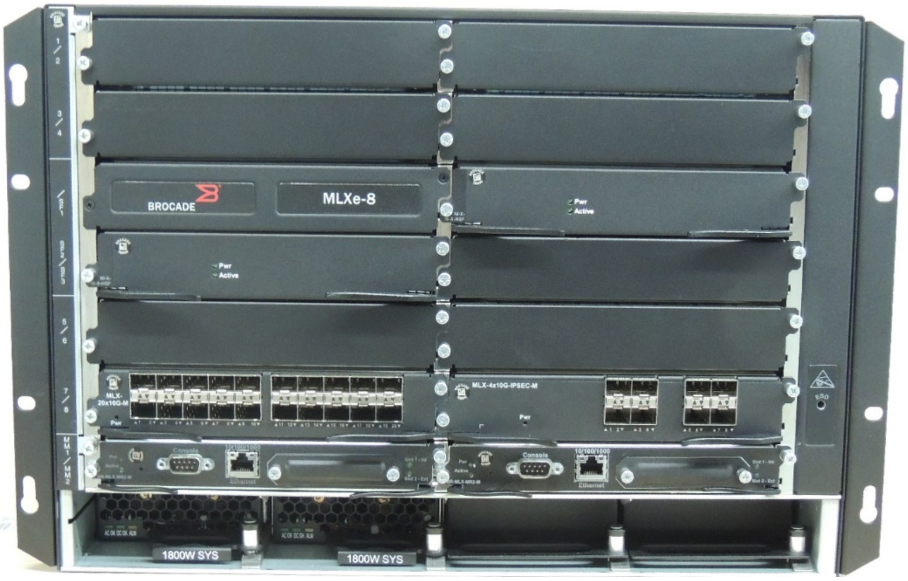

Figure 4 – Brocade MLXe-8 front view

Note: Figure above displays a representation of the MLXe-8 cryptographic module. This is not the only possible configuration. Other possible configurations can be created by utilizing the validated configurations listed in Table 27.

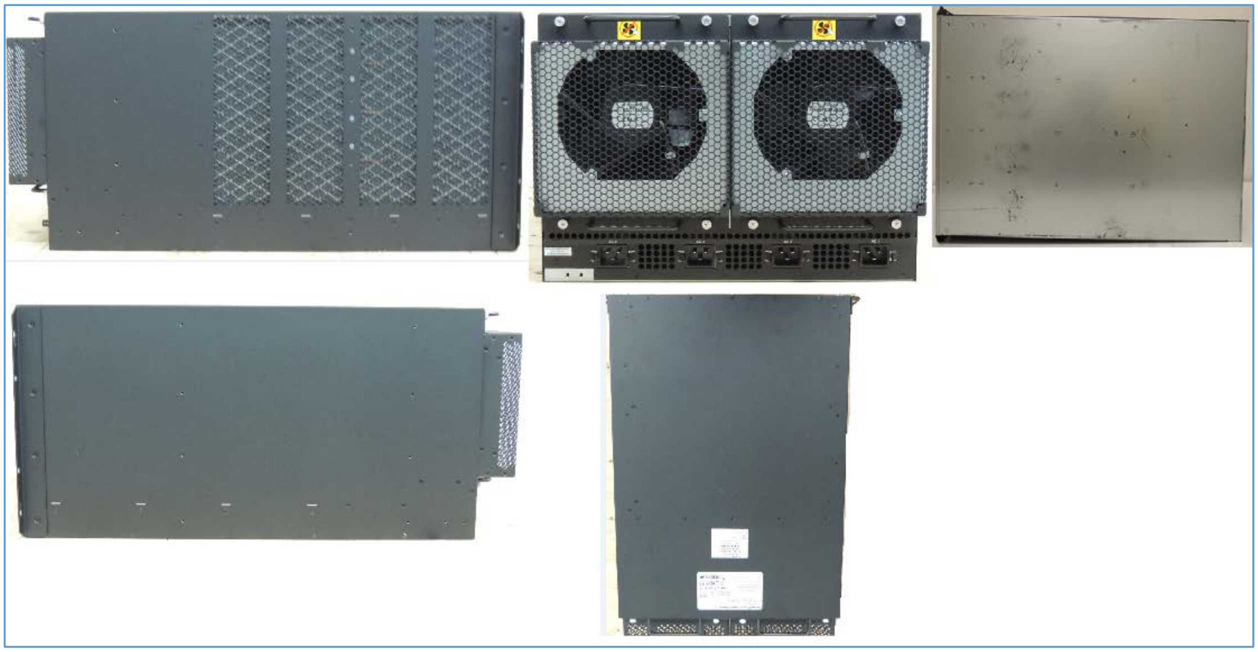

Figure 5 – Brocade MLXe-8: Starting from left to right clockwise: Left side, Rear side, Bottom side, Top side, and Right side

3.11 MLXe-16 images

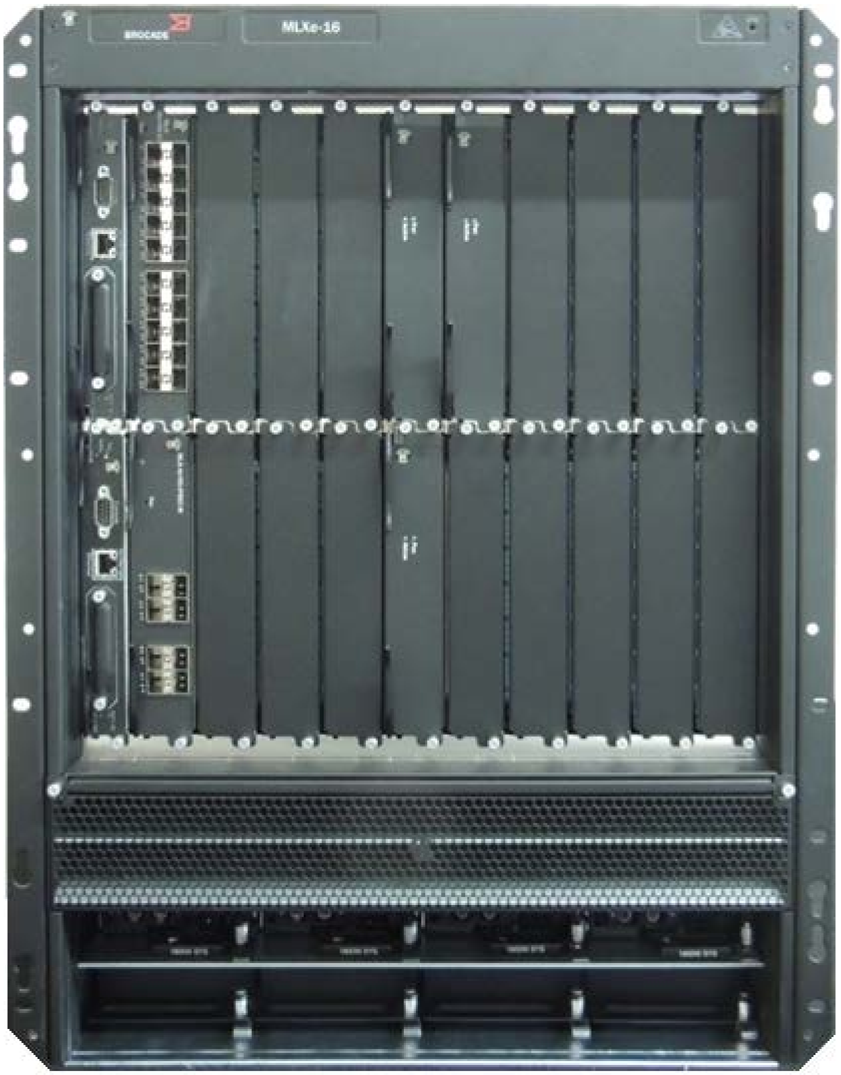

Figure 6 – Brocade MLXe-16 – front view

Note: Figure above displays a representation of the MLXe-16 cryptographic module. This is not the only possible configuration. Other possible configurations can be created by utilizing the validated configurations listed in Table 27.

NEXT PAGE →

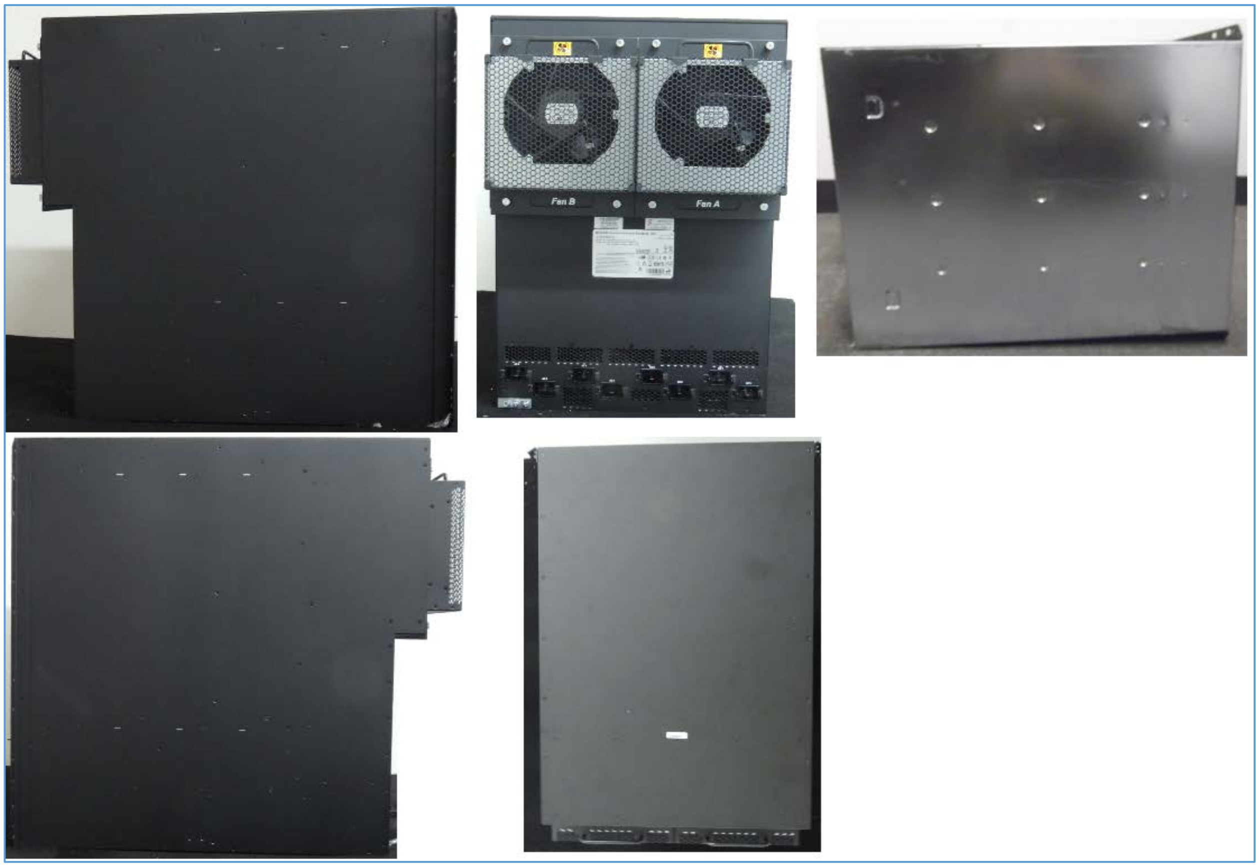

Figure 7 – Brocade MLXe-16: Starting from left to right clockwise: Left side, Rear side, Bottom side, Top side, and Right side

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

3.12 MLXe-32 images

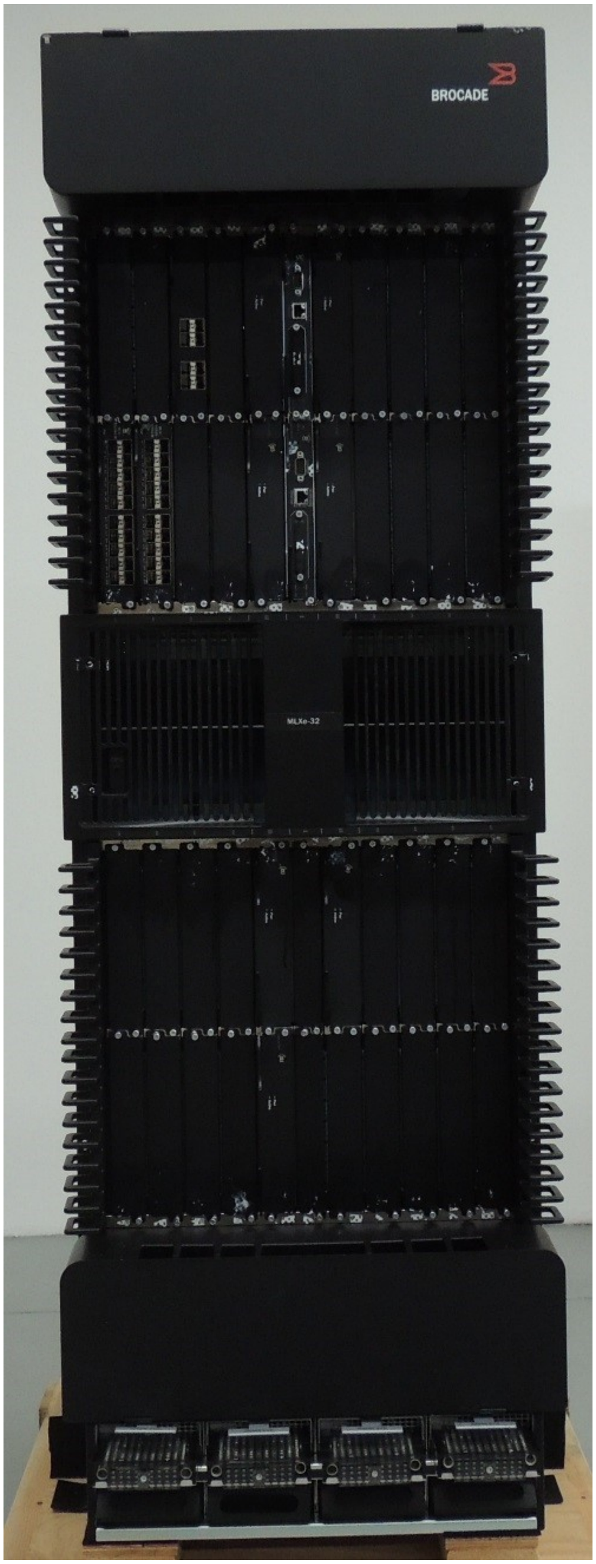

Figure 8 – Brocade MLXe-32 – front view

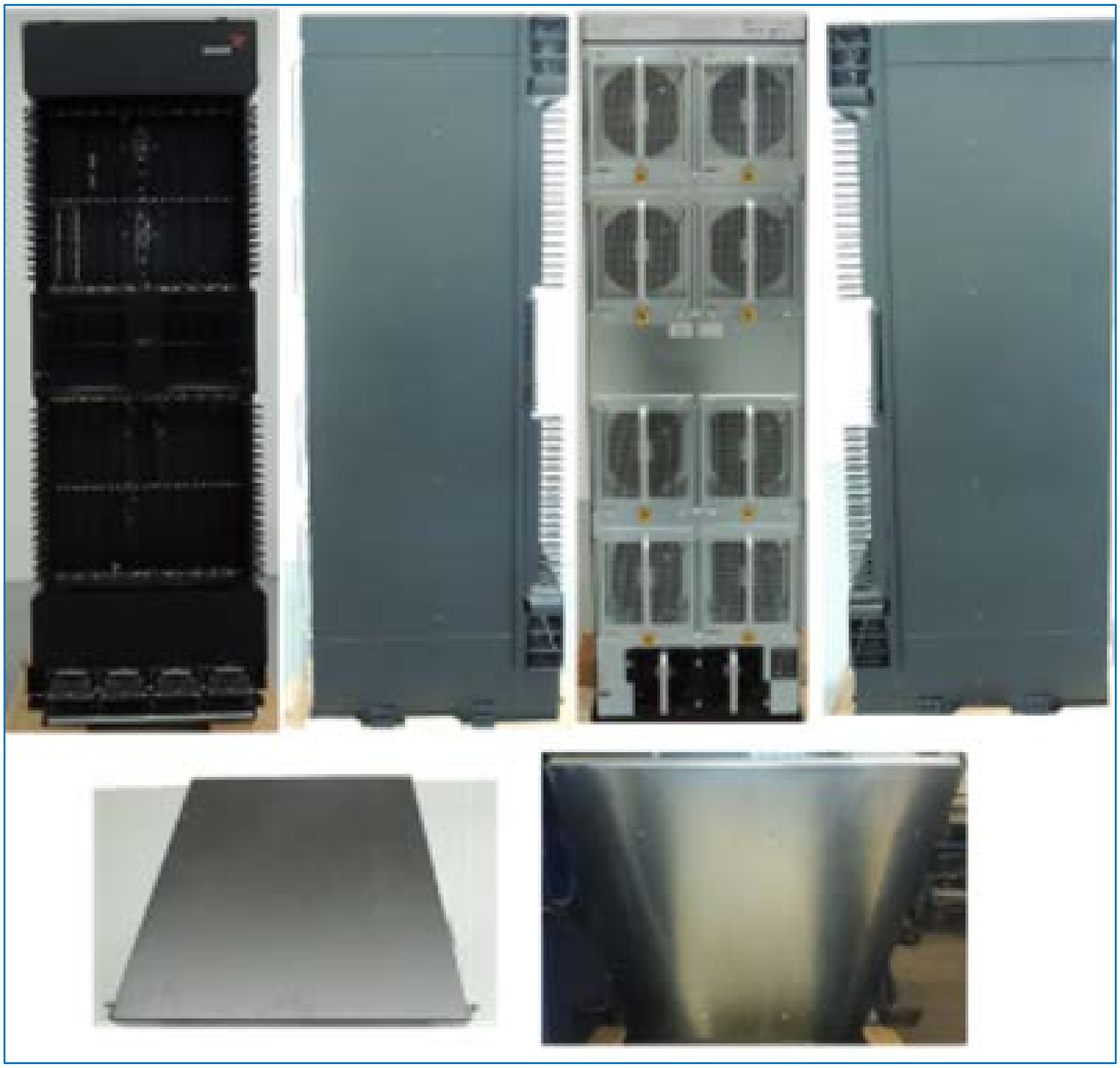

Figure 9 – Brocade MLXe-32: Starting from left to right clockwise: Front side, Left side, Rear side, Right side, Bottom side, and Top side

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

4 Brocade CER 2000 series

There are two main variations to the NetIron Carrier Ethernet Router (CER) 2000 series:

- Brocade NetIron CER Series 2024C-4X
- Brocade NetIron CER Series 2024F-4X

Firmware
Multi-Service IronWare R05.9.00aa

Table 28 - CER 2000 series Firmware Version

SKU	MFG Part Number	Brief Description
BR-CER-2024C-4X-RT-AC	P/N: 80-1006530-01	• 24 RJ45 ports of 10/100/1000 Mbps Ethernet • Uplink ports: 4 RJ45 10/100/1000 Mbps ports or 4 10GE SFP+ uplinks • 500W AC power supply (RPS9)
BR-CER-2024F-4X-RT-AC	P/N: 80-1006529-01	• 24 SFP ports of 100/1000 Mbps Ethernet • Uplink ports: 4 RJ45 10/100/1000 Mbps ports or 4 10GE SFP+ uplinks • 500W AC power supply (RPS9)

Table 29 - CER 2000 series Part Numbers

SKU	MFG Part Number	Brief Description
RPS9	P/N: 80-1003868-01	500W AC power supply for NI CER/CES series

Table 30 - CER 2000 series Power Supply Module Part Numbers

CER Model	Configuration Details
SW-CER-2024-RTUPG (P/N: 80-1004848-01)	RT software upgrade license for NetIron CER 24-port routers (NetIron CER 2024C, NetIron CER 2024F)

Table 31 - CER 2000 Software License

CER Model	Configuration Details
BR-CER-2024F-4X-RT-AC (P/N: 80-1006529-01)	Base: BR-CER-2024F-4X-RT-AC Interface line card: None / Not applicable License: SW-CER-2024-RTUPG (1) Power Supply: RPS9 (P/N: 80-1003868-01) (1)
BR-CER-2024C-4X-RT-AC (P/N: 80-1006530-01)	Base: BR-CER-2024C-4X-RT-AC Interface line card: None / Not applicable License: SW-CER-2024-RTUPG (1) Power Supply: RPS9 (P/N: 80-1003868-01) (1)

Table 32 - Validated CER 2000 series Configuration

4.1 Brocade CER 2000 images

Images of Brocade CER 2000 series models are shown below:

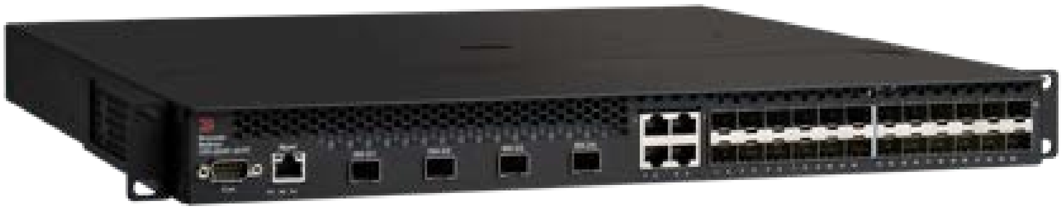

Figure 10 - BR-CER-2024F-4X-RT-AC with Base: BR-CER-2024F-4X-RT-AC and License: SW-CER-2024-RTUPG

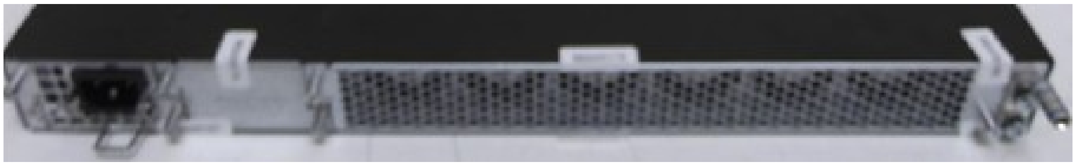

Figure 11 - BR-CER-2024F-4X-RT-AC backside with Power supply RPS9 (AC Power Supply)

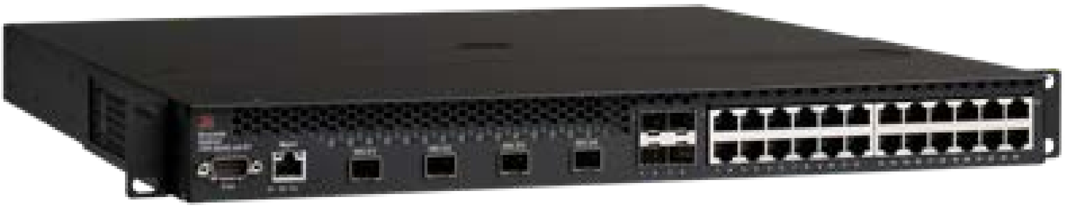

Figure 12 - BR-CER-2024C-4X-RT-AC with Base: BR-CER-2024C-4X-RT-AC and License: SW-CER-2024-RTUPG

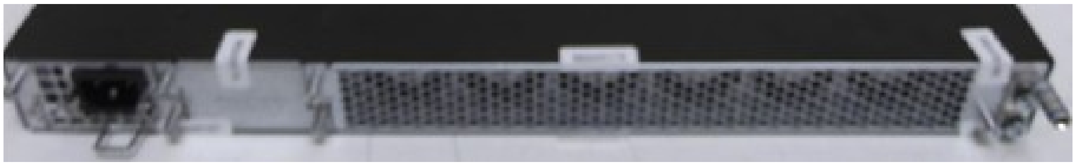

Figure 13 - BR-CER-2024C-4X-RT-AC backside with Power supply RPS9 (AC Power Supply)

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

5 Brocade CES 2000 series

There are two main variations to the NetIron Carrier Ethernet Switch (CES) 2000 Series:

- Brocade NetIron CES Series 2024C-4X
- Brocade NetIron CES Series 2024F-4X

Firmware
Multi-Service IronWare R05.9.00aa

Table 33 - CES 2000 series Firmware Version

SKU	MFG Part Number	Brief Description
BR-CES-2024C-4X-AC	P/N: 80-1000077-01	• 24 RJ45 ports of 10/100/1000 Mbps Ethernet • Uplink ports: 4 RJ45 10/100/1000 Mbps ports or 4 10GE SFP+ uplinks • 500W AC power supply (RPS9)
BR-CES-2024F-4X-AC	P/N: 80-1000037-01	• 24 SFP ports of 100/1000 Mbps Ethernet • Uplink ports: 4 RJ45 10/100/1000 Mbps ports or 4 10GE SFP+ uplinks • 500W AC power supply (RPS9)

Table 34 - CES 2000 series Part Numbers

SKU	MFG Part Number	Brief Description
RPS9	P/N: 80-1003868-01	500W AC power supply for NetIron CER/CES series

Table 35 - CES 2000 series Power Supply Module Part Numbers

CES Model	Configuration Details
BR-CES-2024C-4X-AC	Base: BR-CES-2024C-4X-AC Interface line card: None / Not Applicable Power supply: RPS9 (P/N: 80-1003868-01)(1)
BR-CES-2024F-4X-AC	Base: BR-CES-2024F-4X-AC Interface line card: None Power supply: RPS9 (P/N: 80-1003868-01)(1)

Table 36 - Validated CES 2000 series Configuration

5.1 Brocade CES 2000

Images of Brocade CES 2000 series models are shown below:

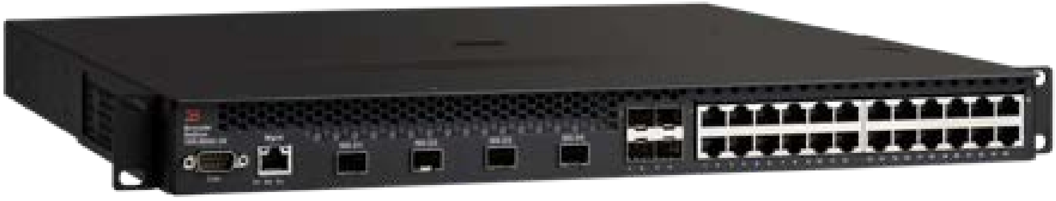

Figure 14 - Front view of BR-CES-2024C-4X-AC

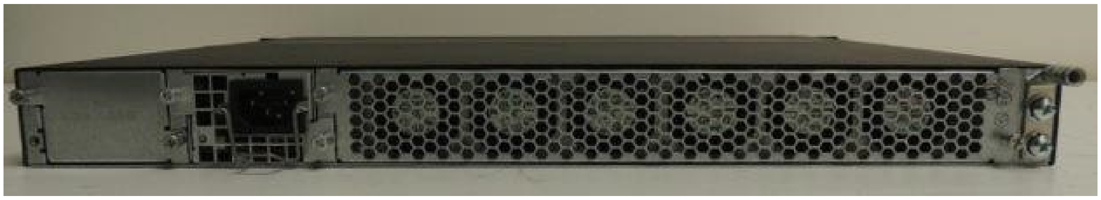

Figure 15 - BR-CES-2024C-4X-AC backside with Power supply: RPS9 (AC Power supply)

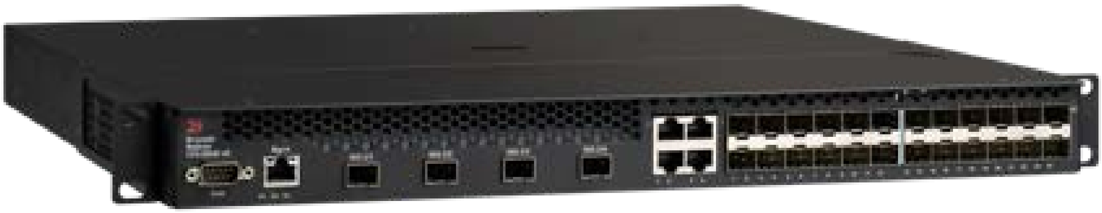

Figure 16 - Front view of BR-CES-2024F-4X-AC

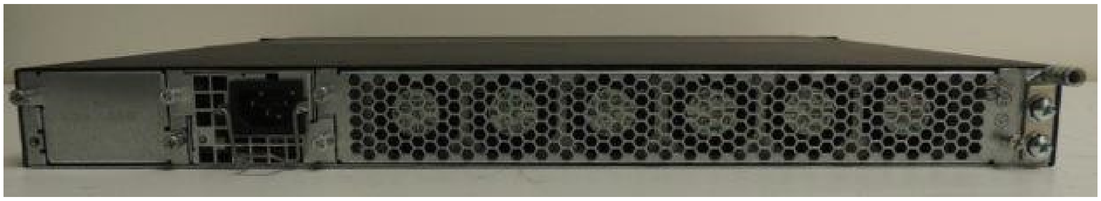

Figure 17 - BR-CES-2024F-4X-AC backside with Power supply: RPS9 (AC Power supply)

NEXT PAGE →

6 Ports and Interfaces

Each MLXe, CER 2000 series and CES 2000 series device provides Networking ports, Console, PCMCIA (MLXe only), Power plugs and status LEDs. This section describes the physical ports and the interfaces they provide for Data input, Data output, Control input, Status output and Power.

Table below shows the correspondence between the physical interfaces of NetIron devices (MLXe, CER, and CES) and logical interfaces defined in FIPS 140-2.

Physical Interface	Logical Interface
Console	**Data input**
Management Port	
Networking ports	
Console	**Data output**
Management Port	
Networking ports	
Console	**Control input**
Management Port	
Networking ports	
PCMCIA (MLXe only)	
Console	**Status output**
LEDs	
Management Port	
Networking ports	
PCMCIA (MLXe only)	
Power plugs	**Power**

Table 37 - Physical/Logical Interface Correspondence

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

6.1 Brocade MLXe series

All interface cards listed in this section are part of the FIPS validation.

6.1.1 MLXe MR2 Management Modules (Management cards)

MLXe MR2 Management Modules (Management cards) are part of the FIPS Validation as per section 3.2 (Table 9 and Table 10) and section 3.8 (Table 27) in this document. The MR2 management card provides physical ports and status indicators. The MR2's major features are listed below.

- 4 GB SDRAM
- One internal 2GB compact flash drive
- One external compact flash slot
- Console: EIA/TIA-232 port
- Management Port: 10/100/1000 Mbps Ethernet port for out-of-band management

6.1.2 BR-MLX-10GX20-M, BR-MLX-10GX20-X2, BR-MLX-1GX20-U10G-M and BR-MLX-1GX20-U10G-X2 line cards

Interface line cards referenced in this section are part of the FIPS Validation as per Section 3 of this document, Table 27.

The BR-MLX-1GX20-U10G-M, BR-MLX-1GX20-U10G-X2, BR-MLX-10GX20-M and BR-MLX-10GX20-X2 interface line cards provide physical ports and status indicators. These interface line cards' major features are listed below.

- Networking ports: 20 port 1/10GE combo port in 10GE mode
- LED indicators
- Power and status LEDs

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

6.1.3 BR-MLX-10GX4-IPSEC-M interface line card

BR-MLX-10GX4-IPSEC-M interface line card is part of the FIPS Validation as per Section 3 of this document, Table 27. The BR-MLX-10GX4-IPSEC-M interface line card provides physical ports and status indicators. This interface line card's major features are listed below.

- Networking ports: 4-port 10 GbE/1 GbE combo and 4-port 1 GbE (-M) IPsec module
- LED indicators
- Power and status LEDs

6.1.4 MLXe Status LED

Power and status LEDs for the interface line cards are described in table below (for a list of all applicable line cards see Table 9, Table 11 and Table 12).

LED	State	Meaning
Port 1 and Port 2	On or blinking	The software is currently accessing the auxiliary flash card
	Off	The software is not currently accessing the axillary flash card
Active	On	The module is functioning as the active management card
	Off	The module is functioning as the standby management card.
Pwr	On	The module is receiving power
	Off	The module is not receiving power
1/10 GbE Port (Upper right LED)	On (Green)	A link is established with a remote port
	Off	A link is not established with a remote port
1/10 GbE Port (Upper left LED)	On or blinking (Yellow)	The port is transmitting and receiving packets
	Off	The port is not transmitting or receiving packets

Table 38 - Power and status LEDs for BR-MLX-10GX20-M, BR-MLX-10GX20-X2, BR-MLX-1GX20-U10G-M, BR-MLX-1GX20-U10G-X2 and BR-MLX-10GX4-IPSEC-M Interface Line cards

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

Power and status LEDs for all Management cards are described in table below (for a list of all applicable Management cards see Table 9, MLXe Management Card Part Numbers.)

LED	State	Meaning
Slot 1(Internal) and Slot 2(External)	On or blinking	The software is currently accessing the compact flash card
	Off	The software is not currently accessing the compact flash card
Active	On	The module is functioning as the active management card
	Off	The module is functioning as the standby management card.
Pwr	On	The module is receiving power
	Off	The module is not receiving power
10/100/1000 Ethernet Port (Upper right LED)	On (Green)	A link is established with a remote port
	Off	A link is not established with a remote port
10/100/1000 Ethernet Port (Upper left LED)	On or blinking (Yellow)	The port is transmitting and receiving packets
	Off	The port is not transmitting or receiving packets

Table 39 - Power and fan status LEDs for the MR2 Management Module

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

6.2 Brocade CER 2000 series/CES 2000 series

Models in the Brocade NetIron CER 2000 series provide 24 Gigabit Ethernet ports. Models in the Brocade NetIron CES 2000 series provide 24 Gigabit Ethernet ports and four fixed 10GbE ports. Each series supports both copper and fiber connecters with some models supporting combination ports. Some models support 10 Gigabit Ethernet uplink ports. All models have an out-of-band Ethernet management port (Gigabit Ethernet RJ-45 connector) and a console management port (RJ-45 serial connector).

6.2.1 CER 2024C

- Console: EIA/TIA-232 port
- Management Port: 10/100/1000 Mbps Ethernet port for out-of-band management
- Networking ports: 24 port 1GbE copper with RJ-45
- Networking ports: 4 port 10GbE uplink fiber SFP+ or copper RJ-45 combo ports
- LED indicators
- Power and status LEDs (see section 6.2.5 for details)

6.2.2 CER 2024F

- Console: EIA/TIA-232 port
- Management Port: 10/100/1000 Mbps Ethernet port for out-of-band management
- Networking ports: 24 port 1GbE fiber with SFP
- Networking ports: 4 port 10GbE uplink fiber SFP+ or copper RJ-45 combo ports
- LED indicators
- Power and status LEDs (see section 6.2.5 for details)

6.2.3 CES 2024C

- Console: EIA/TIA-232 port
- Management Port: 10/100/1000 Mbps Ethernet port for out-of-band management
- Networking ports: 24 port 1GbE copper with RJ-45
- Networking ports: 4 port 10GbE uplink fiber SFP+ or copper RJ-45 combo ports
- LED indicators
- Power and status LEDs (see section 6.2.5 for details)

6.2.4 CES 2024F

- Console: EIA/TIA-232 port
- Management Port: 10/100/1000 Mbps Ethernet port for out-of-band management
- Networking ports: 24 port 1GbE fiber with SFP
- Networking ports: 4 port 10GbE uplink fiber SFP+ or copper RJ-45 combo ports
- LED indicators
- Power and status LEDs (see section 6.2.5 for details)

6.2.5 CER 2000 series / CES 2000 series Status LED

LED	Position	State	Meaning
AC PS1 (labeled P1)	Left side of front panel	Off	Power supply 1 is not installed or is not providing power.
		Amber	Power supply 1 is installed, but not connected or a fault is detected.
		Green	Power supply 1 is installed and is functioning normally.
AC PS1 (labeled P2)	Right side of front panel	Off	Power supply 2 is not installed or is not providing power.
		Amber	Power supply 2 is installed, but not connected or a fault is detected.
		Green	Power supply 2 is installed and is functioning normally.
Fan (labeled Fn)	Right side of front panel	Green	The fan tray is powered on and is operating normal
		Amber or Green blinking	The fan tray is not plugged in.
		Amber	The fan tray is plugged in but one or more fans are faulty.

Table 40 - Power and fan status LEDs for the CER 2000 series and CES 2000 series models

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

6.3 Modes of Operation

The NetIron validated cryptographic modules (Brocade MLXe Series Ethernet Routers, - Brocade NetIron CER 2000 Series Ethernet Routers and Brocade NetIron CES 2000 Series Ethernet Switches) has two modes of operation:

- FIPS Approved mode and
- Non-Approved mode.

Both these modes enforce digital signature based firmware load test. Section 8 describes services and cryptographic algorithms available in FIPS Approved mode.

Section 11.2.1.1 FIPS Approved Mode describes how to invoke FIPS Approved mode.

6.4 Module Validation Level

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

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

Table 41 - NetIron Security Levels

7 Roles

In FIPS Approved mode, NetIron devices support up to five different authenticated roles.

Three of these authenticated roles (Crypto-officer role, Port Configuration Administrator role and User role) are common across MLXe, CER 2000 series and CES 2000 series family of devices.

Two other specific authenticated roles (MACsec Peer role and IKEv2/IPsec Peer role) only apply to MLXe family of devices. These roles are provided to facilitate authentication for MACsec and IPsec features which are only available on MLXe devices.

Role	Supported in platform	Description of the role
Crypto-officer role	MLXe, CES 2000 series and CER 2000 series	The Crypto-officer role on the device in FIPS Approved mode is equivalent to administrator or super-user in non-Approved mode. Hence, the Crypto-officer role has complete access to the system.
Port Configuration Administrator role	MLXe, CES 2000 series and CER 2000 series	The Port Configuration Administrator role on the device in FIPS Approved mode is equivalent to the port-config, a port configuration user in non-Approved mode. Hence, the Port Configuration Administrator role has read-and-write access for specific ports but not for global (system-wide) parameters.
User role	MLXe, CES 2000 series and CER 2000 series	The User role on the device in FIPS Approved mode has read-only privileges and no configuration mode access (user).
MACsec Peer role	MLXe (only)	A peer device which establishes a MACsec connection with the cryptographic module
IKEv2/IPsec Peer role	MLXe (only)	A peer device which establishes an IPsec tunnel which includes IKEv2 negotiation for key establishment, and subsequent IPsec tunnel for data transport between the IPsec peer.

Table 42 - List of Roles supported in NetIron firmware

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

8 Services

This section describes services available in Approved mode of operation, to the operators based on their role.

The services available to an operator depend on the operator's role. Unauthenticated operators may view externally visible status LEDs. LED signals indicate status that allows operators to determine if the network connections are functioning properly. Unauthenticated operators can also perform self-test by power cycling a NetIron device. The following services are available to both unauthenticated and authenticated operators of the module:

- Self-Test
- Show Status

For all other services, an operator must authenticate to the device as described in Section 10.2, Authentication.

NetIron devices provide services for remote communication (NTP, SSHv2, SCP, SNMPv3 and Console) for management and configuration of cryptographic functions.

NetIron MLXe devices (only) provide HTTPS, MACsec and IPsec services for remote communication for data communications.

Service	Supported in platform	Crypto Operations	Additional Information
Console	All NetIron series (MLXe, CES 2000 series and CER 2000 series) support these services.	Local user authentication	No additional information is provided here.
IPsec	MLXe series (only) supports this service CES 2000 series does not support this service. CER 2000 series does not support this service.	IKEv2/IPsec tunnel setup authentication and data encryption	Supported by MLXe interface line cards: • BR-MLX-10GX4-IPSEC-M
HTTPS	MLXe series (only) supports this service CES 2000 series does not support this service. CER 2000 series does not support this service.	TLS authentication and encryption	No additional information is provided here.
MACsec	MLXe series (only) supports this service CES 2000 series does not support this service. CER 2000 series does not support this service.	MACsec connection authentication and encryption	Supported by MLXe interface line cards: • BR-MLX-10GX4-IPSEC-M • BR-MLX-10GX20-M • BR-MLX-1GX20-U10G-M • BR-MLX-10GX20-X2 • BR-MLX-1GX20-U10G-X2

Service	Supported in platform	Crypto Operations	Additional Information
NTP	All NetIron series (MLXe, CES 2000 series and CER 2000 series) support these services.	NTP peer authentication	No additional information is provided here.
SCP	All NetIron series (MLXe, CES 2000 series and CER 2000 series) support these services.	SSHv2/SCP authentication and encryption	No additional information is provided here.
SNMPv3	All NetIron series (MLXe, CES 2000 series and CER 2000 series) support these services.	SNMPv3 authentication and encryption	No additional information is provided here.
SSHv2	All NetIron series (MLXe, CES 2000 series and CER 2000 series) support these services.	SSHv2/SCP authentication and encryption	No additional information is provided here.

Table 43 - List of services in Approved mode of operation

Note that additional algorithm related information and details are available in sections 9.1, 9.2 and 9.3.

Table below summarizes the available FIPS Approved cryptographic functions used within the services available in FIPS Approved mode of operation.

Label	Cryptographic Function	Hardware Platform
AES	Advanced Encryption Standard	All devices
SHS	Secure Hash Standard	All devices
HMAC	Keyed-Hash Message Authentication Code	All devices
DRBG	Deterministic Random Bit Generator	All devices
RSA	Rivest Shamir Adleman	All devices
CVL	SSHv2 and TLS v1.0/1.1 and TLS v1.2 Key Derivation Function, SNMPv3 KDF, IKEv2 KDF, SP800-56A (ECC, FFC)	All devices
ECDSA	Elliptic Curve Digital Signature Algorithm	MLXe only
KBKDF	SP800-108 Key Based Key Derivation Function (CTR_Mode)	MLXe only

Table 44 - FIPS Approved Cryptographic Functions

The table below lists cryptographic functions that while not FIPS Approved are allowed in FIPS Approved mode of operation.

Cryptographic Function	Hardware Platform
Diffie-Hellman (within SCP/SSHv2 protocol and TLS v1.0/1.1 and TLSv1.2 protocols) (key agreement; key establishment methodology provides 112 bits of encryption strength)	All devices
Diffie-Hellman (within IKE v2 protocol) (CVL Cert. #712; key agreement; key establishment methodology provides 112 bits of encryption strength)	MLXe only
EC Diffie-Hellman (within IKE v2 protocol) (CVL Cert. #713, key agreement; key establishment methodology provides between 128 and 192 bits of encryption strength)	MLXe only
HMAC-MD5 is used to support RADIUS for operator authentication only (HMAC-MD5 is not exposed to the operator)	All devices
MD5: Used in the TLS v1.0 and v1.1 KDF in FIPS mode as per SP800-135 (MD5 is not exposed to the operator)	All devices
MD5: Used in TACACS+ for operator authentication only (MD5 is not exposed to the operator).	All devices
NDRNG: Nondeterministic Random Number Generator used for generation of seeds for DRBG only	All devices
RSA key transport (within TLS v1.0/1.1 and TLS v1.2 protocol) (key wrapping; key establishment methodology provides 112 bits of encryption strength)	All devices

Table 45 - Non-Approved Cryptographic Functions Allowed in FIPS Approved Mode

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

8.1 User Role Services

The User role management privilege level allows access to the User EXEC, and Privileged EXEC commands, but only with read access.

8.1.1 SSHv2

The module supports SSHv2. This service provides a secure session between a NetIron device and an SSHv2 client. The NetIron device authenticates an SSHv2 client and provides an encrypted communication channel. An operator may use an SSHv2 session for managing the device via the command line interface. The following cipher sequence is supported for SSHv2:

- aes-256-ctr
- aes-192-ctr
- aes-128-ctr
- aes-256-cbc
- aes-192-cbc, and
- aes-128-cbc

The following key-exchange (KEX) is supported for SSHv2:

- diffie-hellman-group-exchange-sha-256

The following Message Authentication Code (MAC) is supported for SSHv2:

- hmac-sha-1

NetIron devices support three kinds of SSHv2 client authentication:

- password authentication
- keyboard interactive authentication
- public- key authentication

For password authentication, an operator attempting to establish an SSHv2 session provides a password through the SSHv2 client. The NetIron device authenticates operator with passwords stored on the device, on a TACACS+ server, or on a RADIUS server. Section 10.2 Authentication provides authentication details.

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

For public key authentication, possession of a private key serves as an authentication method. In PKI (Public Key Infrastructure), each private key has its corresponding public key and they are referred to a key pair. Every key pair is unique. The cryptographic module uses a database of client public keys and its associated user names and roles to support public key authentication. The SSHv2 client which possesses the private key sends a signature (over some data from the request including the user name) created using the private key. The cryptographic module uses the public key corresponding to the user and verifies the signature to authenticate the user.

In the User role, the client is given access to three commands:

- enable
- exit
- terminal

The enable command allows the operator to re-authenticate using a different role. If the role is the same, based on the credentials given during the enable command, the operator has access to a small subset of commands that can perform ping, traceroute, outbound SSHv2 client in addition to show commands.

8.1.2 HTTPS

NOTE: This service is only available on MLXe products. CER 2000 series / CES 2000 series devices do not provide this service

This service provides a graphical user interface for managing a NetIron MLXe device over a secure communication channel. Using a web browser, an operator connects to a designated TCP port on a NetIron device. The device negotiates a TLS v1.0/1.1 and TLS v1.2 connection with the browser and authenticates the operator. The device uses HTTP over TLS v1.0/1.1 and v1.2 with the following cipher suites:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

In the User role, after a successful login, the default HTML page is the same for any role. The operator can surf to any page after clicking on any URL. However, this operator is not allowed to make any modifications. If the user presses the 'Modify' button within any page, the user will be challenged to reenter the Crypto-officer role's credentials. The challenge dialog box does not close unless the operator provides the Crypto-officer role's access credentials. After three failed attempts, the page '**Protected Object**' is displayed, in effect disallowing any changes from the web.

8.1.3 SNMP

SNMPv1 and SNMPv2c are blocked in FIPS mode. Only SNMPv3 in authPriv mode is allowed while other modes are blocked. SNMP service within the User role allows read-only access to the SNMP MIB within the NetIron device. The device does not provide SNMP access to CSPs when operating in FIPS Approved mode. These CSP MIB objects are a small subset of MIB that represent the security parameters like passwords, secrets and keys. Other MIB objects are made available for read-only access (status output).

8.1.4 Console

Console connections occur via a directly connected RS-232 serial cable. Once authenticated in the User role, the module provides console commands to display information about a NetIron device and perform basic tasks (such as pings). The User role has read-only privileges and no configuration mode access. The list of commands available are the same as the list mentioned in the SSHv2 service.

8.1.5 NTP

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

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

8.2 Port Configuration Administrator Role Services

The Port Configuration Administrator role management privilege level allows read-and-write access for port configuration, but not for global (system-wide) parameters.

8.2.1 SSHv2

This service is described in Section 8.1.1 above.

The Port Configuration Administrator role will have 7 commands, which allows this user to run show commands, run ping or traceroute and the enable command which allows this user to re-authenticate as described in Section 8.1.1. Within the configuration mode, this role provides access to all the port configuration commands. That is, all sub-commands within "`interface eth 1/1`" command. This operator cannot transfer and store software images and configuration files between the network and the system. However, this operator can review the configuration.

8.2.2 HTTPS

NOTE: This service is only available on MLXe products. CER 2000 series / CES 2000 series devices do not provide this service

This service is described in Section 8.1.2 above.

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

8.2.3 SNMP

This service is described in Section 8.1.3 above.

The SNMP service is not available for the Port Configuration Administrator role.

8.2.4 Console

This service is described in Section 8.1.4 above.

Console access as the Port Configuration Administrator role provides an operator with the same capabilities as User role Console commands plus configuration commands associated with a network port on the device. The commands available to operator within the Port Configuration Administrator role are same as those mentioned in the SSHv2 service in Section 8.1.1.

8.2.5 NTP

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

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

8.3 Crypto-officer Role Services

The Crypto-officer role management privilege level allows complete read-and-write access to the system. This is generally for system administrators and is the only management privilege level that allows one to configure passwords. The Crypto-officer role is able to perform firmware loading for the device as it has complete access to the system.

8.3.1 SSHv2

This service is described in Section 8.1.1 above.

The Crypto-officer role can perform configuration changes to the module. This role has full read and write access to the NetIron device.

8.3.2 SCP

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

8.3.3 HTTPS

NOTE: This service is only available on MLXe products. CER 2000 series / CES 2000 series devices do not provide this service

This service is described in Section 8.1.2 above.

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

8.3.4 SNMP

This service is described in Section 8.1.3 above.

The SNMP service within Crypto-officer role allows access to the SNMP MIB within the NetIron device as per the capability of the SNMP agent, using SNMPv3 version in authPriv security mode. The device does not provide SNMP access to CSPs when operating in FIPS Approved mode. These CSP MIB objects are a small subset of MIB that represent the security parameters like passwords, secrets and keys. Other MIB objects are made available for access similar to non-Approved mode of operation.

8.3.5 Console

This service is described in Section 8.1.4 above.

Console commands provide an authenticated Crypto-officer role complete access to all the commands within the NetIron device. This operator can enable, disable and perform status checks. This operator can also enable any service by configuring the corresponding command. For example, to turn on SSHv2 service, the operator creates a pair of RSA host keys, to configure the authentication scheme for SSHv2 access.

In case of MLXe series products only, to enable the Web Management service, the operator would securely import RSA private host key and a digital certificate using corresponding commands (over a secured SSHv2 connection), and enable the HTTPS server.

The Crypto-officer can zeroize CSPs using "`fips zeroize all`" from the console command line.

8.3.6 NTP

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

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

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

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

8.4 MACsec Peer Role Services

8.4.1 MACsec

NOTE: This service is only available on MLXe products. CER 2000 series / CES 2000 series devices do not provide this service

This implicit role is available on the module and allows an MKA session to be established with a remote peer based on the MACsec configuration on the device.

8.5 IKEv2/IPsec Peer Role Services

8.5.1 IKEv2/IPsec Negotiation – IPsec Traffic

NOTE: This service is only available on MLXe products. CER 2000 series / CES 2000 series devices do not provide this service

This implicit role is available on the IPsec supported interface line card and allows IKEv2 and IPsec sessions to be established with a remote peer based on the IPsec configuration on the device.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

8.6 Non-Approved Mode Services

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

Function/Service	Role(s)	Additional Details	Product Family
BGP	This is not a user accessible service	Border Gateway Protocol (BGP) is a standardized exterior gateway protocol. This is an implicit service, configured by Crypto-officer role. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)	MLXe series, CES/CER 2000 series products
File copy	Crypto-officer role	File copy over HTTPS service This service is used to transfer files between the NetIron device and HTTPS server, using HTTPS protocol. See, section 8.1.2 for more details on supported TLS cipher list.	MLXe series, CES/CER 2000 series products
HTTP	Crypto-officer role, User role	This service provides a graphical user interface for managing a NetIron MLXe device over an unsecure communication channel. Modes – Not Applicable Key sizes – Not Applicable (plaintext; no cryptography)	MLXe series products
MPLS	This is not a user accessible service	Multiprotocol Label Switching (MPLS) can be used to direct packets through a network over a predetermined path of routers. Forwarding decisions in MPLS are based on the contents of a label applied to the packet. This is an implicit service, configured by Crypto-officer role. Modes: MD5 for authentication Key sizes: Up to 80 characters	MLXe series, CES/CER 2000 series products
NTP (Authentication using MD5)	This is not a user accessible service	Network Time Protocol Modes: MD5 for authentication Key sizes: 20 bytes	MLXe series, CES/CER 2000 series products
OpenFlow	This is not a user accessible service	OpenFlow protocol allows external entity to control the behavior of the NetIron device by installing flows that affects the packet forwarding action of the device. The protocol can run over TCP or TLS. This is an implicit service, configured by Crypto-officer role. See, section 8.1.2 for more details on supported TLS cipher list.	MLXe series, CES/CER 2000 series products

Function/Service	Role(s)	Additional Details	Product Family
OSPFv2	This is not a user accessible service	Open Shortest Path First (OSPF) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). This is an implicit service, configured by Crypto-officer role. Modes: MD5 for authentication Key sizes: Not Applicable (plaintext; no cryptography)	MLXe series, CES/CER 2000 series products
OSPFv3	This is not a user accessible service	Open Shortest Path First (OSPF) is a link-state routing protocol. IPv6 supports OSPF Version 3 (OSPFv3), which functions similarly to OSPFv2 with some enhancements. Modes: HMAC-SHA-1-96 (non-compliant) for authentication Key sizes: 160 bits	MLXe series, CES/CER 2000 series products
SNMP	Crypto-officer role, User role	SNMPv1, SNMPv2c and SNMPv3 KDF (non-compliant) in noAuthNoPriv, authNoPriv modes. Modes: DES in authPriv mode for SNMPv3 KDF (non-compliant) Key sizes: DES 56 bits NOTE: Keys derived from the SNMPv3 KDF in the non-Approved mode cannot be used in the Approved mode.	MLXe series, CES/CER 2000 series products
SSHv2/SCP	Crypto-officer role, Port Configuration Administrator role, User role	Secure Shell (SSHv2) is a cryptographic (encrypted) network protocol for initiating text-based shell sessions on remote machines in a secure way. SCP (Secure Copy) uses security built into SSH server to transfer files between hosts on a network. It uses SSHv2 as a transport. Modes: RSA (non-compliant) Key sizes: 1024 bit Modes: Triple-DES (non-compliant) Key sizes: Three-Key Triple-DES Modes: DH Key Exchange (non-compliant) Groups: DH Group1 (768-bit) using SHA-1, DH Group14 (2048-bit) using SHA-1	MLXe series, CES/CER 2000 series products
Syslog	This is not a user accessible service	Syslog is a standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. This is an implicit service, configured by Crypto-officer role. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)	MLXe series, CES/CER 2000 series products

Function/Service	Role(s)	Additional Details	Product Family
TACACS	This is not a user accessible service	TACACS (Terminal Access Controller Access Control System) is an authentication protocol running over UDP which allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system. This is an implicit service, configured by Crypto-officer role. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)	MLXe series, CES/CER 2000 series products
Telnet	Crypto-officer role, Port Configuration Administrator role, User role	Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP). Modes – Not Applicable Key sizes – Not Applicable (plaintext; no cryptography)	MLXe series, CES/CER 2000 series products
TFTP	Crypto-officer role	Trivial File Transfer Protocol (TFTP) is a file transfer protocol notable for its simplicity. It is generally used for automated transfer of configuration or boot files between machines in a local environment. Compared to FTP, TFTP is extremely limited, providing no authentication, and is rarely used interactively by a user. Modes – Not Applicable Key sizes – Not Applicable (plaintext; no cryptography)	MLXe series, CES/CER 2000 series products
“Two way encryption”	Crypto-officer role, Port Configuration Administrator role, User role	Base64 is a number of similar encoding schemes that encode binary data by treating it numerically and translating it into a base 64 representation. Modes – Not Applicable Key sizes – Not Applicable (plaintext; no cryptography)	MLXe series, CES/CER 2000 series products
VRRP/VRRP-E	This is not a user accessible service	Virtual Router Redundancy Protocol (VRRP) and Virtual Router Redundancy Protocol (VRRP-E) Enhancement This is an implicit service, configured by Crypto-officer role. Modes: Layer 3 mode Key sizes: Not Applicable (plaintext; no cryptography)	MLXe series, CES/CER 2000 series products
VSRP	This is not a user accessible service	Virtual Switch Redundancy Protocol This is an implicit service, configured by Crypto-officer role. Modes: Layer 2 mode Key sizes: Not Applicable (plaintext; no cryptography)	MLXe series, CES/CER 2000 series products

Table 46 - Functions/Services, Roles in Non-Approved Mode Services

8.6.1 Non-Approved Algorithms

The module provides the following non-FIPS approved algorithms in the non-Approved mode of operation:

- MD5
- DES
- SNMPv3 KDF (non-compliant)
- RSA 1024-bit key size
- Triple-DES (non-compliant)
- DH Group1 (768-bit)
- DH Group14 (2048-bit) (non-compliant)
- SHA-1 (non-compliant)
- HMAC-SHA-1-96 (non-compliant)

The use of any such service in a non-Approved manner in Table 46 is an explicit violation of this Security Policy and is explicitly disallowed by this Security Policy.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

9 Algorithm certificates

This section provides information on all related cryptographic algorithms and their associated certificates..

9.1 Algorithm certificates in MLXe

Algorithm	Supports	Certificate
Advanced Encryption Standard (AES)	MLXe MR2: 128, 192, and 256-bit keys, ECB, CBC and CTR (internal counter source) modes	#2717
Advanced Encryption Standard (AES)	CMAC (Generation/Verification) (KS: 128; Block Size(s): Full / Partial; Msg Len(s) Min: 0 Max: 2^16 ; Tag Len(s) Min: 2 Max: 16) KW (AE, AD, AES-128, FWD, 128, 256, 192, 320, 4096)	#2946
Advanced Encryption Standard (AES)	CFB128 (e/d; 128);	#3144
Component Test Key Derivation Function (CVL)	TLS v1.0/1.1 KDF	#175
Component Test Key Derivation Function (CVL)	TLS v1.2 KDF	#393
Component Test Key Derivation Function (CVL)	SSHv2 KDF	#175
Component Test Key Derivation Function (CVL)	SNMPv3 KDF	#404
Deterministic Random Bit Generator (DRBG) NOTE: The algorithm was also certified for Hash_Based DRBG, but the DRBG runs in CTR mode. Hash_Based DRBG is not available within any service in Approved mode of operation.	SP800-90A CTR_DRBG	#454
ECDSA	FIPS186-4: PKG: CURVES (P-256 P-384 ExtraRandomBits TestingCandidates) PKV: CURVES (P-256 P-384) SigGen: CURVES (P-256: (SHA-224, 256, 384, 512) P-384: (SHA-224, 256, 384, 512) SigVer: CURVES (P-256: (SHA-1, 224, 256, 384, 512) P-384: (SHA-1, 224, 256, 384, 512))	#761
Keyed-Hash Message Authentication code (HMAC)	HMAC-SHA-1, HMAC-SHA-256	#1696

Algorithm	Supports	Certificate
Secure Hash Algorithm NOTE: The algorithm was also certified for SHA-224 and SHA-512 but they are not used in any service in any mode of operation.	SHA-1, SHA-256, and SHA-384	#2282
Rivest Shamir Adleman Signature Algorithm (RSA) NOTE: The module does not support 1024-bit keys in Approved mode operation.	2048-bit (Key generation, signature generation and verification) keys	#1413
SP800-108 (KBKDF)	CTR_Mode	#35

Table 47 - Algorithm Certificates for the MLXe Series

Algorithm	Supports	Certificate

Advanced Encryption Standard (AES)
NOTE: Brocade uses Broadcom AES Cert #2154 Only the AES modes listed in this table are used in this cryptographic module; all other modes listed in the Broadcom AES Cert #2154 are not supported by this cryptographic module.
	ECB (e only; 128);
	GCM (KS: AES_128 (e/d) Tag Length(s): 128)
	IV Generated: (Internally (using Section 8.2.1));
	PT Lengths Tested: (24, 1024);
	AAD Lengths tested: (160, 1024);
	IV Lengths Tested: (8, 1024);
	96BitIV_Supported
	GMAC_Not_Supported
	"Four channel, 10 Gigabit Ethernet PHY with MACsec."
		#2154

Table 48 - Algorithm Certificates for BR-MLX-10GX20-M, BR-MLX-10GX20-X2, BR-MLX-1GX20-U10G-M and BR-MLX-1GX20-U10G-X2 interface line cards

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

Algorithm	Supports	Certificates

Advanced Encryption Standard (AES)
NOTE: Brocade uses Freescale AES Cert #1648. Only the AES modes listed in this table are used in this cryptographic module; all other modes listed in the Freescale AES Cert #1648 are not supported by this cryptographic module.
	ECB (e/d; 128, 192, 256);
	GCM
	(KS: AES_128(e/d) Tag Length(s): 128 120 112 104 96 64 32)
	(KS: AES_192(e/d) Tag Length(s): 128 120 112 104 96 64 32)
	(KS: AES_256(e/d) Tag Length(s): 128 120 112 104 96 64 32)
	IV Generated: (Externally);
	PT Lengths Tested: (1024);
	AAD Lengths tested: (1024);
	IV Lengths Tested: (8, 1024);
	96BitIV_Supported;
	OtherIVLen_Supported
	GMAC_Supported
	CBC (e/d; 128, 192, 256);
		#1648

Advanced Encryption Standard (AES)
NOTE: Brocade uses Broadcom AES Cert #2154 Only the AES modes listed in this table are used in this cryptographic module; all other modes listed in the Broadcom AES Cert #2154 are not supported by this cryptographic module.
	ECB (e only; 128);
	GCM (KS: AES_128 (e/d) Tag Length(s): 128)
	IV Generated: (Internally (using Section 8.2.1));
	PT Lengths Tested: (24, 1024);
	AAD Lengths tested: (160, 1024);
	IV Lengths Tested: (8, 1024);
	96BitIV_Supported
	GMAC_Not_Supported
	"Four channel, 10 Gigabit Ethernet PHY with MACsec."
		#2154

Advanced Encryption Standard (AES)	ECB (e only; 128 , 256); GCM (KS: AES_128(e/d) Tag Length(s): 128) (KS: AES_256(e/d) Tag Length(s): 128) IV Generated: (Internally (using Section 8.2.1)) ; PT Lengths Tested: (128 , 1024) ; AAD Lengths tested: (64 , 96) ; IV Lengths Tested: (0 , 0) ; 96BitIV_Supported GMAC_Not_Supported	#3478
Component Test, All of SP800-56A Except KDF (CVL)	DH (FFC)	#712
Component Test, All of SP800-56A Except KDF (CVL)	ECDH (ECC, P-256 and P-384)	#713
Component Test Key Derivation Function (CVL)	IKEv2	#1029
Deterministic Random Bit Generator (DRBG)	SP800-90A HASH_DRBG	#684

Algorithm	Supports	Certificates
ECDSA NOTE: The algorithm was also certified for SHA-1, SHA-224 and SHA-512 but they are not used in any service in any mode of operation.	FIPS 186-4 P-384, P-256 PKG: CURVES(P-256 P-384 ExtraRandomBits TestingCandidates) PKV: CURVES(P-256 P-384) SigGen: CURVES(P-256: (SHA-224, 256, 384, 512) P-384: (SHA-224, 256, 384, 512) SigVer: CURVES(P-256: (SHA-1, 224, 256, 384, 512) P-384: (SHA-1, 224, 256, 384, 512))	#809
Keyed-Hash Message Authentication Code (HMAC) NOTE: The algorithm was also certified for HMAC-SHA-1, HMAC-SHA-224 and HMAC-SHA-512 but they are not used in any service in any mode of operation.	HMAC-SHA-256, HMAC-SHA-384	#2848
Secure Hash Algorithm NOTE: The algorithm was also certified for SHA-1, SHA-224 and SHA-512 but they are not used in any service in any mode of operation.	SHA-256, SHA-384	#934

Table 49 - Algorithm Certificates for BR-MLX-10GX4-IPSEC-M interface line cards

NOTE: Further details for each CAVP algorithm validation certificate, including but not limited to details on the associated processors, can be found at the CAVP website:

http://csrc.nist.gov/groups/STM/cavp/validation.html

NOTE: Operators 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: The module does not allow the use of 1024-bit RSA key in the FIPS Approved mode of operation due to the SP800-131A transition effective January 1, 2014.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

9.2 Algorithm certificates in CER 2000 series / CES 2000 series

Algorithm	Supports	Certificate
Advanced Encryption Standard (AES)	128, 192, and 256-bit keys, ECB, CBC and CTR	#2715
Advanced Encryption Standard (AES)	CFB128	#3143
Component Test Key Derivation Function (CVL)	SNMPv3 KDF	#403
Component Test Key Derivation Function (CVL)	TLS v1.0/1.1 and SSHv2 KDF	#173
Component Test Key Derivation Function (CVL)	TLS v1.2 KDF	#394
Deterministic Random Bit Generator (DRBG) NOTE: The algorithm was also certified for Hash_Based DRBG, but the DRBG runs in CTR mode. Hash_Based DRBG is not available within any service in Approved mode of operation.	SP800-90A CTR_DRBG	#452
Keyed-Hash Message Authentication code (HMAC)	HMAC-SHA-1, HMAC-SHA-256	#1694
Rivest Shamir Adleman Signature Algorithm (RSA) NOTE: The module does not support 1024-bit keys in FIPS Mode	2048-bit (Key generation, signature generation and verification) keys	#1411
Secure Hash Algorithm NOTE: The algorithm was also certified for SHA-224 and SHA-512 but they are not used in any service in any mode of operation.	SHA-1, SHA-256, SHA-384	#2280

Table 50 - Algorithm Certificates for CER 2000 series / CES 2000 series

Operators 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: The module does not allow the use of 1024-bit RSA or 1024-bit DSA keys in the FIPS Approved mode of operation due to the SP800-131A transition effective January 1, 2014.

9.3 non-Approved but allowed cryptographic methods

See Table 45 for additional information on Non-Approved Cryptographic Functions Allowed in FIPS Approved Mode.

10 Policies

10.1 Security Rules

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

Security rules are as follows:

1) The cryptographic module provides role-based authentication.
2) Until the module is placed in a valid role, the operator does not have access to any Critical Security Parameters (CSPs).
3) The AES GCM session key is established via the IKEv2 KDF (internally). The 96-bit IV is also constructed internally (deterministically) as per FIPS 140-2 IG A.5 Scenario 3. The GCM key and IV are session specific; if the module loses power the implementation is required to renegotiate a new IKE session and thus a new GCM key and IV will be created.
4) The AES GCM session key is established via the SP800-108 KDF (internally). The 96-bit IV is also constructed internally (deterministically) as per FIPS 140-2 IG A.5 Scenario 3. The GCM key and IV are session specific; if the module loses power the implementation is required to renegotiate a new MKA session and thus a new GCM key and IV will be created.
5) The cryptographic module performs the following tests:
    a) Power-up Self-Tests (see table, below)
        i) Cryptographic Known Answer Tests (KAT) are list in the table below

KAT tests	MLXe product	CER 2000 series / CES 2000 series product
Three-Key Triple-DES KAT (encrypt)	✓	✓
Three-Key Triple-DES KAT (decrypt)	✓	✓
AES-128 (ECB, CBC and CFB128) KAT (encrypt)	✓	✓
AES-128 (ECB, CBC and CFB128) KAT (decrypt)	✓	✓
AES-128 CMAC KAT (generation)	✓	Not Applicable
AES-128 CMAC KAT (verification)	✓	Not Applicable
AES-KW KAT (wrap)	✓	Not Applicable
AES-KW KAT (unwrap)	✓	Not Applicable
ECDSA P-256 and P-384 pairwise consistency test (sign)	✓	Not Applicable
ECDSA P-256 and P-384 pairwise consistency test	✓	Not Applicable

KAT tests	MLXe product	CER 2000 series / CES 2000 series product
(verify)		
SHA-1, 256, 384, 512 KAT (hashing)	✓	✓
HMAC-SHA-1, 256 KAT (hashing)	✓	✓
RSA 2048 bit key size KAT (encrypt)	✓	✓
RSA 2048 bit key size KAT (decrypt)	✓	✓
RSA 2048 bit key size, SHA-256, 384, 512 Hash KAT (signature generation)	✓	✓
RSA 2048 bit key size, SHA-256, 384, 512 Hash KAT (signature verification)	✓	✓
SP800-90A DRBG KAT	✓	✓
SP800-135 TLS v1.0/1.1 KDF KAT	✓	✓
SP800-135 SSHv2 KDF KAT	✓	✓
SP800-135 TLS v1.2 KDF KAT	✓	✓
SP800-135 SNMPv3 KDF KAT	✓	✓
SP800-135 IKEv2 KDF KAT	✓	Not Applicable
SP800-108 KBKDF KAT	✓	Not Applicable
AES-128 GCM KAT	✓	Not Applicable
ECDH (P-384) KAT	✓	Not Applicable

Table 51 - Power-Up Self-Tests - Cryptographic Known Answer Tests (KAT)

ii) Firmware Integrity Test: (CRC 16 and Digital Signature using RSA 2048 SHA-256)

iii) Critical functions test: RSA 2048 encrypt/decrypt

iv) Message reporting for Power on Self-Test (POST)

If the module does not detect an error during the Power on Self-Test (POST), at the conclusion of the test, the console displays the message shown below.

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

If the module detects an error during the POST, at the conclusion of the test, the console displays the message shown below.

Also, the message logging will display the message shown below.

```
FIPS Fatal Cryptographic Module Failure <Reason String>
```

After displaying the failure messages, the module reboots.

b) Conditional Self-Tests (see table, below)

Conditional Self-Tests	MLXe product	CER 2000 series / CES 2000 series product
Continuous Test: Non-Deterministic Random Number Generator (NDRNG) Test performed on non-Approved NDRNG	✓	✓
Continuous Test: Random Number Generator Test performed on Approved DRBG.	✓	✓
RSA 2048 SHA-256 Pairwise Consistency Test (sign)	✓	✓
RSA 2048 SHA-256 Pairwise Consistency Test (verify)	✓	✓
RSA 2048 SHA-256 Pairwise Consistency Test (encrypt)	✓	✓
RSA 2048 SHA-256 Pairwise Consistency Test (decrypt)	✓	✓
ECDSA P-256 and P-384 Pairwise Consistency Test (sign)	✓	Not Applicable
ECDSA P-256 and P-384 Pairwise Consistency Test (verify)	✓	Not Applicable
Firmware Load Test: RSA 2048 SHA-256 Signature Verification	✓	✓
Bypass Test: Alternating Bypass Test	✓	Not Applicable
Manual Key Entry Test	Not Applicable	Not Applicable

Table 52 - Conditional Self-Tests

i) Message reporting for failure of Conditional Self-Tests

If the module detects an error during the Conditional Self-Test, it displays and logs the message shown below.

```
FIPS Fatal Cryptographic Module Failure <Reason String>
```

After displaying the failure message, the module reboots.

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

7) Data output to services defined in section 8 (Services) is inhibited during key generation, self-tests, zeroization, and error states.

8) For MLXe only - The operator shall enter minimum 112 bit IKEv2 Pre-Shared Key (PSK).

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

10) The following protocols have not been reviewed or tested by the CAVP nor CMVP:

   a) TLS v1.0/1.1

   b) SSHv2

   c) TLS v1.2

   d) SNMPv3

   e) IKEv2 (for MLXe only)

10.1.1 Cryptographic Module Operational Rules

In order to operate an MLXe, CER 2000 series and CES 2000 series device securely, an operator should be aware of the following rules for FIPS Approved mode of operation.

Do not make external communication channels/ports available before initialization of an MLXe, CER 2000 series and CES 2000 series device.

The operator shall not invoke the following commands:

- Commands for OpenFlow
  - `openflow enable`
  - `openflow controller`
  - `openflow default send-to-controller`
- Commands for HTTPS File Copy
  - `copy https flash <ip-address> username <username> password <password> <filename> <destination-filename>`
  - `copy {flash|slot1|slot2} https {<ipv4-addr>|<ipv6-addr>} <remote-filename><source-filename>`

NOTE: Execution of any of the commands listed above places the module strictly in the non-FIPS Approved mode of operation.

MLXe, CER 2000 series and CES 2000 series devices implement FIPS Approved SP800-90A Deterministic Random Bit Generator (DRBG) in Counter (CTR) Mode.

MLXe, CER 2000 series and CES 2000 series devices use FIPS Approved key generation methods:

- RSA public and private keys
- ECDSA public and private keys (for MLXe only)

MLXe, CER 2000 series and CES 2000 series devices restrict key entry and key generation to authenticated roles.

NEXT PAGE →

10.2 Authentication

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

To implement one or more authentication methods for securing access to the device, an operator in the Crypto-officer role configures authentication-method lists that set the order in which a device consults authentication methods. In an authentication-method list, an operator specifies an access method (SSHv2, Web, SNMP, and so on) and the order in which the device tries one or more of the following authentication methods:

1. Line password authentication,
2. Enable password authentication,
3. Local user authentication,
4. RADIUS authentication with exec authorization and command authorization, and
5. TACACS+ authentication with exec authorization and command authorization

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

NetIron devices allow multiple concurrent operators through SSHv2 and the console. One operator's configuration changes can overwrite the changes of another operator.

10.2.1 Line Authentication Method

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

To use line authentication, a Crypto-officer role must set the Telnet password. Please note that when operating in FIPS Approved mode, Telnet is disabled and Line Authentication is not available.

10.2.2 Enable Authentication Method

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

To use enable authentication, a Crypto-officer role must set the password for each privilege level.

10.2.3 Local Authentication Method

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

To use local authentication, a Crypto-officer role must define user accounts. The definition includes a user name, password, and privilege level (which determines role).

NEXT PAGE →

10.2.4 RADIUS Authentication Method

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

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

1. A user previously authenticated by a RADIUS server enters a command on the NetIron device.
2. The NetIron device looks at its configuration to see if the command is at a privilege level that requires RADIUS command authorization.
3. If the command belongs to a privilege level that requires authorization, the NetIron device looks at the list of commands returned to it when RADIUS server authenticated the user.

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

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

10.2.5 TACACS+ Authentication Method

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

To use TACACS+ authentication, a Crypto-officer role must configure TACACS+ server settings along with authentication and authorization settings.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

10.2.6 Strength of Authentication

This section describes the strength of each authentication method

10.2.6.1 MACsec Peer Role (only applicable to MLXe)

Knowledge of strength of MACsec Pre-Shared Key:

Specifically in reference to MACsec Peer role only, the probability of a successful random guess of the AES 128-bit pre-shared key is 1/ 2^128 for a random attempt, which is less than 1/1,000,000. The module only supports a maximum of 60 attempts during a one minute period due to the timing of the protocol. This means that the probability of false authorization with multiple consecutive random attempts during a one minute period is 60 / 2^128, which is less than 1/100,000.

10.2.6.2 IKEv2/IPsec Peer Role (only applicable to MLXe)

Knowledge of strength of IKEv2 ECDSA Private Key:

> When configuring the smallest curve P-256, the probability that a random attempt will succeed or a false acceptance will occur is 1/2^128, which is less than 1/1,000,000.
>
> The maximum attempts allowed in a one minute period is equal to 256 attempts (e.g. max number of 256 SA sessions supported by the module). Therefore, the probability of a random success in a one minute period is 256/2^128, which is less than 1/100,000.

Knowledge of strength of IKEv2 Pre-Shared Key (PSK):

> The IKEv2 Pre-Shared Key is a 112-bit HMAC Key, 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 maximum attempts allowed in a one minute period is equal to 256 attempts (e.g. max number of 256 SA sessions supported by the module). Therefore, the probability of a random success in a one minute period is 256/2^112, which is less than 1/100,000.

10.2.6.3 All other roles

All other roles can utilize all other available techniques for the purpose of authentication.

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

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

RADIUS and TACACS+ support minimum 8 character passwords selected from the following character set: digits (Qty. 10), lowercase (Qty. 26) and uppercase (Qty. 26) letters, and punctuation marks (Qty. 18), for a total of 80 characters. Therefore, the probability of a successful random attempt is 1/80^8, which is less than 1/1,000,000.

A user gets three attempts before lockdown. When lockdown occurs, the user is locked out until the device is rebooted. Rebooting takes longer than one minute. Therefore, the maximum number of attempts per minute is 3. Thus, the probability of a successful random attempt within a one minute period is 3/80^8, which is less than 1/100,000.

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

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

10.3 Access Control and Critical Security Parameters (CSPs)

Table 53 and Table 54 summarize the access operators in each role have to CSPs. Blank table cells indicate that there is no security relevance between the role and the CSP. The table entries have the following meanings:

- r – Operator can read the value of the item,
- w – Operator can write a new value for the item,
- x – Operator can use the value of the item (for example encrypt with an encryption key), and
- d – Operator can delete the value of the item (zeroize) by executing a `fips zeroize all` command. See item 4a in Section 11.2.1.1 for further details.

ROLE➔	Crypto-officer role						User role					Port Configuration Administrator role				
Service CSP	SSHv2	SCP	HTTPS (MLXe only)	SNMP	Console	NTP	SSHv2	HTTPS (MLXe only)	SNMP	Console	NTP	SSHv2	HTTPS (MLXe only)	SNMP	Console	NTP
SSHv2 Host RSA Private Key (2048 bit)	xwd	x			wd		x					x				
SSHv2 Client RSA Private Key	xwd	x			wd		x					x				
SSHv2 DH Group-14 Private Key 2048 bit MODP	xwd	x			wd		x					x				
SSHv2 DH Shared Secret Key (2048 bit)	x	x			xd		x					x				
SSHv2/SCP Session Keys (128, 192 and 256 bit (AES CBC and AES CTR)	x	x			xd		x					x				

ROLE➔	Crypto-officer role						User role					Port Configuration Administrator role				
Service CSP	SSHv2	SCP	HTTPS (MLXe only)	SNMP	Console	NTP	SSHv2	HTTPS (MLXe only)	SNMP	Console	NTP	SSHv2	HTTPS (MLXe only)	SNMP	Console	NTP
SSHv2/SCP Authentication Key (HMAC-SHA-1, 160 bits)	x	x			xd		x					x				
SNMPv3 KDF State				xwd												
SSHv2 KDF Internal State	x	x			xd		x					x				
TLS Host RSA Private Key (RSA 2048 bit; MLXe only)	rwd		x		rwd			x					x			
TLS Host DH Group-14 Private Key 2048 bit MODP (MLXe only)	d		xwd		d			xwd					xwd			
TLS Pre-Master Secret (MLXe only)			x		xd			x					x			
TLS Master Secret (MLXe only)			x		xd			x					x			
TLS KDF Internal State (MLXe only)	xd		x		xd			x					x			
TLS Session Key (MLXe only)			x		xd			x					x			

ROLE➔	Crypto-officer role						User role					Port Configuration Administrator role				
Service / CSP	SSHv2	SCP	HTTPS (MLXe only)	SNMP	Console	NTP	SSHv2	HTTPS (MLXe only)	SNMP	Console	NTP	SSHv2	HTTPS (MLXe only)	SNMP	Console	NTP
TLS Authentication Key (MLXe only)			xd		xd			x					x			
MP DRBG Key (applies to CES/CER and MLXe MP)	x	x	x		xd		x	x				x	x			
MP DRBG Internal State (applies to CES/CER and MLXe MP)	xd	x	x		xd		x	x				x	x			
MP DRBG Seed (applies to CES/CER and MLXe MP)	x	x	x		xd		x	x				x	x			
MP DRBG Value V (applies to CES/CER and MLXe MP)	x	x	x		xd		x	x				x	x			
NTP Secret	xrwd	xrwd	xrwd		xrwd	xrwd	x	x		x	r	x	x		x	r
LP DRBG Internal State (MLXe LP only)	xd	x	x		xd		x	x				x	x			
LP DRBG Seed (MLXe LP only)	x	x	x		xd		x	x				x	x			

ROLE➔	Crypto-officer role						User role					Port Configuration Administrator role				
Service / CSP	SSHv2	SCP	HTTPS (MLXe only)	SNMP	Console	NTP	SSHv2	HTTPS (MLXe only)	SNMP	Console	NTP	SSHv2	HTTPS (MLXe only)	SNMP	Console	NTP
LP DRBG Value C (MLXe LP only)	x	x	x		xd		x	x				x	x			
LP DRBG Value V (MLXe LP only)	x	x	x		xd		x	x				x	x			
Local - User Password	xrwd	xrwd	xrwd	x	xrwd		x	x	x	x						
Local - Port Administrator Password	xrwd	xrwd	rwd		xrwd							x	x		x	
Local - Crypto-officer Password	xrwd	xrwd	xrwd		xrwd											
RADIUS Secret	xrwd	xrwd	xrwd		xrwd		x	x		x		x	x		x	
TACACS+ Secret	xrwd	xrwd	xrwd		xrwd		x	x		x		x	x		x	
SNMPv3 secret	xrwd	xrwd	xrwd	xrwd	xrwd		x	x	x	x		x	x	x	x	
Firmware Load RSA Public Key	x		x		xd											
SSHv2 Host RSA Public Key (2048 bit)	xrwd	xrw			rwd		x					x				
SSHv2 Client RSA Public Key	xrwd	xrwd			xrwd		x					x				

ROLE➔	Crypto-officer role						User role					Port Configuration Administrator role				
Service CSP	SSHv2	SCP	HTTPS (MLXe only)	SNMP	Console	NTP	SSHv2	HTTPS (MLXe only)	SNMP	Console	NTP	SSHv2	HTTPS (MLXe only)	SNMP	Console	NTP
SSHv2 DH Group-14 Public Key 2048 bit MODP	x	x			xd		x					x				
SSHv2 DH Group-14 Peer Public Key 2048 bit MODP	x	x			xd		x					x				
TLS Host RSA Public Key (RSA 2048 bit; MLXe only)	rwd		x		rwd			x					x			
TLS Peer Public Key (RSA 2048 bit, MLXe only)	rwd		x		rwd			x					x			
TLS Host DH Group-14 Public Key 2048 bit MODP (MLXe only)			xwd		d			xwd					xwd			
TLS Peer DH Group-14 Public Key 2048 bit MODP (MLXe-only)			xd		d			xd					xd			
IKEv2 ECDSA Public Key (P-256) (MLXe only)	rwd	rw			rwd											

ROLE➔	Crypto-officer role						User role					Port Configuration Administrator role				
Service CSP	SSHv2	SCP	HTTPS (MLXe only)	SNMP	Console	NTP	SSHv2	HTTPS (MLXe only)	SNMP	Console	NTP	SSHv2	HTTPS (MLXe only)	SNMP	Console	NTP
IKEv2 ECDSA Public Key (P-384) (MLXe only)	rwd	rw			rwd											
MKA Connectivity Association Key (CAK) (MLXe only)	wd	rwd			wd											
MKA Connectivity Key Name (CKN) (MLXe only)	rwd	rwd			rwd											
MKA SP800-108 KDF State (MLXe only)	rwd				rwd											
IKEv2 ECDSA Private Key (P-256) (MLXe only)	rwd	rw			rwd											
IKEv2 ECDSA Private Key (P-384) (MLXe only)	rwd	rw			rwd											
IKEv2 Pre-Shared Key (PSK) (MLXe only)	rwd				rwd											

Table 53 - Access Control Policy and Critical Security Parameters (CSPs)

NEXT PAGE →

NOTE: MACsec and IPSec Access Control Policy and CSPs table, below, is **only** applicable to MLXe products. These CSPs are not applicable to CER 2000 series / CES 2000 series devices.

For MLXe product only

ROLE ➔	MACsec Peer role	IKEv2/IPsec Peer role
CSP / Service	MACsec	IKEv2 Negotiation - IPsec Traffic
MKA Integrity Checksum Key (ICK)	xrwd	
MKA Key Encryption Key (KEK)	xrwd	
MKA Secure Association Key (SAK)	xrwd	
MKA SP800-108 KDF State	xrwd	
MKA Connectivity Association Key (CAK)	rd	
MKA Connectivity Key Name (CKN)	rd	
IKEv2 DH Group-14 Private Key 2048 bit MODP		xrwd
IKEv2 DH Group-14 Public Key 2048 bit MODP		xrwd
IKEv2 DH Group-14 Shared Secret 2048 bit MODP		xrwd
IKEv2 ECDSA Private Key (P-256)		xrd
IKEv2 ECDSA Private Key (P-384)		xrd
IKEv2 ECDSA Public Key (P-256)		xrd
IKEv2 ECDSA Public Key (P-384)		xrd
IKEv2 ECDH Group 19 Private Key (P-256)		xrwd
IKEv2 ECDH Group 20 Private Key (P-384)		xrwd
IKEv2 ECDH Group 19 Public Key (P-256)		xrwd
IKEv2 ECDH Group 20 Public Key (P-384)		xrwd
IKEv2 ECDH Group-19 Shared Secret (P-256)		xrwd
IKEv2 ECDH Group-20 Shared Secret (P-384)		xrwd

ROLE →	MACsec Peer role	IKEv2/IPsec Peer role
CSP / Service	MACsec	IKEv2 Negotiation - IPsec Traffic
IKEv2 Encrypt/Decrypt Key		xrwd
IKEv2/IPsec Authentication Key		xrwd
IPsec ESP Encrypt/Decrypt Key		xrwd
IKEv2 KDF State		xrwd
IKEv2 Pre-Shared Key (PSK)		xrd
LP DRBG Seed		xrd
LP DRBG Value V		xrd
LP DRBG Value C		xrd
LP DRBG Internal State		xrd
PKI SCEP Enrollment RSA 2048-bit Private Key		xrwd
PKI SCEP Enrollment RSA 2048-bit Public Key		xrwd

Table 54 - MACsec and IPSec Access Control Policy and Critical Security Parameters (CSPs)

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

10.3.1 CSP Zeroization

The SSHv2 session key is transient. It is zeroized at the end of a session and recreated at the beginning of a new session.

The TLS pre-master secret is generated during the TLS handshake. It is destroyed after it is used.

For MLXe only, the TLS session key is generated for every HTTPS session. The TLS session key is deleted after the session is closed.

The DRBG seed and CTR_DRBG Entropy is recomputed periodically on 100 millisecond intervals. Each time this occurs, four bytes of the seed are written into an 8K buffer. When the buffer is full the DRBG V and Key values are regenerated and the buffer is zeroized.

The DH private exponent is generated at the beginning of DH KEX. A new random number overwrites the memory location used to store the value each time a new session is initiated.

For SSHv2, the RSA private key is stored in a locally generated file on flash during the key generation process. The file is removed during zeroization. The crypto key zeroize command removes the keys.

On MLXe device (only), run the "`clear ikev2 sa`" command to manually reset the IPsec tunnel once the FIPS mode is disabled.

Execute the "`no fips enable`" command to complete zeroize process on all host key pairs. Execution of "`no fips enable`" command is required for all (MLXe, CER 2000 series and CES 2000 series) NetIron devices.

All other CSPs can be zeroized by executing the "`fips zeroize all`" command.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

10.4 Physical Security

NetIron devices require the Crypto-officer role to install tamper evident labels in order to meet FIPS 140-2 Level 2 Physical Security requirements. The tamper evident labels are available from Brocade under part number XBR-000195. The Crypto-officer role shall follow the Brocade FIPS Security Seal application procedures prior to operating the module in FIPS Approved mode. The FIPS seal application procedure is available in section, 14 - Appendix A: Tamper Evident Seal Application Procedure.

Physical Security Mechanisms	Recommended Frequency of Inspection	Inspection Guidance Details
Tamper Evident Labels	12 months	The security officer shall periodically monitor the state of all applied seals for evidence of tampering. A seal serial number mismatch, a seal placement change, a checkerboard destruct pattern that appears in peeled film and adhesive residue on the substrate are evidence of tampering. The security officer shall periodically view each applied seal under a UV light to verify the presence of a UV wallpaper pattern. The lack of a wallpaper pattern is evidence of tampering.

Table 55 - Inspection of Physical Security Mechanisms

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

11 Crypto-officer Guidance

For each module to operate in a FIPS Approved mode of operation, the tamper evident seals supplied in Brocade XBR-000195 must be installed, as defined in section, 14 - Appendix A: Tamper Evident Seal Application Procedure.

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

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

11.1 FIPS Approved Mode Status

NetIron devices provide the "`fips show`" command to display status information about the device's configuration. This information includes the status of administrative commands for security policy, the status of security policy enforcement, and security policy settings. The "`fips enable`" command changes the status of administrative commands; see also Section 11.2 FIPS Approved Mode.

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

```
MP FIPS Version: BRCD-IP-CRYPTO-VER-3.0a
LP FIPS Version: BRCD-LP-CRYPTO-VER-1.0a
FIPS mode   : Administrative status OFF: Operational status OFF
FIPS CC mode: Administrative status OFF: Operational status OFF
```

Table 56 - Sample output - MLXe in non-Approved mode

```
FIPS Version: BRCD-IP-CRYPTO-VER-3.0a
FIPS mode   : Administrative status OFF: Operational status OFF
FIPS CC mode: Administrative status OFF: Operational status OFF
```

Table 57 - Sample output – CES/CER in non-Approved mode

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

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

The status ‘Clear’ refers to the fact that when FIPS Approved mode is disabled at a later point in time, the corresponding CSPs will be affected based on the FIPS policy settings for that CSP.

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

```
FIPS Validated Cryptographic Module
MP FIPS Version: BRCD-IP-CRYPTO-VER-3.0a
LP FIPS Version: BRCD-LP-CRYPTO-VER-1.0a
FIPS mode   : Administrative status ON: Operational status ON
FIPS CC mode: Administrative status OFF: Operational status OFF

System Specific:
OS monitor access status is: Disabled

Management Protocol Specific:
Telnet server                 : Disabled
Telnet client                 : Disabled
TFTP client                   : Disabled
HTTPS SSL 3.0                 : Disabled
SNMP v1, v2, v2c              : Disabled
SNMP Access to security objects: Disabled
Password Display              : Disabled
Critical security Parameter updates across FIPS boundary:
(i.e. during "fips zeroize" ..., or "no fips enable")   :
Protocol Shared secret and host passwords: Clear
SSH RSA Host keys                         : Clear
HTTPS RSA Host Keys and Signature        : Clear
```

Table 58 - Sample output - MLXe in FIPS Approved mode

```
FIPS Validated Cryptographic Module
FIPS Version: BRCD-IP-CRYPTO-VER-3.0a
FIPS mode   : Administrative status ON: Operational status ON
FIPS CC mode: Administrative status OFF: Operational status OFF

System Specific:
OS monitor access status is: Disabled

Management Protocol Specific:
Telnet server                 : Disabled
Telnet client                 : Disabled
TFTP client                   : Disabled
SNMP v1, v2, v2c              : Disabled
SNMP Access to security objects: Disabled
Password Display              : Disabled
Critical security Parameter updates across FIPS boundary:
(i.e. during "fips zeroize" ..., or "no fips enable")   :
Protocol Shared secret and host passwords: Clear
SSH RSA Host keys                         : Clear
```

Table 59 - Sample output – CES/CER in FIPS Approved mode

11.2 FIPS Approved Mode

This section describes the FIPS Approved mode of operation and the sequence of actions that put a NetIron device in FIPS Approved mode.

FIPS Approved mode disables the following:

1. Enter command `no web-management hp-top-tools` in order to turn off access by HP ProCurve Manager via port 280.
2. Telnet access including the "`telnet server command`"
3. AAA authentication for the console using "`enable aaa console`" command is temporarily disabled to allow console access to configure SSH parameters. This command can be enabled after SSH is confirmed operational
4. Command "`ip ssh scp disable`"
5. TFTP access
6. SNMP access to CSP MIB objects
7. Access to all commands that allows debugging memory content within the monitor mode
8. In MLXe devices (only), access to the following commands get disabled:
   - HTTP access including the web-management http command
   - HTTPS SSL 3.0 access
   - Command web-management allow-no-password

Entering FIPS Approved mode also clears:

1. Protocol shared secret and host passwords
2. For MLXe only
   HTTPS RSA host keys and certificate

FIPS Approved mode enables:

1. SCP
2. For MLXe only
   HTTPS TLS v1.0/1.1 and TLS v1.2

11.2.1 Invoking FIPS Approved Mode

11.2.1.1 Invoking FIPS Approved Mode for Brocade MLXe Series Devices

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

1) Assume Crypto-officer role
   a) The authentication methods available for assuming the Crypto-officer role through the console terminal port are defined in Section 10.2. Both the Enable Authentication Method and Local Authentication Method can be used to assume the Crypto-officer role.
2) Copy signature files of all the affected images to the flash memory.
3) Enter command: `fips enable`
   a) The device enables FIPS administrative commands. The device is not in FIPS Approved Mode of operation yet. Do not change the default strict FIPS security policy, which is required for FIPS Approved mode.

4) Enter command: `fips zeroize all`
   a) The device zeroizes the shared secrets use by various networking protocols including host access passwords, SSHv2 Host keys, and HTTPS host keys with the digital signature.
5) Once the module completes zeroization, configure all users of the module and authentication methods as per Section 10.2.
6) Enter command: `write memory`
   a) The device saves the running configuration as the startup configuration
7) Enter command: reload
   a) The device reboots, does a Power-On Self-Test and if successful, begins operation in FIPS Approved mode.
8) Enter command: `fips show`
   a) The device displays the FIPS-related status, which should confirm the security policy is the default security policy.
9) Inspect the physical security of the module, including placement of tamper evident labels according to section, 14 - Appendix A: Tamper Evident Seal Application Procedure.

11.2.1.2 Invoking FIPS Approved Mode for Brocade CER 2000 series and CES 2000 series Devices

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

1) Assume Crypto-officer role
   a) The authentication methods available for assuming the Crypto-officer role through the console terminal port are defined in Section 10.2.
2) Copy signature files of all the affected images to the flash memory.
3) Enter command: `fips enable`
   a) The device enables FIPS administrative commands. The device is not in FIPS Approved Mode of operation yet. Do not change the default strict FIPS security policy, which is required for FIPS Approved mode.
4) Enter command: `fips zeroize all`
   a) The device zeroizes the shared secrets used by various networking protocols including host access passwords, and SSHv2 Host keys with the digital signature.
5) Once the module completes zeroization, configure all users of the module and authentication methods as per Section 10.2.
6) Enter command: `write memory`
   a) The device saves the running configuration as the startup configuration
7) Enter command: `reload`
   a) The device reboots, does a Power-On Self-Test and if successful, begins operation in FIPS Approved mode.
8) Enter command: `fips show`
   a) The device displays the FIPS-related status, which should confirm the security policy is the default security policy.
9) Inspect the physical security of the module, including placement of tamper evident labels according to section, 14 - Appendix A: Tamper Evident Seal Application Procedure.

11.2.2 Negating FIPS Approved Mode

11.2.2.1 Negating FIPS Approved Mode for Brocade MLXe Series Devices

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

1) Enter command: `no fips enable`
   a) This will return the device back to normal, non-Approved mode by enabling the networking protocols that were disallowed in FIPS Approved mode of operation. For example, Telnet, HTTP, TFTP will be enabled again. In addition, the restrictions against the non-Approved cryptographic algorithms will also be lifted. For example, MD5, DES algorithms would be allowed.
   b) The device zeroizes the shared secrets used by various networking protocols including host access passwords, SSHv2 Host keys, and HTTPS host keys with the digital signature.
2) Once the module completes zeroization, configure all users of the module and authentication methods as per Section 9.2.
3) Enter command: `write memory`
   a) The device saves the running configuration as the startup configuration
4) Enter command: reload
   a) Reload the device to begin non-Approved mode of operation.

11.2.2.2 Negating FIPS Approved Mode for Brocade CER 2000 Series and CES 2000 Series Devices

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

1) Enter command: `no fips enable`
   a) This will return the device back to normal, non-Approved mode by enabling the networking protocols that were disallowed in FIPS Approved mode of operation. For example, Telnet, TFTP will be enabled again. In addition, the restrictions against the non-Approved cryptographic algorithms will also be lifted. For example, MD5, DES algorithms would be allowed.
   b) The device zeroizes the shared secrets used by various networking protocols including host access passwords, SSHv2 client and server keys, and TLS client keys with the digital signature.
2) Once the module completes zeroization, configure all users of the module and authentication methods as per Section 9.2.
3) Enter command: `write memory`
   a) The device saves the running configuration as the startup configuration
4) Enter command: reload
   a) Reload the device to begin non-Approved mode of operation.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

12 Mitigation of other attacks

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

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

Table 60 - Mitigation of other attacks

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

13 Glossary

Term/Acronym	Description
AES	Advanced Encryption Standard
CBC	Cipher-Block Chaining
CLI	Command Line Interface
CFP	C Form-factor Pluggable
CSP	Critical Security Parameter
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook mode
ECDSA	Elliptic Curve Digital Signature Algorithm
GbE	Gigabit Ethernet
HMAC	Keyed-Hash Message Authentication Code
KDF	Key Derivation Function
LED	Light-Emitting Diode
LP	Line Processor
Mbps	Megabits per second
MP	Management Processor
NDRNG	Non-Deterministic Random Number Generator
NI	NetIron platform
OC	Optical Carrier
RADIUS	Remote Authentication Dial in User Service
RSA	Rivest Shamir Adleman
SCP	Secure Copy
SFM	Switch Fabric Module
SFP	Small Form-factor Pluggable
SFPP	Small Form-factor Plus Pluggable
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Networking
SSHv2	Secure Shell
TACACS	Terminal Access Control Access-Control System
TDEA	Triple-DES Encryption Algorithm
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
XFP	10 Gigabit Small Form Factor Pluggable

Table 61 - Glossary

14 Appendix A: Tamper Evident Seal Application Procedure

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

- Tamper Evident Security Seals
    - Count 120
    - Checkerboard destruct pattern with ultraviolet visible "Secure" image

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

14.1 Brocade MLXe devices

14.1.1 MLXe-4 device

Use the figures in this section as a guide for tamper evident security seal placement on a Brocade MLXe-4 device. Each Brocade MLXe-4 device requires the placement of nineteen (19) seals:

- Front: Fifteen (15) seals are required to complete the physical security. Unused slots must be filled with the module or filler panel appropriate for that slot to satisfy the physical security requirements and maintain adequate cooling. See Figure 18 for correct seal orientation and positioning.
- Rear: Four (4) seals are required to complete the physical security requirements. Affix one seal at each designated location. Each seal is applied from the top panel of the chassis to the flange of each of the four fan FRUs. You must bend each seal to place them correctly. See Figure 19 for correct seal orientation and positioning.

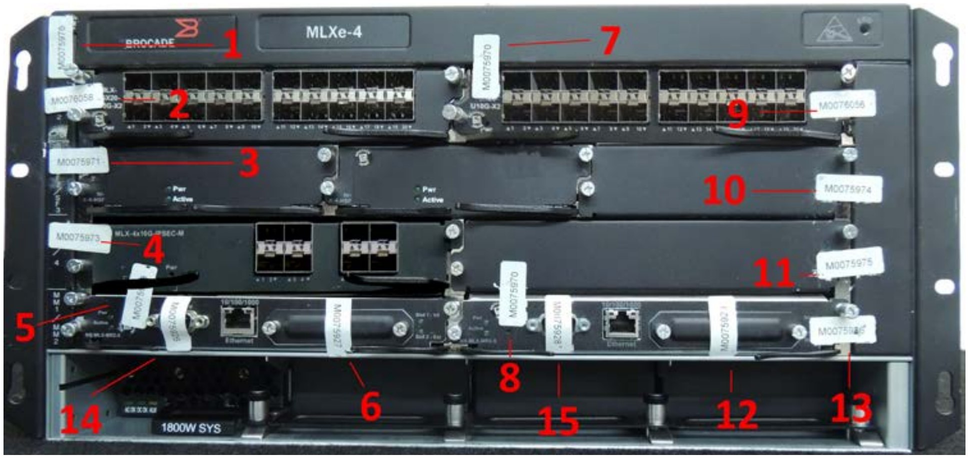

Figure 18 - Front view of Brocade MLXe-4 with security seals

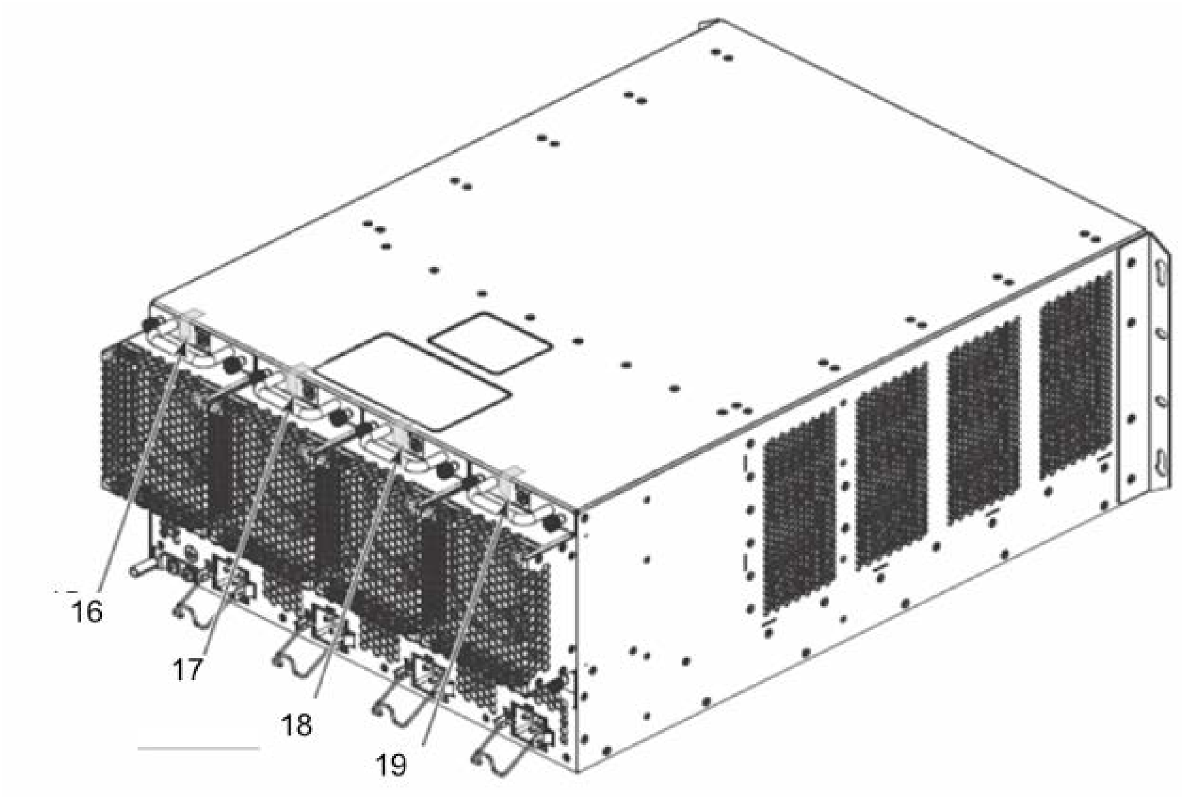

Figure 19 - Rear view of Brocade MLXe-4 device with security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

14.1.2 MLXe-8 device

Use the figures in this section as a guide for tamper evident security seal placement on a Brocade MLXe-8 device. Each Brocade MLXe-8 device requires the placement of twenty-two (22) seals:

- Front: Twenty (20) seals are required to complete the physical security requirements. Unused slots must be filled with the module or filler panel appropriate for that slot to satisfy the physical security requirements and maintain adequate cooling. See Figure 20 for correct seal orientation and positioning.
- Rear: Two (2) seals are required to complete the physical security requirements. Affix one (1) seal at each designated location. Each seal is applied from the top panel of the chassis to the flange of each of the two fan FRUs. You must bend each seal to place them correctly. See Figure 21 for correct seal orientation and positioning.

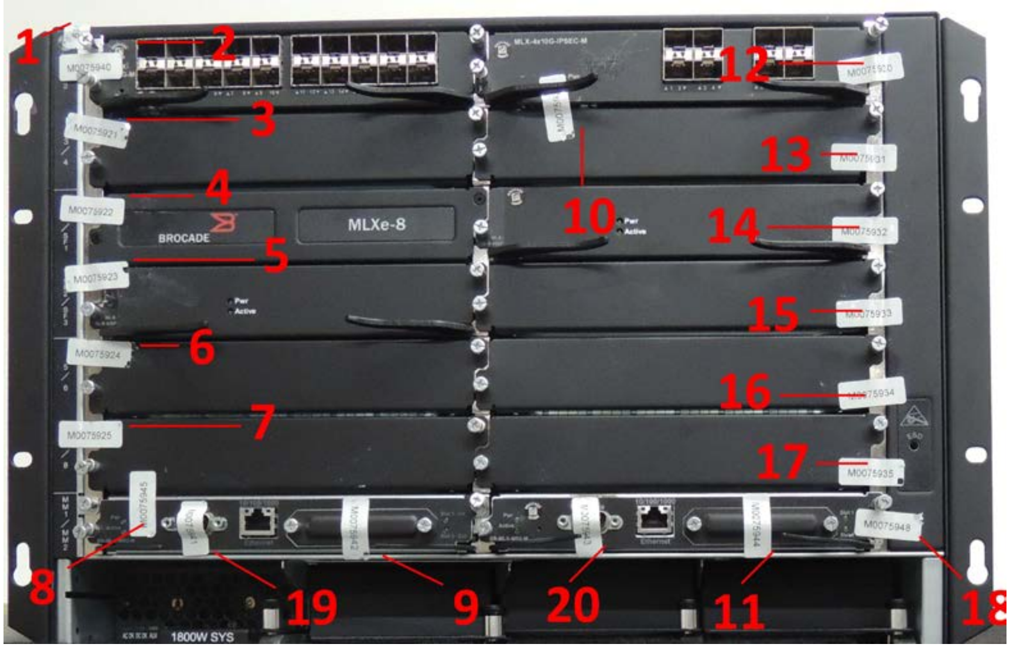

Figure 20 - Front view of Brocade MLXe-8 device with security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

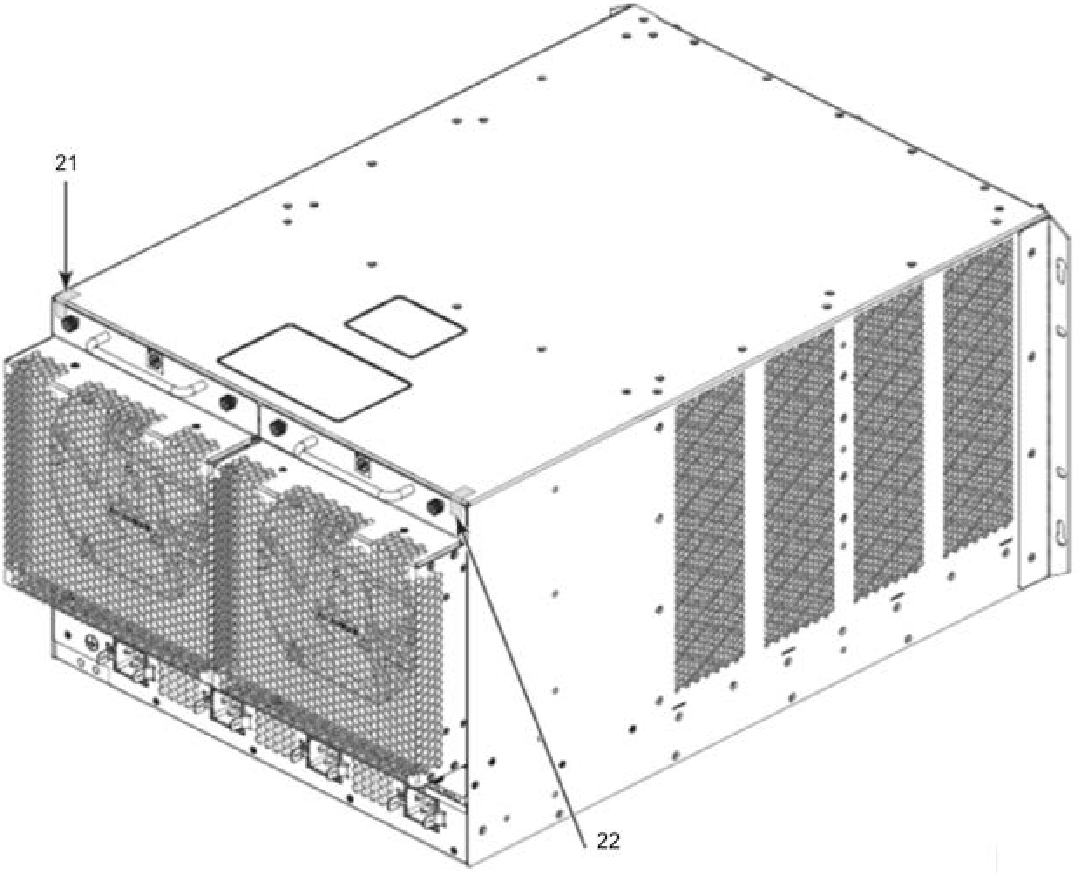

Figure 21 - Rear view of Brocade MLXe-8 device with security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

14.1.3 MLXe-16 device

Use the figures in this section as a guide for tamper evident security seal placement on a Brocade MLXe-16 device. Each Brocade MLXe-16 device requires the placement of twenty-nine (29) seals:

- Front: Twenty-seven (27) seals are required to complete the physical security. Unused slots must be filled with the module or filler panel appropriate for that slot to satisfy the physical security requirements and maintain adequate cooling. See Figure 22 for correct seal orientation and positioning.
- Rear: Two (2) seals are required to complete the physical security requirements. Affix one (1) seal at each designated location. Each seal is applied from the back panel of the chassis to the flange of each of the two fan FRUs. See Figure 23 for correct seal orientation and positioning.

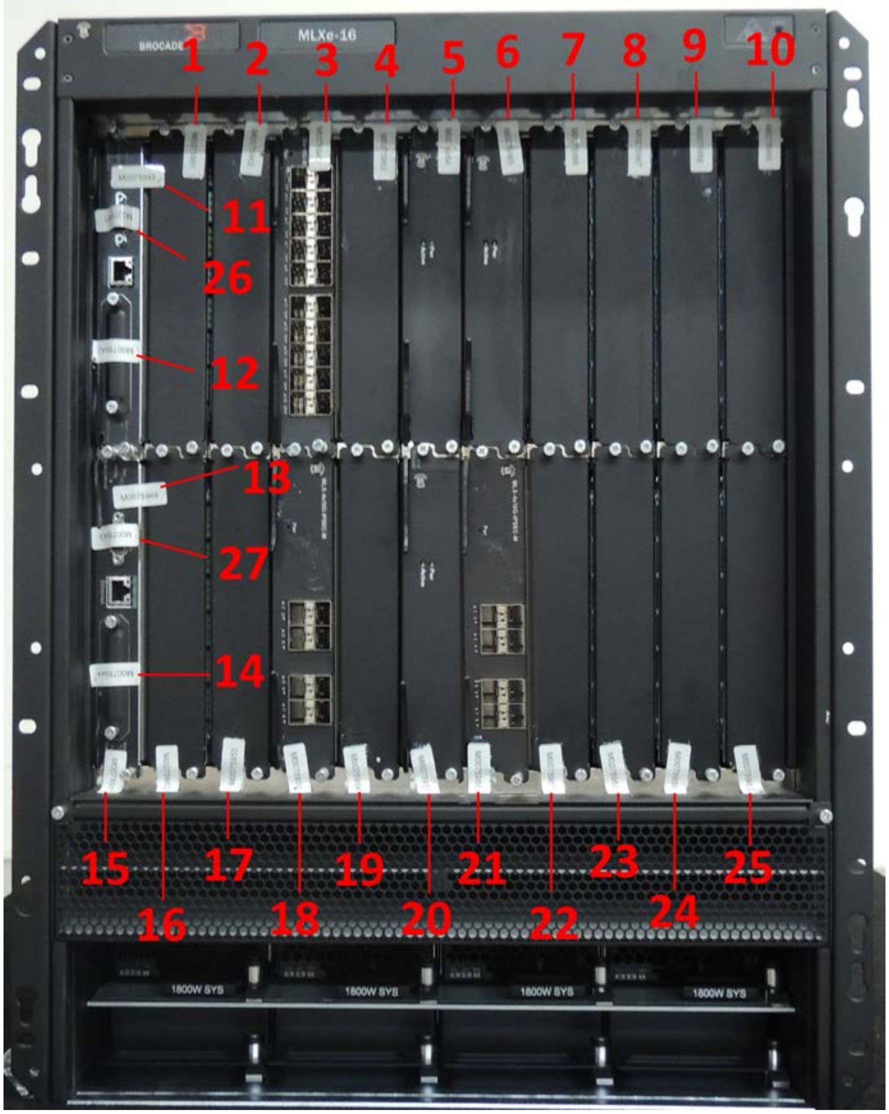

Figure 22 - Front view of Brocade MLXe-16 device with security seals

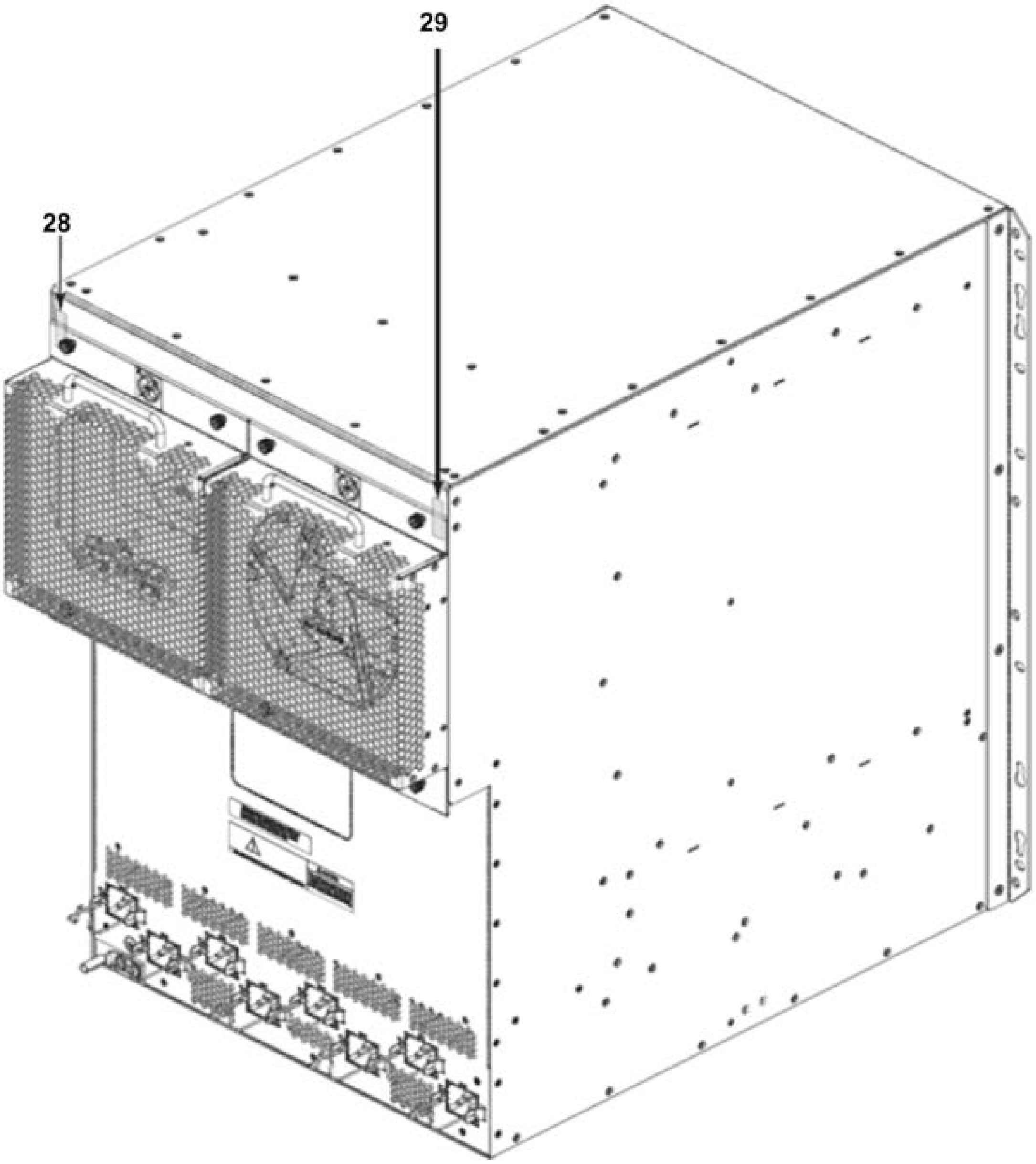

Figure 23 - Rear view of Brocade MLXe-16 device with security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

14.1.4 MLXe-32 device

Use the figures in this section as a guide for tamper evident security seal placement on a Brocade MLXe-32 device. Each Brocade MLXe-32 device requires the placement of seventy-one (71) seals. The left side, right side, top side and bottom side of the chassis do not require any labels:

- Front upper chassis: Uses twenty-six (26) labels. For labels 1 through 10, apply a label to the top edge of one of the following (dependent on configuration); filler panel, interface line card, or switch fabric module. For labels 11 & 14 apply a label horizontally to the management card with half on the management card itself and the other half placed on the adjacent panel. For labels 12 & 15 apply a label horizontally to the management card with the intent of covering the console port that is present on the module. For labels 13 & 16 apply a label horizontally to the management card with the intent of covering the open slot on the management card. For labels 17 through 26, apply a label to the bottom edge of one of the following (dependent on configuration); filler panel, interface line card, or switch fabric module.
- Front middle chassis (grill): Uses four (4) labels. For labels 27 through 30 place a label over each screw horizontally with the intention of completely masking the screw that attaches the grill to the middle. The label should be placed horizontally & flat directly over the surface of the screw.
- Front lower chassis: Uses twenty-two (22) labels. For labels 31 through 41, apply a label to the top edge of one of the following (dependent on configuration); filler panel, interface line card or switch fabric module. For labels 42 through 52, apply a label to the bottom edge of one of the following (dependent on configuration); filler panel, interface line card, or switch fabric module.
- Back upper chassis: Uses eight (8) labels. For labels 53 & 54, apply a label vertically with the bottom half of the label placed on the fan module itself. For labels 55 through 58, place a label horizontally with approximately half on the fan module itself and the other half wrapping onto the silver edge. For labels 59 & 60 place a label vertically with the top half of the label placed on the fan module.
- Back lower chassis: Uses eleven (11) labels. For labels 61 & 62, apply a label vertically with the bottom half of the label placed on the fan. For labels 63 through 66, place a label horizontally with approximately half on the fan module. For labels 67 & 68, apply a label vertically with the top half of the label placed on the fan module. For labels 69 & 71, place a label horizontally with approximately half the label on the black fan module and the other half on the silver surface of the module itself. For label 70, place the label vertically equally divided amongst the two black fan modules.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

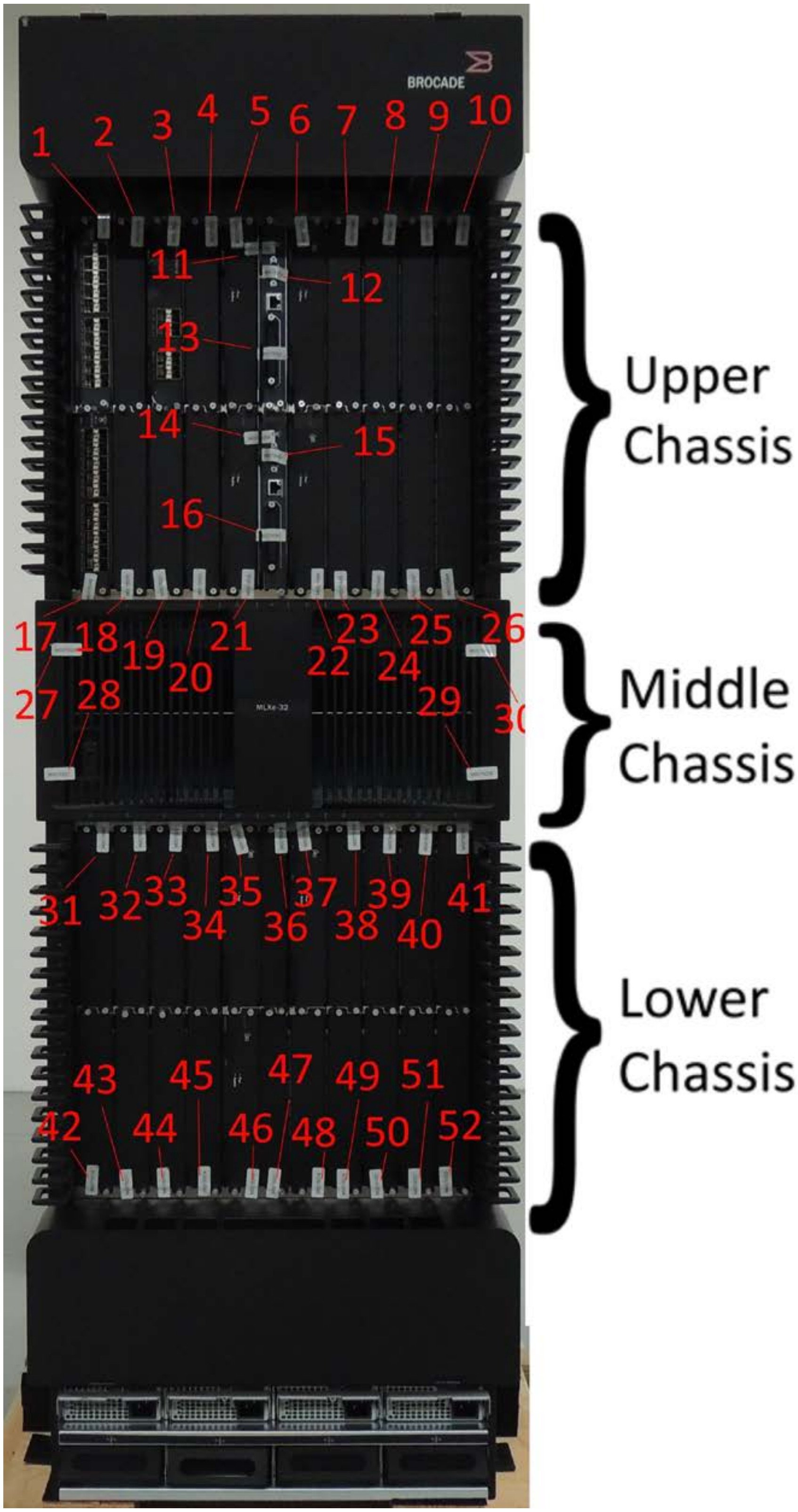

Figure 24 - Front overview of MLXe-32 Configuration 1 with tamper labels

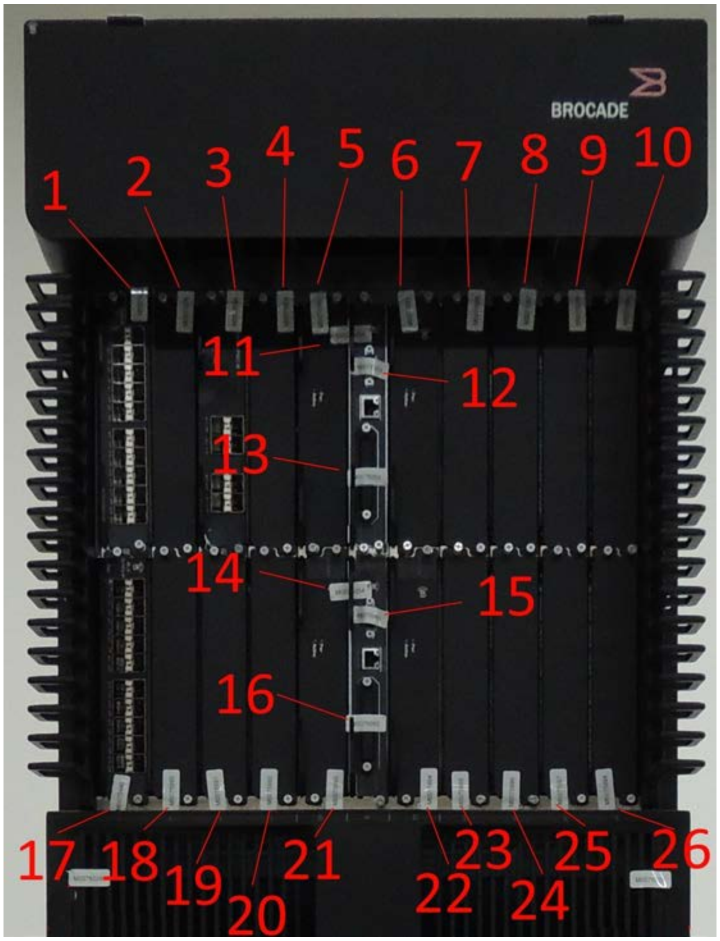

Figure 25 - Front upper chassis of MLXe-32 Configuration 1 with tamper labels

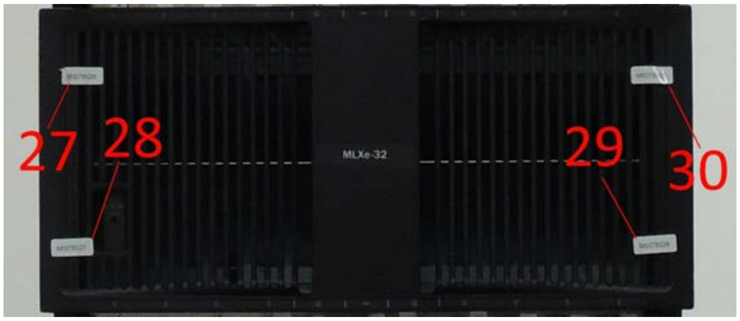

Figure 26 - Front middle chassis (grill) of MLXe-32 Configuration 1 with tamper labels

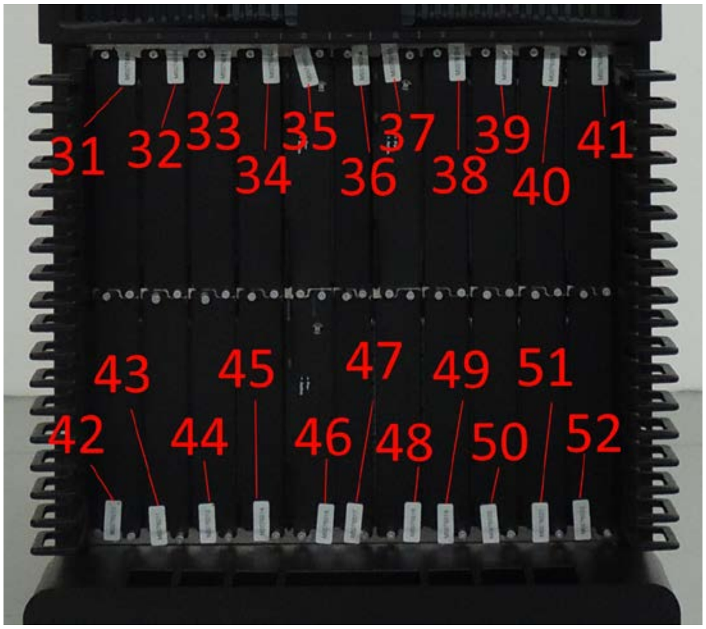

Figure 27 - Front lower chassis of MLXe-32 Configuration 1 with tamper labels

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

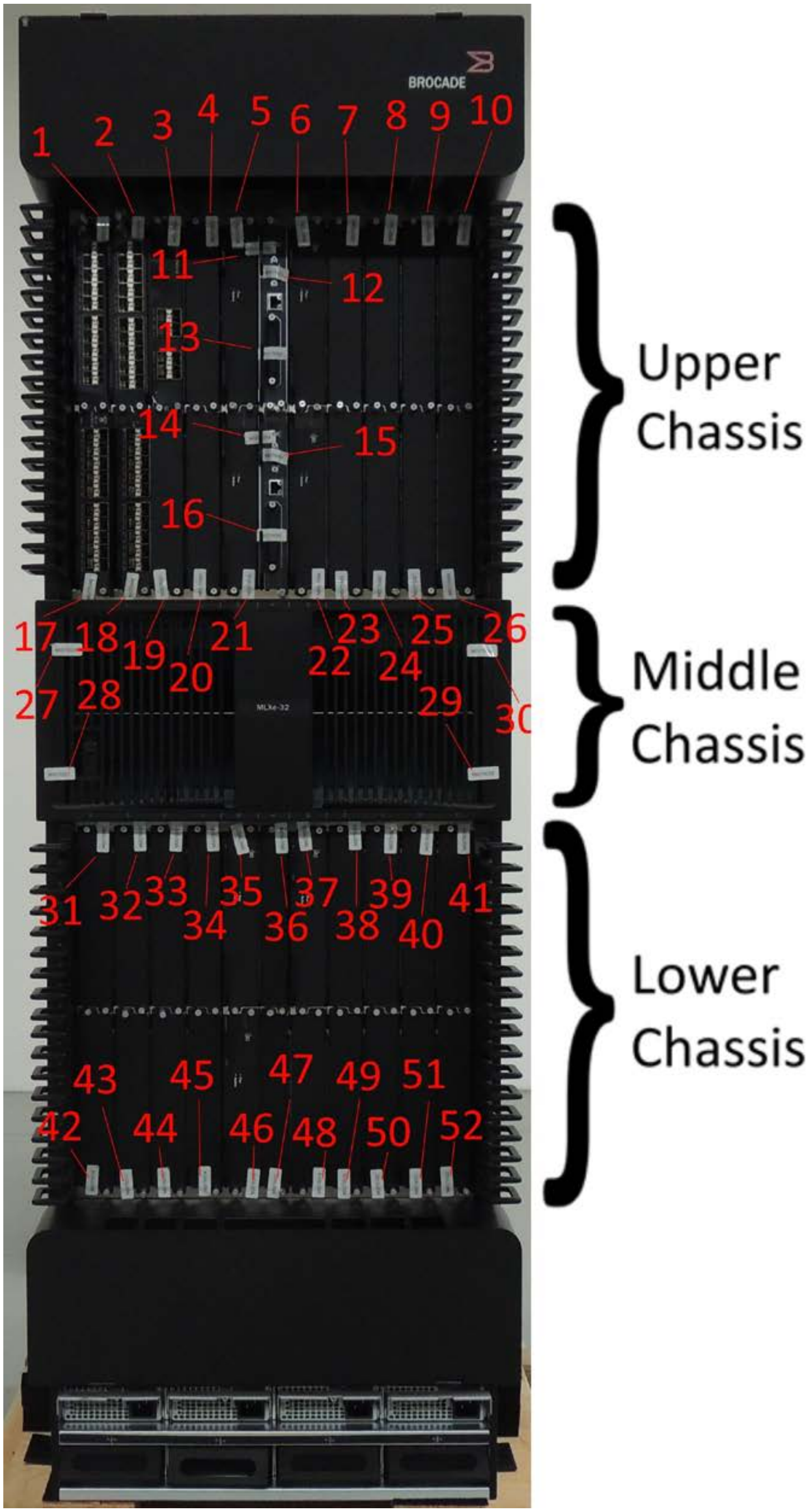

Figure 28 - Front overview of MLXe-32 Configuration 2 with tamper labels

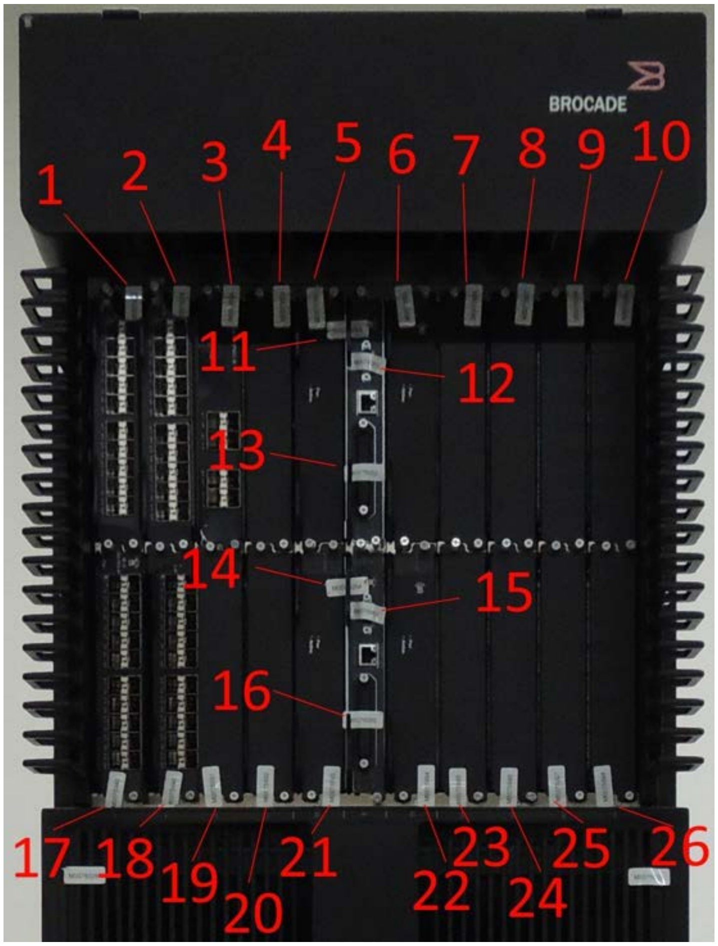

Figure 29 - Front overview of MLXe-32 Configuration 2 with tamper labels

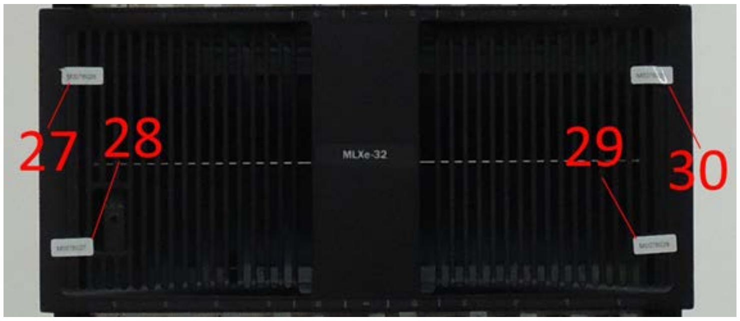

Figure 30 - Front middle chassis (grill) of MLXe-32 Configuration 2 with tamper labels

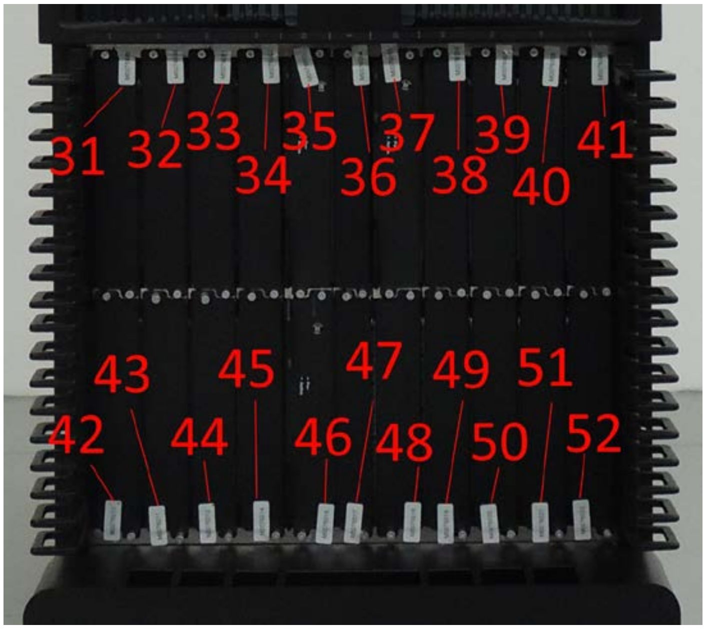

Figure 31 - Front lower chassis of MLXe-32 Configuration 2 with tamper labels

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

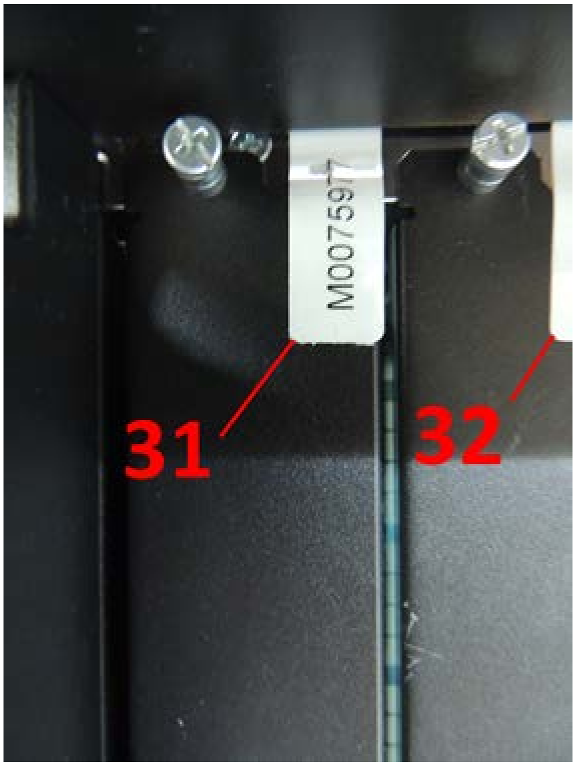

Figure 32 - Label 31 example of MLXe-32

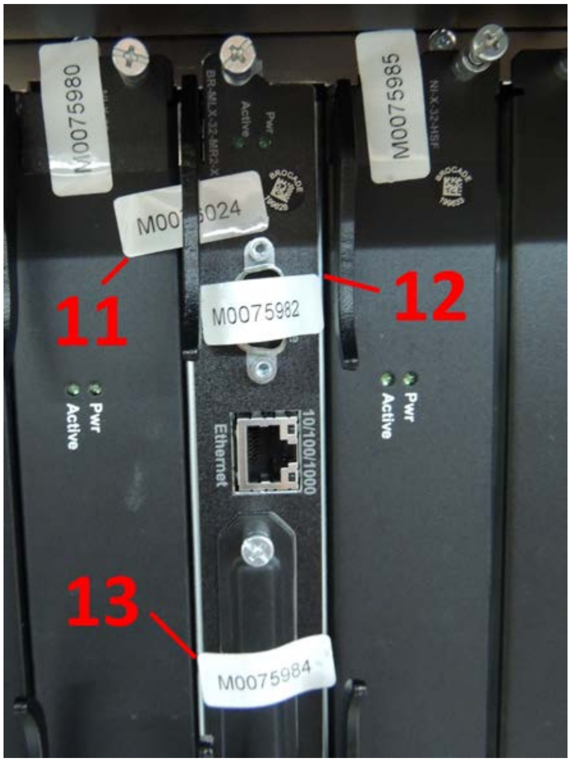

Figure 33 - Label 11 example of MLXe-32

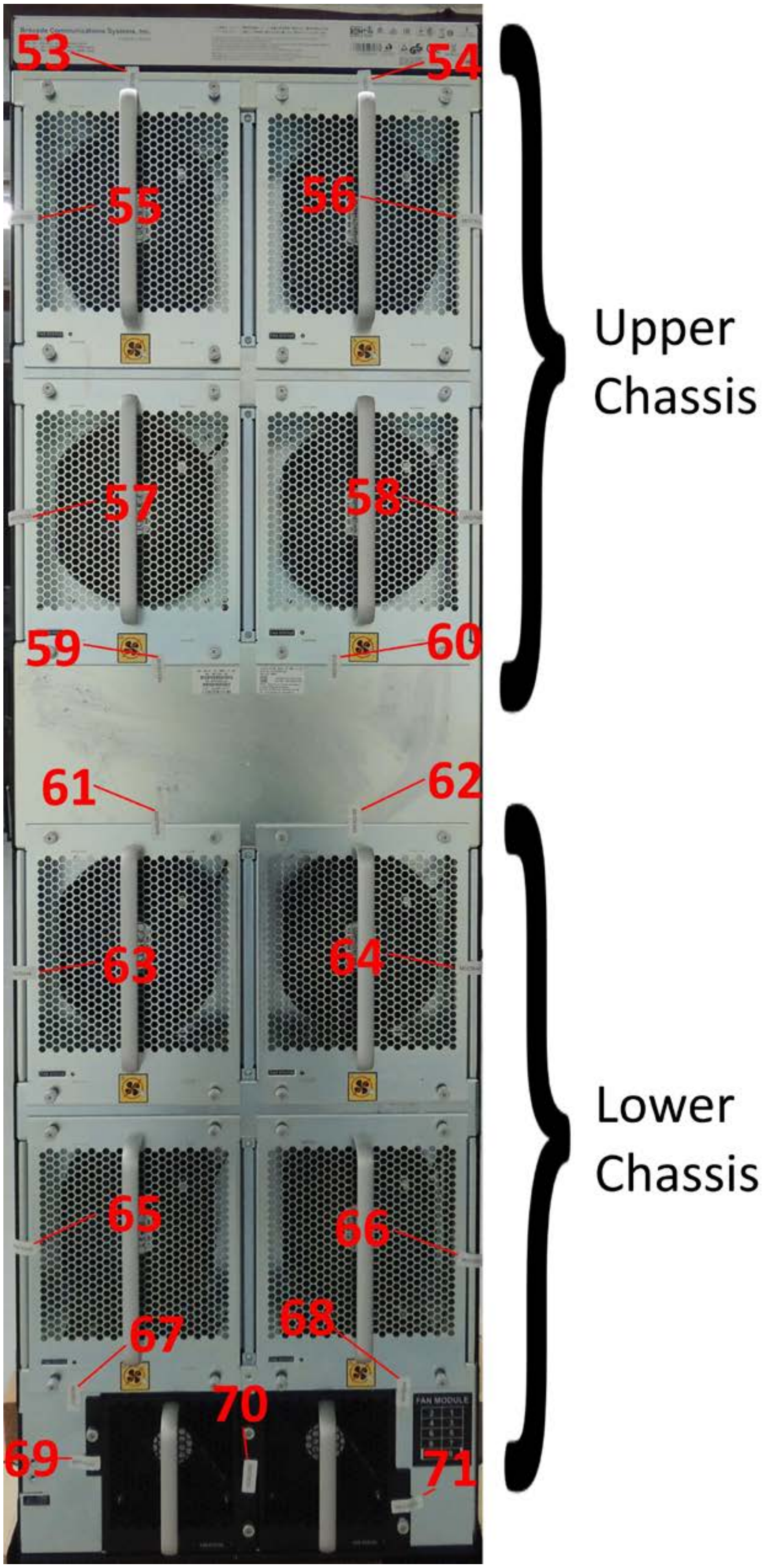

Figure 34 - Back overview of MLXe-32 with tamper labels

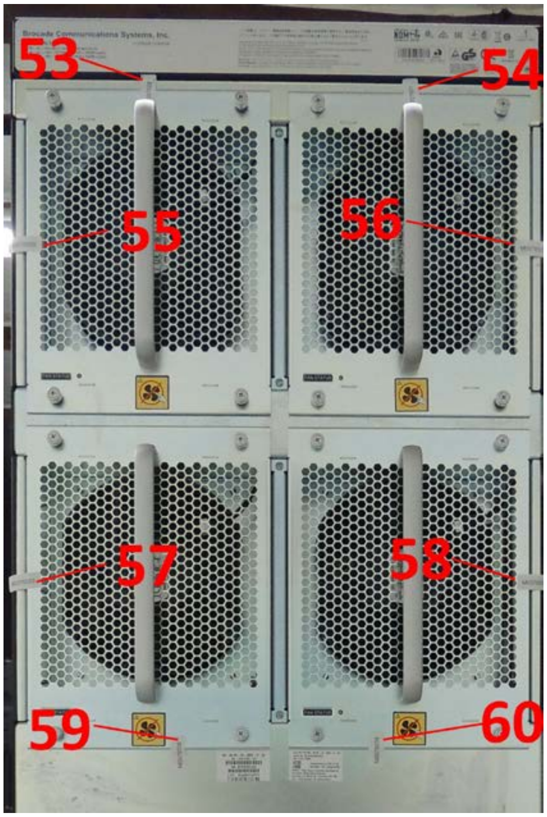

Figure 35 - Back upper chassis of MLXe-32 with tamper labels

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

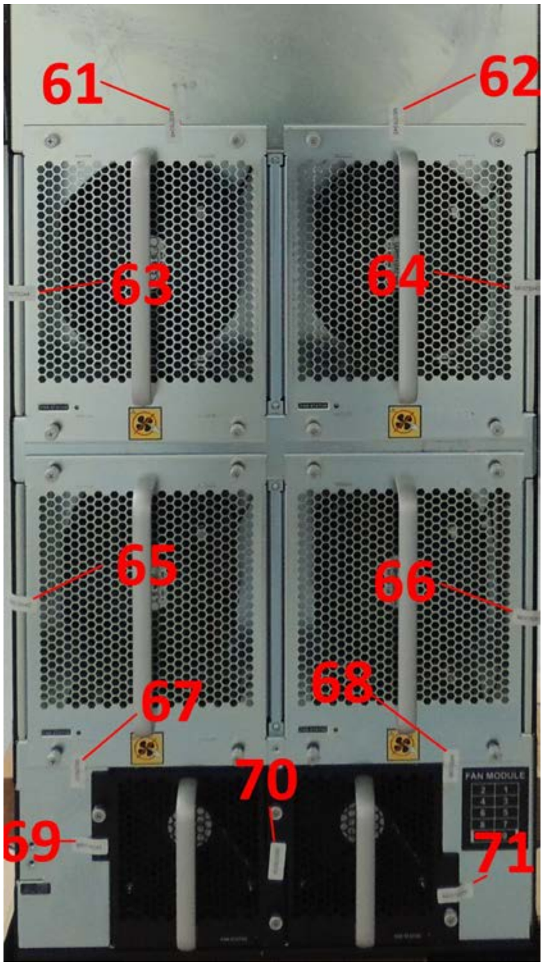

Figure 36 - Back lower chassis of MLXe-32 with tamper labels

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

14.1 Brocade CER 2000 series

14.1.1 CER 2024C-4X-RT devices

Use the figures in this section as a guide for security seal placement on a Brocade NetIron CER 2024C-4X-RT. Brocade NetIron CER 2024C-4X-RT device require the placement of eighteen (18) seals:

- Top front: Affix one (1) seal over each flat head that connects the top cover to the base of the chassis. Five (5) seals are needed to complete this step of the procedure (Seals 1 through 5). One (1) seal is placed vertically over the console port (Seal 18). See Figure 37 for correct seal orientation and positioning.
- Right and left sides: Affix three (3) seals on the left and right sides of the device. The seals must be vertically oriented, cover the flathead screws that attach the top cover to the base of the chassis and wrap around to the bottom of the chassis. Six (6) seals are needed to complete this step of the procedure (Seals 6 through 11). The orientation and placement of seals on the left and right sides mirrors each other. See Figure 38 and Figure 39 for correct seal orientation.
- Rear: Affix six (6) seals across the back of the chassis to inhibit the removal of a power supply, power supply filler panel or fan module. Seal 13 wraps from the top cover to the filler panel. Seals 15 and 16 wrap from the top cover to the fan module. See Figure 40 for correct seal placement. Seal 12 touches both the power supply module and filler panel before wrapping onto the bottom of the chassis. Seals 14 and 17 wrap from the fan module to the bottom of the chassis.
See Figure 40 and Figure 41 for correct seal placement.

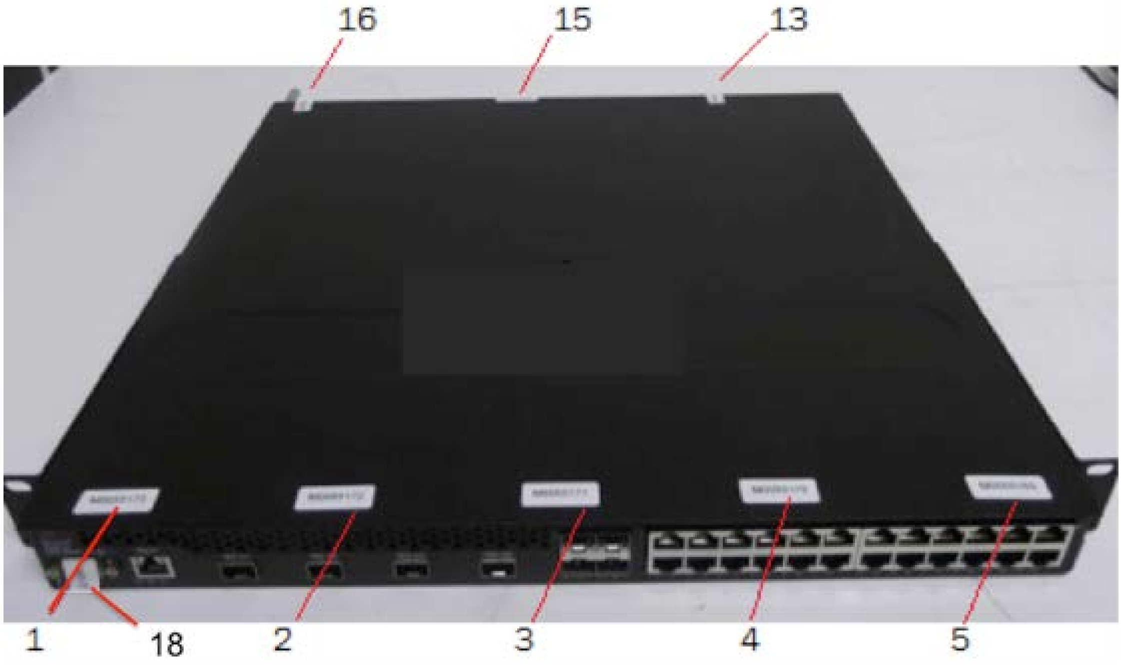

Figure 37 - Top front view of Brocade CER 2024C-4X-RT device with security seals

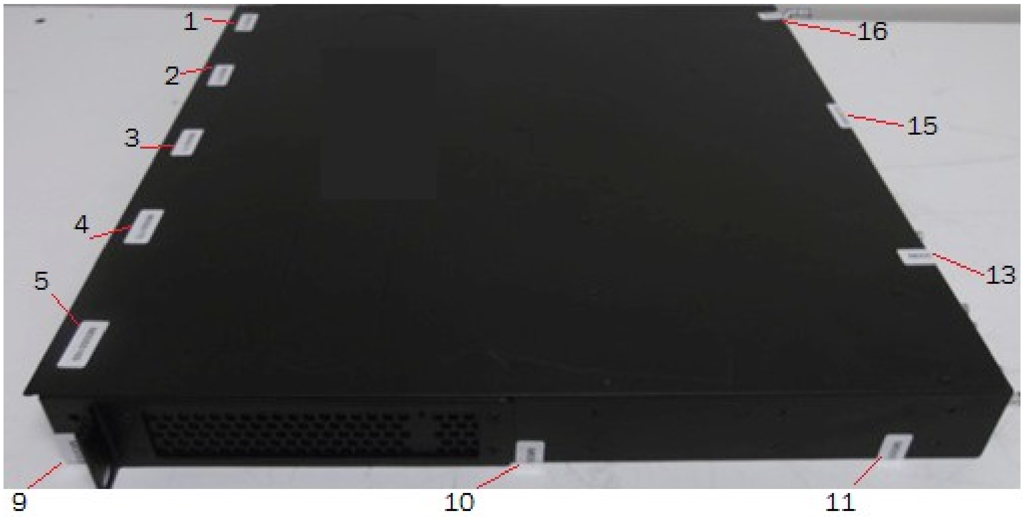

Figure 38 - Right view of Brocade CER 2024C-4X-RT device with security seals

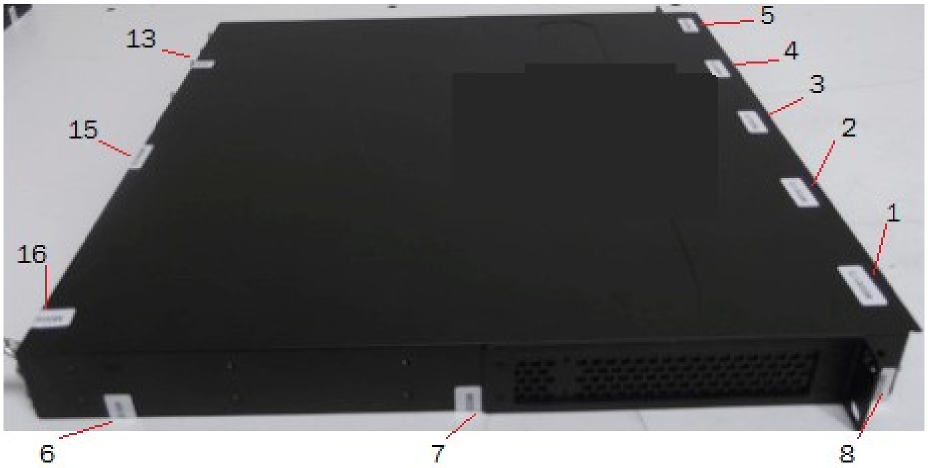

Figure 39 - Left side view of Brocade CER 2024C-4X-RT device with security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

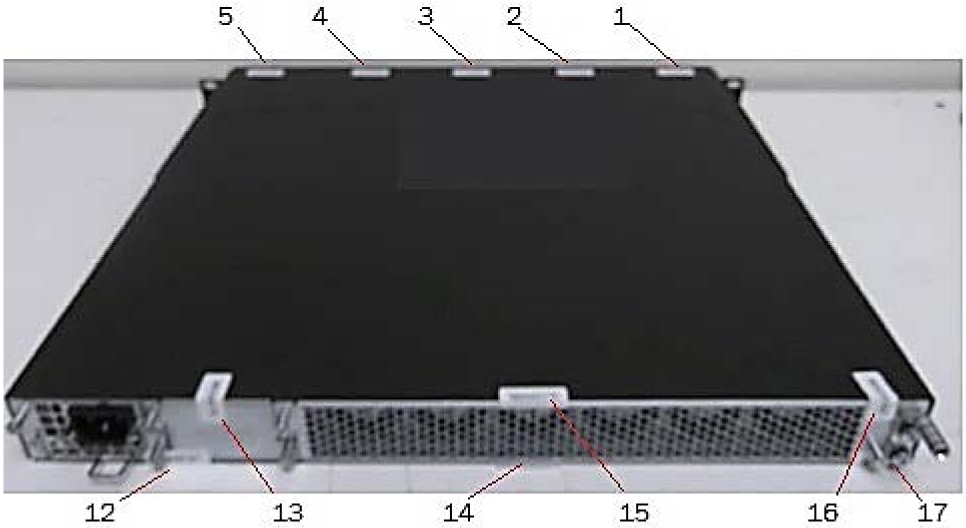

Figure 40 - Rear view of Brocade CER 2024C-4X-RT device with security seals

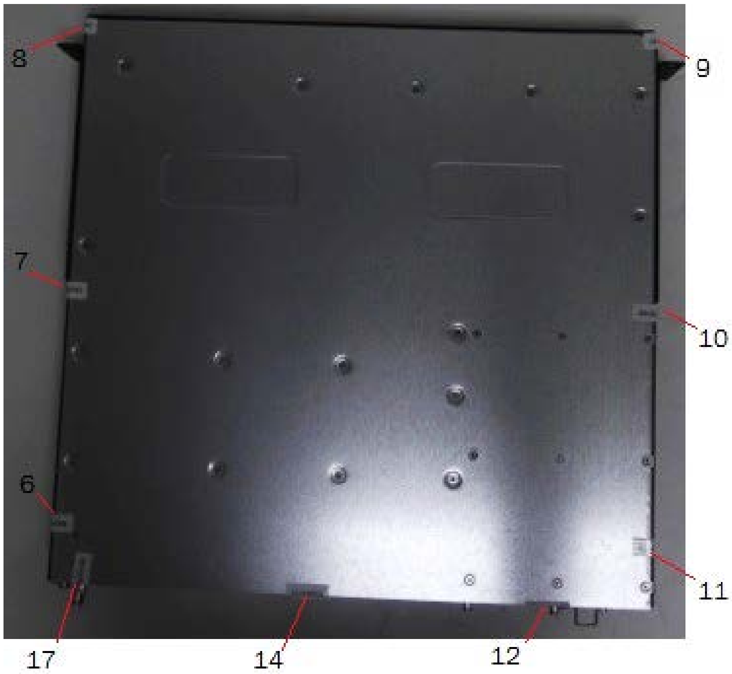

Figure 41 - Bottom view of Brocade CER 2024C-4X-RT device with security seals

14.1.2 CER 2024F-4X-RT devices

Use the figures in this section as a guide for security seal placement on a Brocade NetIron CER 2024F-4X-RT. Brocade NetIron CER 2024F-4X-RT devices require the placement of twenty (20) seals:

- Top front: Affix one (1) seal over each flat head that connects the top cover to the base of the chassis. Five (5) seals are needed to complete this step of the procedure (Seals 1 through 5). 1 seal is placed vertically over the console port (Seal 20). See Figure 42 for correct seal orientation and positioning.
- Right and left sides: Affix three (3) seals on the left and right sides of the device. The seals must be vertically oriented, cover the flathead screws that attach the top cover to the base of the chassis and wrap around to the bottom of the chassis. Six (6) seals are needed to complete this step of the procedure (Seals 6 through 11). The orientation and placement of seals on the left and right sides mirrors each other. See Figure 43 and Figure 44 for correct seal orientation.
- Rear: Affix eight (8) seals across the back of the chassis to inhibit the removal of a power supply, power supply filler panel or fan module. Seal 12 wraps from the top cover to the filler panel. Seal 13 wraps from the filler panel to the bottom of the chassis. Seal 14 wraps from power supply module to the top of the chassis. Seal 15 wraps from the bottom cover to the power supply module. Seals 16 and 19 wrap from the top cover to the fan module. Seal 17 and 18 wrap from the fan module to the bottom side of the chassis. See Figure 45 and Figure 46 for correct seal orientation and positioning.

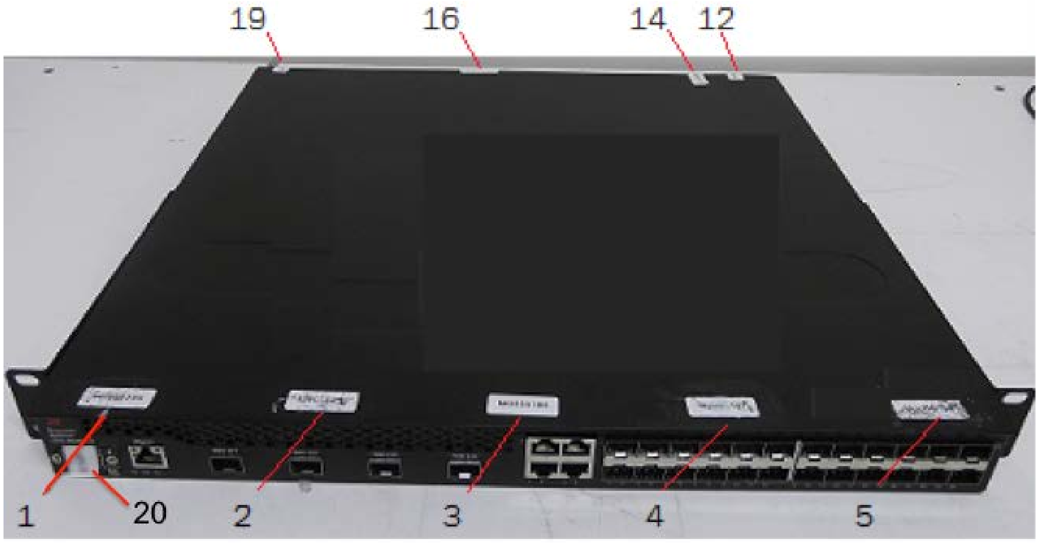

Figure 42 - Top front view of Brocade CER 2024F-4X-RT device with security seals

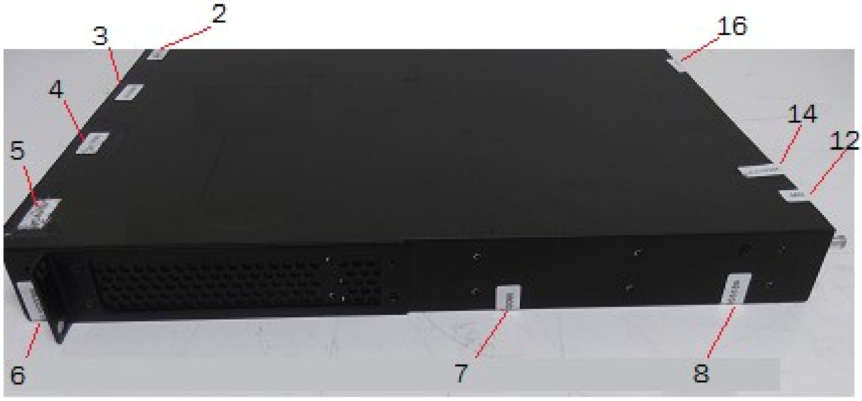

Figure 43 - Right side view of Brocade CER 2024F-4X-RT device with security seals

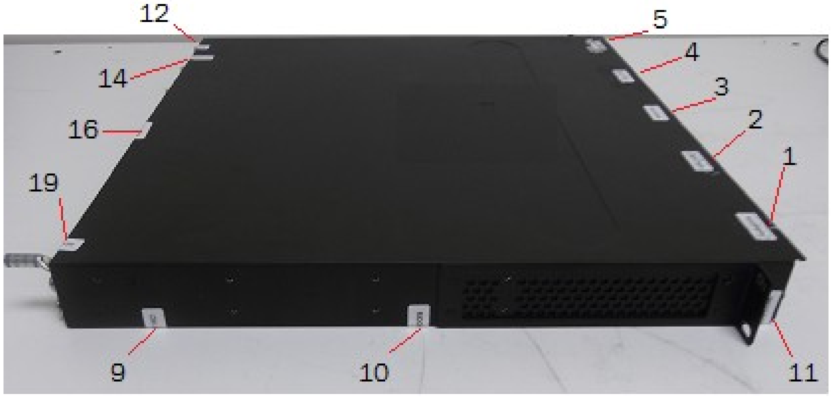

Figure 44 - Left side view of Brocade CER 2024F-4X-RT device with security seals

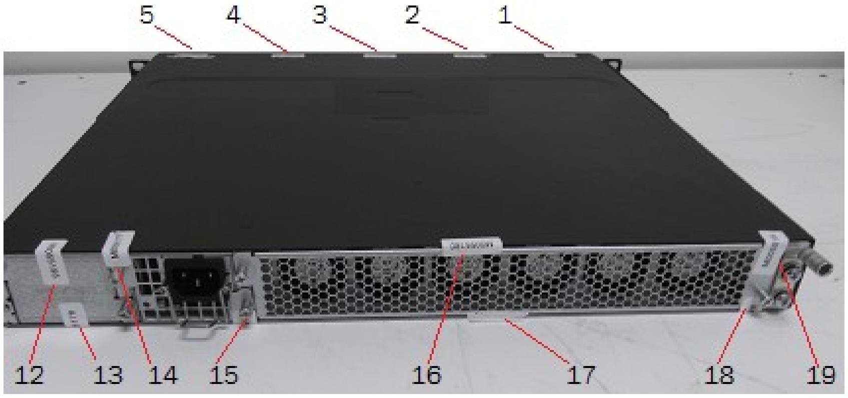

Figure 45 - Rear view of Brocade CER 2024F-4X-RT device with security seals

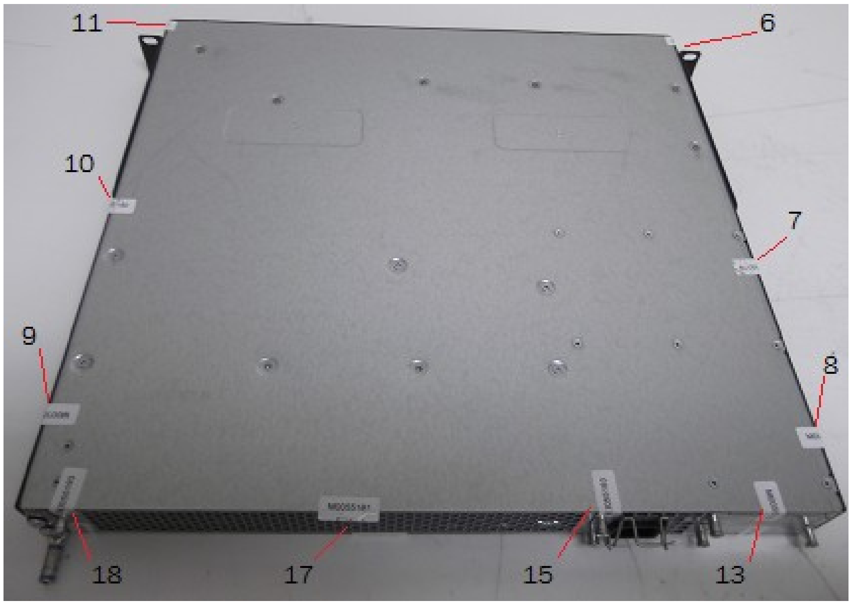

Figure 46 - Bottom view of Brocade CER 2024F-4X-RT device with security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

14.2 Brocade CES 2000 series devices

14.2.1 CES 2024C-4X devices

Use the figures in this section as a guide for security seal placement on Brocade NetIron CES 2024C-4X device. Brocade NetIron CES 2024C-4X device require the placement of twenty (20) seals:

- Top front: Affix one (1) seal over each flat head that connects the top cover to the base of the chassis. Five (5) seals are needed to complete this step of the procedure (Seals 1 through 5). One (1) seal is placed vertically over the console port (Seal 20). See Figure 47 for the correct seal orientation and positioning.
- Right and left sides: Affix three (3) seals on the left and right sides of the device. The seals must be vertically oriented, cover the flathead screws that attach the top cover to the base of the chassis and wrap around to the bottom of the chassis. Six (6) seals are needed to complete this step of the procedure (Seals 6 through 11). See Figure 48 and Figure 49 for correct seal orientation. The orientation and placement of seals on the left and right sides mirrors each other.
- Rear: Affix eight (8) seals across the back of the chassis to inhibit the removal of a power supply, power supply filler panel or fan module. Seal 12 wraps from the top cover to the filler panel. Seal 13 wraps from the bottom cover of the chassis to the filler panel. Seal 14 wraps from the top cover to the power supply module. Seals 16 and 18 wrap from the top cover to the fan module. Seal 15 wraps from the power supply module to the bottom of the chassis. Seals 17 and 19 wrap from the fan module to the bottom of the chassis. See Figure 50 and Figure 51 for correct seal orientation and positioning.

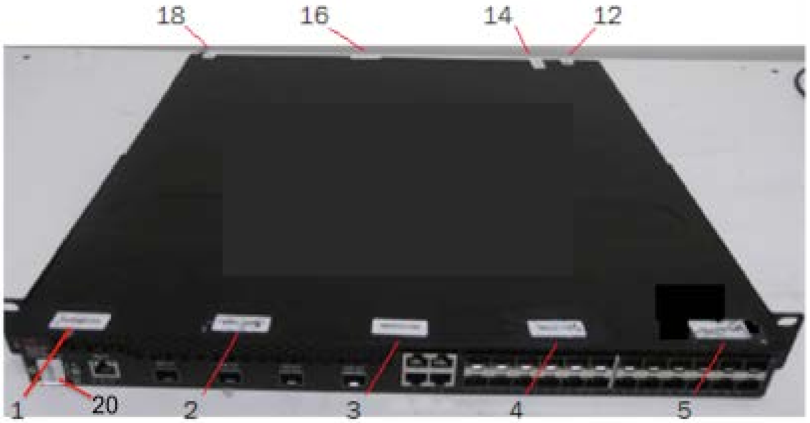

Figure 47 - Top front view of Brocade CES 2024C-4X device with security seals

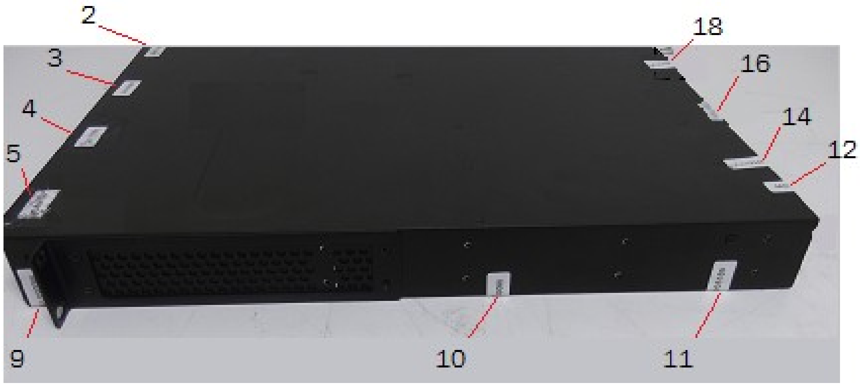

Figure 48 - Right side view of Brocade CES 2024C-4X device with security seals

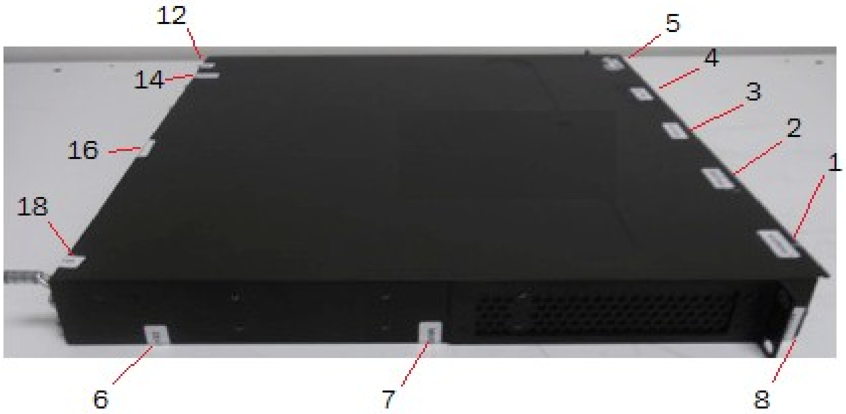

Figure 49 - Left side view of Brocade CES 2024C-4X device with security seals

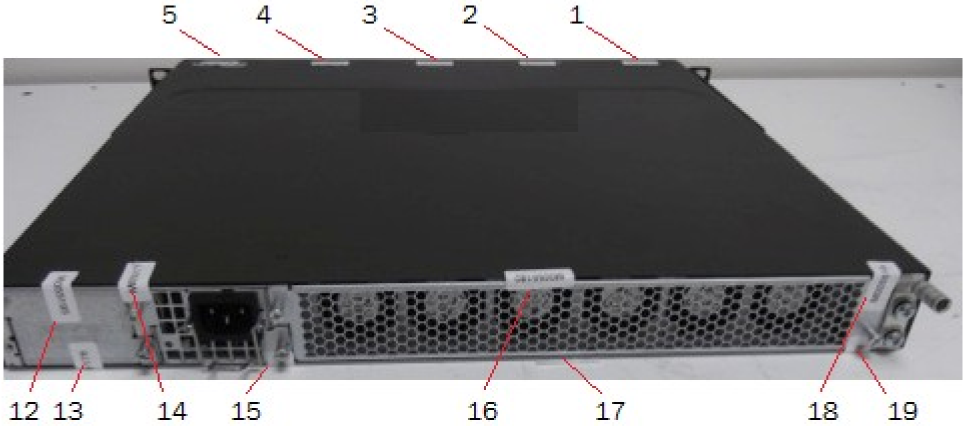

Figure 50 - Rear view of Brocade CES 2024C-4X device with security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

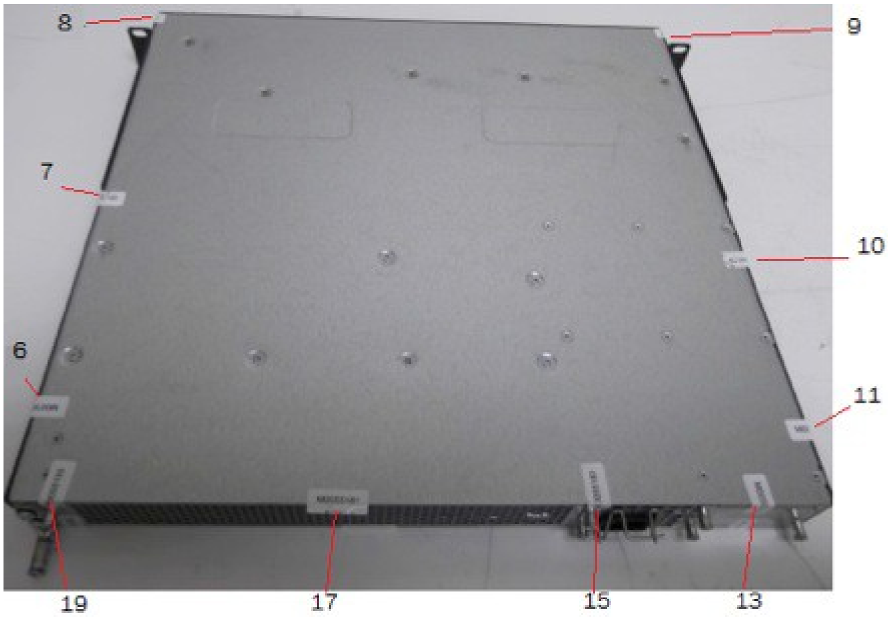

Figure 51 - Bottom view of Brocade CES 2024C-4X device with security seals

14.2.2 CES 2024F-4X devices

Use the figures in this section as a guide for security seal placement on Brocade NetIron CES 2024F-4X device. Brocade NetIron CES 2024F-4X device require the placement of twenty (20) seals:

- Top front: Affix one (1) seal over each flat head that connects the top cover to the base of the chassis. Five (5) seals are needed to complete this step of the procedure (Seals 1 through 5). One (1) seal is placed vertically over the console port (Seal 20). See Figure 52 for the correct seal orientation and positioning.
- Right and left sides: Affix three (3) seals on the left and right sides of the device. The seals must be vertically oriented, cover the flathead screws that attach the top cover to the base of the chassis and wrap around to the bottom of the chassis. 6 seals are needed to complete this step of the procedure (Seals 6 through 11). See Figure 53 and Figure 54 for correct seal orientation. The orientation and placement of seals on the left and right sides mirrors each other.
- Rear: Affix eight (8) seals across the back of the chassis to inhibit the removal of a power supply, power supply filler panel or fan module. Seal 12 wraps from the top cover to the filler panel. Seal 13 wraps from the bottom of the chassis to the filler panel. Seal 14 wraps from the top cover to the power supply module. Seals 16 and 18 wrap from the top cover to the fan module. Seal 15 touches the power supply module before wrapping onto the bottom of the chassis. Seals 17 and 19 wrap from the fan module to the bottom of the chassis. See Figure 55 and Figure 56 for correct seal orientation and positioning.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

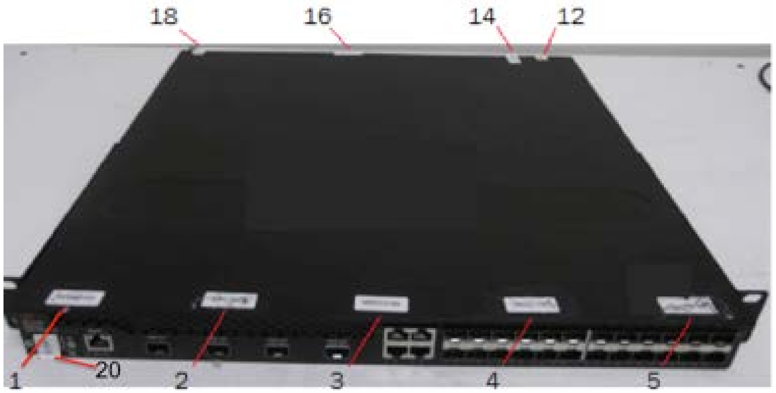

Figure 52 - Top front view of Brocade CES 2024F-4X device with security seals

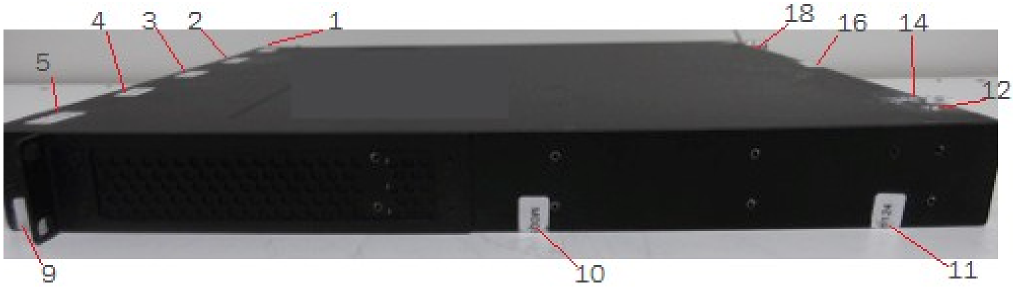

Figure 53 - Right side view of Brocade CES 2024F-4X device with security seals

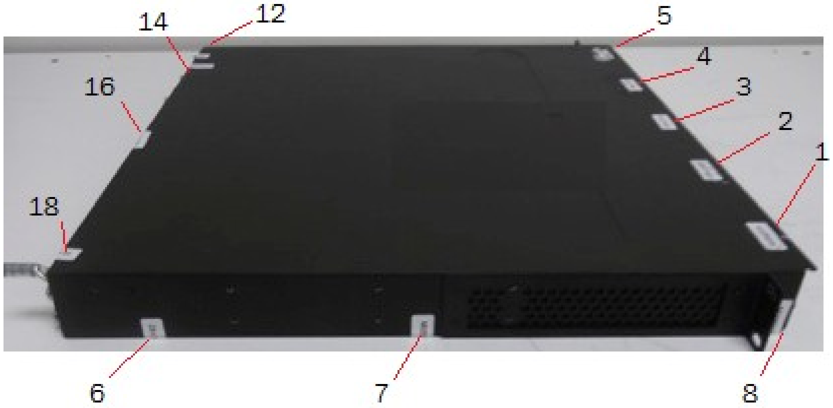

Figure 54 - Left side view of Brocade CES 2024F-4X device with security seals

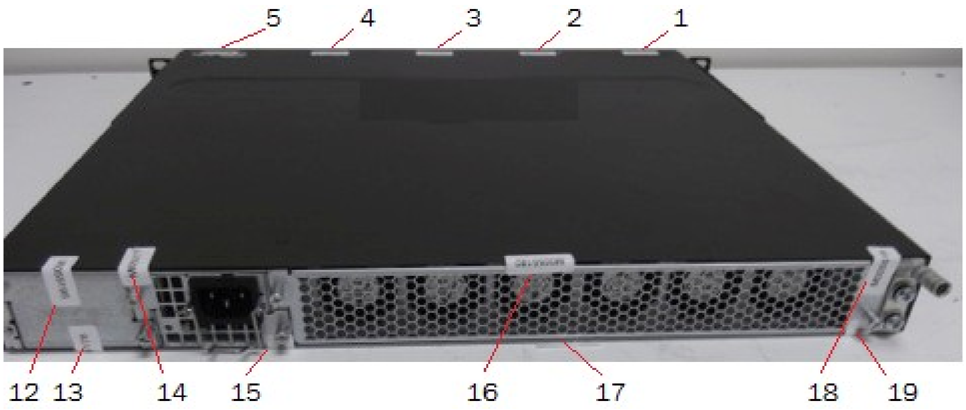

Figure 55 - Rear side view of Brocade CES 2024F-4X device with security seals

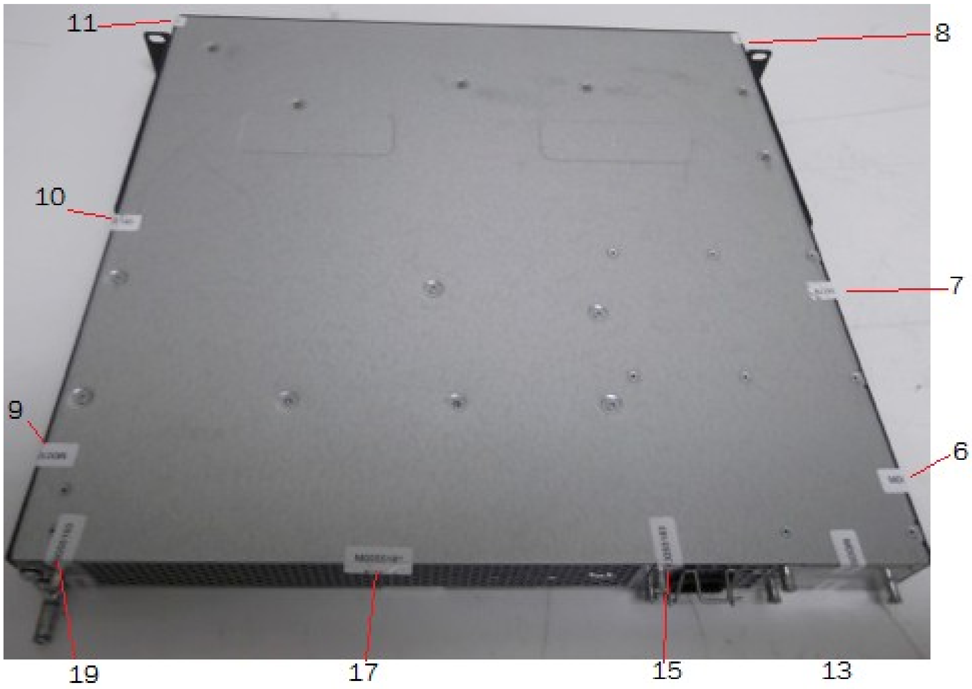

Figure 56 - Bottom view of Brocade CES 2024F-4X device with security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

15 Appendix B: Critical Security Parameters

NOTE: These are abbreviations used in this section.

Term used in this section	description
MLXe-MACsec cards	This abbreviation refers to the following interface cards: • BR-MLX-10GX20-M, • BR-MLX-1GX20-U10G-M, • BR-MLX-10GX20-X2, • BR-MLX-1GX20-U10G-X2 • BR-MLX-10GX4-IPSEC-M
MLXe-IPsec card	This abbreviation refers to the BR-MLX-10GX4-IPSEC-M interface card.
MLXe-MP-MGMT card	This abbreviation refers to the following interface cards: • BR-MLX-MR2-M • BR-MLX-MR2-X • BR-MLX-32-MR2-M • BR-MLX-32-MR2-X
CES-CER devices	Brocade CES 2000 series and CER 2000 series product models.

Table 62 - Acronyms used in appendix B

The module supports the following CSPs and public keys:

15.1 Authentication Key

1) IKEv2/IPSec Authentication Key (MLXe-IPsec card)

- Description: Authentication

- Type: 256 bits or 384 bits HMAC

- Generation: N/A

- Establishment: IKEv2 KDF as per SP800-135 Section 4.1.1; allowed method as per FIPS 140-2 IG D.8 Scenario 4

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: IKEv2 SPI

- Zeroization: "fips zeroize all" command

2) Local - Crypto-officer Password (MLXe-MP-MGMT card, CES-CER devices)

- Description: Locally configured password used to authenticate operators (8 to 48 characters)
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Entered AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Output: Output AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Storage: Plaintext in Compact Flash
- Key-to-Entity: user
- Zeroization: "fips zeroize all" command

3) Local - Port Administrator Password (MLXe-MP-MGMT card, CES-CER devices)

- Description: Locally configured password used to authenticate operators (8 to 48 characters)
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Entered AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Output: Output AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Storage: Plaintext in Compact Flash
- Key-to-Entity: user
- Zeroization: "fips zeroize all" command

4) Local - User Password (MLXe-MP-MGMT card, CES-CER devices)

- Description: Locally configured password used to authenticate operators (8 to 48 characters)
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Entered AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Output: Output AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Storage: Plaintext in Compact Flash
- Key-to-Entity: user
- Zeroization: "fips zeroize all" command

5) SSHv2/SCP Authentication Key (HMAC-SHA-1, 160 bits) (MLXe-MP-MGMT card, CES-CER devices)

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

- Type: HMAC-SHA-1

- Generation: N/A

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

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: User

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

6) TLS Authentication Key (MLXe-MP-MGMT card, CES-CER devices)

- Description: HMAC-SHA-1 key (20 bytes) used to provide data authentication for TLS v1.0/1.1 sessions; HMAC-SHA-256 key (32 bytes) used to provide data authentication for TLS v1.2 sessions

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

- Generation: N/A

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

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: user

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

15.2 KDF

7) IKEv2 KDF State (MLXe-IPsec card)

- Description: IKEv2 KDF State on LP

- Type: HMAC-SHA-256 and HMAC-SHA-384

- Generation: N/A

- Establishment: IKEv2 KDF as per SP800-135 Section 4.1.1; allowed method as per FIPS 140-2 IG D.8 Scenario 4

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: IKEv2 SPI

- Zeroization: "fips zeroize all" command

8) MKA Integrity Checksum Key (ICK) (MLXe-MP-MGMT card)

- Description: Integrity Checksum Key - 128 bits in length on MP
- Type: AES-CMAC
- Generation: Approved as per FIPS 140-2 IG 7.10; derived from SP800-108 KDF
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process MKA
- Zeroization: Session termination and "fips zeroize all" command

9) MKA Key Encryption Key (KEK) (MLXe-MP-MGMT card)

- Description: Key Encryption Key - 128 bits on MP
- Type: AES Key Wrap
- Generation: Approved as per FIPS 140-2 IG 7.10; derived from SP800-108 KDF
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process MKA
- Zeroization: Session termination and "fips zeroize all" command

10) MKA SP800-108 KDF State (MLXe-MP-MGMT card)

- Description: KDF State on MP
- Type: SP800-108
- Generation: Via SP800-108 KDF
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process MKA
- Zeroization: Session termination and "fips zeroize all" command

11) SSHv2 KDF Internal State (MLXe-MP-MGMT card, CES-CER devices)

- Description: Used to generate Host encryption and authentication key on MP
- Type: SHA-256
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: user
- Zeroization: Session termination and "fips zeroize all" command

12) TLS KDF Internal State (MLXe-MP-MGMT card, CES-CER devices)

- Description: Values of the KDF internal state on MP
- Type: TLS v1.0/1.1 (HMAC-SHA-1/HMAC-MD5); TLS v1.2 (HMAC-SHA-256)
- Generation: N/A
- Establishment: TLS v1.0/1.1 and TLS v1.2 KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: user
- Zeroization: Session termination and "fips zeroize all" command

13) SNMPv3 KDF State (MLXe-MP-MGMT card)

- Description: SHA-1 Key Localization Function
- Generation: N/A
- Establishment: SNMPv3 KDF (SP800-135 Section 5.4); allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-To-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

15.3 Line card (LP) DRBG

14) LP DRBG Internal State (MLXe-IPsec card)

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

15) LP DRBG Seed (MLXe-IPsec card)

- Description: Seeding material for the SP800-90A HASH_DRBG: 440 bits
- 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 all" command

16) LP DRBG Value C (MLXe-IPsec card)

- Description: Internal State of SP800-90A HASH_DRBG: 440 bits
- Type: SP800-90A DRBG
- Generation: SP800-90A DRBG
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

17) LP DRBG Value V (MLXe-IPsec card)

- Description: Internal State of SP800-90A HASH_DRBG: 440 bits
- Type: SP800-90A DRBG
- Generation: SP800-90A DRBG
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

15.4 Management card (MP) DRBG

18) MP DRBG Internal State (MLXe-MP-MGMT card, CES-CER devices)

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

19) MP DRBG Seed (MLXe-MP-MGMT card, CES-CER devices)

- Description: Seeding material for the SP800-90A CTR_DRBG
- 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 all" command

20) MP DRBG Value V (MLXe-MP-MGMT card, CES-CER devices)

- Description: Internal State of SP800-90A CTR_DRBG: 128 bits
- Type: SP800-90A DRBG
- Generation: SP800-90A DRBG
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

21) MP DRBG Key (MLXe-MP-MGMT card, CES-CER devices)

- Description: Internal State of SP800-90A CTR_DRBG: 256 bits
- Type: SP800-90A DRBG
- Generation: SP800-90A DRBG
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

15.5 Private Keys

*** SSHv2 ***

22) SSHv2 Client RSA Private Key (MLXe-MP-MGMT card, CES-CER devices)

- Description: (2048 bit); Used to establish shared secrets (SSHv2)
- Type: RSA Private Key
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

23) SSHv2 DH Group-14 Private Key 2048 bit MODP (MLXe-MP-MGMT card, CES-CER devices)

- Description: Used in SCP and SSHv2 to establish a shared secret
- Type: DH Private Key
- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is Approved as per SP800-56A
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process
- Zeroization: Session termination and "fips zeroize all" command

24) SSHv2 Host RSA Private Key (2048 bit) (MLXe-MP-MGMT card, CES-CER devices)

- Description: Used to authenticate SSHv2 server to client
- Type: RSA Private Key
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
- Establishment: N/A
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM and BER encoded (plaintext) in Compact Flash
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

*** TLS ***

25) TLS Host RSA Private Key (RSA 2048 bit) (MLXe-MP-MGMT card)

- Description: RSA key used to establish TLS v1.0/1.1 and TLS v1.2 sessions
- Type: RSA Private Key
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method
- Establishment: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session; Approved as per FIPS 140-2 IG D.9
- Entry: AES Encrypted and HMAC-SHA-1 authenticated over SSHv2 session
- Output: N/A
- Storage: Plaintext in RAM and DER encoded (plaintext) in Compact Flash
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

26) TLS Host DH Group-14 Private Key 2048 bit MODP (MLXe-MP-MGMT card)

- Description: Used in TLS to establish a Pre-Master secret

- Type: DH Private Key

- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is Approved as per SP800-56A

- Establishment: N/A

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: Process

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

*** IKEv2 ***

27) IKEv2 DH Group-14 Private Key 2048 bit MODP (MLXe-IPsec card)

- Description: DH private key

- Type: DH

- 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 Approved as per SP800-56A

- Establishment: N/A

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: IKEv2 SPI

- Zeroization: "fips zeroize all" command

28) IKEv2 ECDH Group-19 Private Key (P-256) (MLXe-IPsec card)

- Description: ECDH private key

- Type: ECDH

- 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: N/A

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: IKEv2 SPI

- Zeroization: "fips zeroize all" command

29) IKEv2 ECDH Group-20 Private Key (P-384) (MLXe-IPsec card)

- Description: ECDH private key

- Type: ECDH

- 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: N/A

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: IKEv2 SPI

- Zeroization: "fips zeroize all" command

30) IKEv2 ECDSA Private Key (P-256) (MLXe-MP-MGMT and MLXe-IPsec cards)

- Description: Private Key

- Type: ECDSA

- Generation: - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method (MLXe-MP-MGMT card)

- Establishment: N/A

- Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9 (MLXe-MP-MGMT card)

- Output: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9 (MLXe-MP-MGMT card)

- Storage: Local persistent on MM and running on Power PC Flash (MLXe-MP-MGMT and MLXe-IPsec cards)

- Key-to-Entity: IKEv2/IPsec Peer role (MLXe-MP-MGMT and MLXe-IPsec cards)

- Zeroization: "fips zeroize all" command

31) IKEv2 ECDSA Private Key (P-384) (MLXe-MP-MGMT and MLXe-IPsec cards)

- Description: Private Key

- Type: ECDSA

- Generation: - Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method (MLXe-MP-MGMT card only)

- Establishment: N/A

- Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9 (MLXe-MP-MGMT card)

- Output: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9 (MLXe-MP-MGMT card)

- Storage: Local persistent on MM and running on Power PC Flash (MLXe-MP-MGMT and MLXe-IPsec cards)

- Key-to-Entity: IKEv2/IPsec Peer role (MLXe-MP-MGMT and MLXe-IPsec card)

- Zeroization: "fips zeroize all" command

*** PKI ***

32) PKI SCEP Enrollment RSA 2048-bit Private Key (MLXe-MP-MGMT card)

- Description: One time key: SCEP protocol signing. Generated during certificate enrollment

- Type: RSA key pair

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

- Establishment: N/A

- Entry: N/A

- Output: N/A

- Storage: Temporarily stored in memory not Flash

- Key-to-Entity: IKEv2/IPsec Peer role

- Zeroization: Key is destroyed/zeroized as soon as the SCEP enrollment is complete.

15.6 Public Keys

*** SSHv2 ***

33) SSHv2 Client RSA Public Key (MLXe-MP-MGMT card and CES-CER devices)

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

- Type: RSA Public Key

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

- Establishment: N/A

- Entry: N/A

- Output: Plaintext

- Storage: Plaintext in RAM, Plaintext in Compact Flash

- Key-to-Entity: Process

34) SSHv2 DH Group-14 Peer Public Key 2048 bit MODP (MLXe-MP-MGMT card and CES-CER devices)

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

- Type: DH Peer Public Key

- Generation: N/A

- Establishment: N/A

- Entry: Plaintext

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: Process

35) SSHv2 DH Group-14 Public Key 2048 bit MODP (MLXe-MP-MGMT card and CES-CER devices)

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

- Type: DH Public Key

- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is Approved as per SP800-56A

- Establishment: N/A

- Entry: N/A

- Output: Plaintext

- Storage: Plaintext in RAM, Plaintext in Compact Flash

- Key-to-Entity: Process

36) SSHv2 Host RSA Public Key (2048 bit) (MLXe-MP-MGMT card and CES-CER devices)

- Description: Used to establish shared secrets (SSHv2)

- Type: RSA Public Key

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

- Establishment: N/A

- Entry: N/A

- Output: Plaintext

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

- Key-to-Entity: Process

*** TLS ***

37) TLS Host RSA Public Key (RSA 2048 bit) (MLXe-MP-MGMT card)

- Description: Used by client to encrypt TLS pre-master secret

- Type: TLS host Public key

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

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

- Entry: AES Encrypted and HMAC-SHA-1 authenticated over SSHv2 session

- Output: Plaintext

- Storage: Plaintext in RAM, Plaintext in Compact Flash

- Key-to-Entity: Process

38) TLS Peer Public Key (RSA 2048 bit) (MLXe-MP-MGMT card and CES-CER devices)

- Description: Used to authenticate the client

- Type: TLS Peer Public Key

- Generation: N/A

- Establishment: N/A

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

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: Process

39) TLS Host DH Group-14 Public Key 2048 bit MODP (MLXe-MP-MGMT card)

- Description: Used in TLS to establish a Pre-Master secret

- Type: DH Public Key

- Generation: As per SP800-133 Section 6.2, the random value (K) needed to generate key pairs for the finite field is the output of the SP800-90A DRBG; this is Approved as per SP800-56A

- Establishment: N/A

- Entry: N/A

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

- Storage: Plaintext in RAM

- Key-to-Entity: Process

40) TLS Peer DH Group-14 Public Key 2048 bit MODP (MLXe-MP-MGMT card)

- Description: Used in TLS to establish a Pre-Master secret

- Type: DH Public Key

- Generation: N/A

- Establishment: N/A

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

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: Process

*** IKEv2 ***

41) IKEv2 DH Group-14 Public Key 2048 bit MODP (MLXe-IPsec card)

- Description: DH public key

- Type: DH

- 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 Approved as per SP800-56A

- Establishment: N/A

- Entry: N/A

- Output: Plaintext

- Storage: Plaintext in RAM

- Key-to-Entity: IKEv2 SPI

42) IKEv2 ECDH Group-19 Public Key (P-256) (MLXe-IPsec card)

- Description: ECDH public key

- Type: ECDH

- 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: N/A

- Entry: N/A

- Output: Plaintext

- Storage: Plaintext in RAM

- Key-to-Entity: IKEv2 SPI

43) IKEv2 ECDH Group-20 Public Key (P-384) (MLXe-IPsec card)

- Description: ECDH public key

- Type: ECDH

- 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: N/A

- Entry: N/A

- Output: Plaintext

- Storage: Plaintext in RAM

- Key-to-Entity: IKEv2 SPI

44) IKEv2 ECDSA Public Key (P-256) (MLXe-MP-MGMT and MLXe-IPsec cards)

- Description: Public Key

- Type: ECDSA

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

- Establishment: N/A

- Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9 (MLXe-MP-MGMT card only)

- Output: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9 (MLXe-MP-MGMT card only)

- Storage: Plaintext in RAM, Plaintext in Compact Flash (MLXe-MP-MGMT and MLXe-IPsec cards)

- Key-to-Entity: IKEv2/IPsec Peer role (MLXe-MP-MGMT and MLXe-IPsec cards)

45) IKEv2 ECDSA Public Key (P-384)

- Description: Public Key

- Type: ECDSA

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

- Establishment: N/A

- Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9 (MLXe-MP-MGMT card)

- Output: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9 (MLXe-MP-MGMT card)

- Storage: Plaintext in RAM, Plaintext in Compact Flash (MLXe-MP-MGMT and MLXe-IPsec cards)

- Key-to-Entity: IKEv2/IPsec Peer role (MLXe-MP-MGMT and MLXe-IPsec cards)

*** PKI ***

46) PKI SCEP Enrollment RSA 2048-bit Public Key (MLXe-MP-MGMT card)

- Description: One time key: SCEP protocol signing. Generated during certificate enrollment

- Type: RSA key pair

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

- Establishment: N/A

- Entry: N/A

- Output: N/A

- Storage: Temporarily stored in memory not Flash

- Key-to-Entity: IKEv2/IPsec Peer role

*** Firmware ***

47) Firmware Load RSA Public Key (MLXe-MP-MGMT card and CES-CER devices)

- Description: RSA 2048-bit public key used to verify signature of firmware of the module
- Type: RSA Public Key
- Generation: N/A, Generated outside the module
- Establishment: N/A
- Entry: Through firmware update
- Output: N/A
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: Process

15.7 Session Keys

*** IKEv2 ***

48) IKEv2 Encrypt/Decrypt Key (MLXe-IPsec card)

- Description: Encryption/Decryption on LP only used for IKEv2 control packets
- Type: AES-128-CBC and AES-256-CBC
- Generation: N/A
- Establishment: IKEv2 KDF as per SP800-135 Section 4.1.1; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: IKEv2 SPI
- Zeroization: "fips zeroize all" command

*** IPsec ***

49) IPsec ESP Encrypt/Decrypt Key (MLXe-IPsec card)

- Description: Encryption and Decryption on LP used for IPsec encapsulated data packets
- Type: AES-128-GCM and AES-256-GCM
- Generation: N/A
- Establishment: IKEv2 KDF as per SP800-135 Section 4.1.1; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: IPsec SPI
- Zeroization: "fips zeroize all" command

*** MKA ***

50) MKA Secure Association Key (SAK) (MLXe-MP-MGMT card and MLXe-MACsec cards)

- Description: Secure association key on MP

- Type: 128 bits AES-GCM Key

- Generation: Approved as per FIPS 140-2 IG 7.10; derived from SP800-108 KDF (MLXe-MP-MGMT card)

- Establishment: Key transport: AES key wrapped with the KEK; Allowed as per FIPS 140-2 IG D.9 (MLXe-MP-MGMT card)

- Entry: Entered AES key wrapped with the KEK in MKA Peer mode (MLXe-MP-MGMT card)

- Output: Output AES key wrapped with the KEK in MKA server mode (MLXe-MP-MGMT card)

- Storage: Plaintext in RAM, Plaintext in Broadcom chip (MLXe-MP-MGMT card and MLXe-MACsec cards.)

- Key-to-Entity: Process MACsec (MLXe-MP-MGMT card and MLXe-MACsec cards.)

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

*** SSHv2 ***

51) SSHv2/SCP Session Keys (128, 192 and 256 bit (AES CBC and AES CTR) (MLXe-MP-MGMT card, CES-CER devices)

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

- Type: AES CBC Key

- Generation: N/A

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

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

-Key-to-Entity: user

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

*** TLS ***

52) TLS Session Key (MLXe-MP-MGMT card and CES-CER devices)

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

- Type: AES CBC

- Generation: N/A

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

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: user

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

15.8 Shared Secret

*** IKEv2 ***

53) IKEv2 DH Group-14 Shared Secret 2048 bit MODP (MLXe-IPsec card)

- Description: DH shared secret on LP
- Type: DH
- Generation: N/A
- Establishment: IKEv2 DH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: IKEv2 SPI
- Zeroization: "fips zeroize all" command or when the session is deleted.

54) IKEv2 ECDH Group-19 Shared Secret (P-256) (MLXe-IPsec card)

- Description: ECDH shared secret on LP
- Type: ECDH
- Generation: N/A
- Establishment: IKEv2 ECDH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: IKEv2 SPI
- Zeroization: "fips zeroize all" command or when the session is deleted.

55) IKEv2 ECDH Group-20 Shared Secret (P-384) (MLXe-IPsec card)

- Description: ECDH shared secret on LP
- Type: ECDH
- Generation: N/A
- Establishment: IKEv2 ECDH Key Agreement; allowed method as per FIPS 140-2 IG D.8 Scenario 4
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: IKEv2 SPI
- Zeroization: "fips zeroize all" command or when the session is deleted.

56) IKEv2 Pre-Shared Key (PSK) (MLXe-MP-MGMT and MLXe-IPsec card)

- Description: Pre-Shared Key; configured on MP but used on LP

- Type: HMAC (minimum 112 bits to max 100 bytes)

- Generation: N/A

- Establishment: N/A

- Entry: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9 (MLXe-MP-MGMT card)

- Output: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9 (MLXe-MP-MGMT card)

- Storage: Plaintext in RAM (MLXe-MP-MGMT and MLXe-IPsec cards)

- Key-to-Entity: IKEv2 SPI (MLXe-IPsec card)

- Zeroization: "fips zeroize all" command

*** MKA ***

57) MKA Connectivity Association Key (CAK)

- Description: Connectivity Association Key - 128 bits in length on MP

- Type: KDF Input

- Generation: N/A

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

- Entry: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session (MLXe-MP-MGMT card)

- Output: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session (MLXe-MP-MGMT card)

- Storage: Plaintext in RAM, Plaintext in Flash (MLXe-MP-MGMT card)

- Key-to-Entity: Process User (MLXe-MACsec cards)

- Zeroization: "fips zeroize all" command

58) MKA Connectivity Key Name (CKN) (MLXe-MP-MGMT and MLXe-MACsec cards)

- Description: Connectivity Key Name – between 8 bits to 256bits in length on MP

- Type: KDF Input

- Generation: N/A

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

- Entry: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session (MLXe-MP-MGMT card)

- Output: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session (MLXe-MP-MGMT card)

- Storage: Plaintext in RAM, Plaintext in Flash (MLXe-MP-MGMT card)

- Key-to-Entity: Process User (MLXe-MACsec-card)

- Zeroization: "fips zeroize all" command

*** RADIUS ***

59) RADIUS Secret (MLXe-MP-MGMT card and CES-CER devices)

- Description: Used to authenticate the RADIUS server (8 to 64 characters) on MP
- Type: Authentication data
- Generation: N/A
- Establishment: N/A
- Entry: Entered AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Output: Output AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Storage: Plaintext in RAM and Compact Flash
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

*** SNMPv3 ***

60) SNMPv3 secret (MLXe-MP-MGMT card and CES-CER devices)

- Description: Used for authentication (SHA1, Password is 8 to 20 characters long) and for privacy (AES, Password 12 to 16 characters)
- Type: Authentication data and privacy
- Generation: N/A - generated outside of the module
- Establishment: N/A
- Entry: Configured by the operator, entered encrypted/authenticated over SSHv2 session
- Output: SHA1 hashed in configuration, output encrypted / authenticated over SSHv2 session
- Storage: SHA1 digest and AES are stored in Compact Flash
- Key-to-Entity: Process: user
- Zeroization: Session termination and "fips zeroize all" command

61) NTP secret (MLXe-MP-MGMT card and CES-CER devices)

- Description: Authentication (SHA1, Password is 8 to 16 characters long)
- Type: Authentication data
- Generation: N/A - generated outside of the module
- Establishment: N/A
- Entry: Entered AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Output: Entered AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Storage: Plaintext in RAM and Compact Flash
- Key-to-Entity: Process: user
- Zeroization: Session termination and "fips zeroize all" command

*** SSHv2 ***

62) SSHv2 DH Shared Secret Key (2048 bit) (MLXe-MP-MGMT card, and CES-CER devices)

- Description: Output from the DH Key agreement primitive - (K) and (H). This key is used by SSHv2 KDF to derive (client and server) session keys on MP.

- Type: DH Shared Secret Key

- Generation: N/A

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

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: user

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

*** TACACS+ ***

63) TACACS+ Secret (MLXe-MP-MGMT card and CES-CER devices)

- Description: Used to authenticate the TACACS+ packets from the server on MP. Shared secret size is between 8 to 64 characters long

- Type: Authentication data

- Generation: N/A

- Establishment: N/A

- Entry: Entered AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session

- Output: Output AES encrypted & HMAC-SHA-1 authenticated over SSHv2 session

- Storage: Plaintext in RAM and Compact Flash

- Key-to-Entity: Process

- Zeroization: "fips zeroize all" command

*** TLS ***

64) TLS Master Secret (MLXe-MP-MGMT card and CES-CER devices)

- Description: 48 bytes secret value used to establish the TLS Session Key and TLS Authentication Key on MP

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

- Generation: N/A

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

- Entry: N/A

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: user

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

65) TLS Pre-Master Secret (MLXe-MP-MGMT card and CES-CER devices)

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

- Type: 48 bytes TLS v1.0/1.1 and TLS v1.2 CSP

- Generation: Generated when the module behaves as a TLS Client; can also be established during the TLS v1.0/1.1 and TLS v1.2 handshake using RSA key transport

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

- Entry: RSA key wrapped (after padding to block size) during TLS v1.0/1.1 and TLS v1.2 handshake

- Output: N/A

- Storage: Plaintext in RAM

- Key-to-Entity: user

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