Brocade® MLXe® Series Ethernet Routers

FIPS 140-2 Non-Proprietary Security Policy

Document Version 1.0

November 14th, 2017

Brocade Communications Systems, Inc.

Copyright Brocade Communications 2017. May be reproduced only in its original entirety [without revision].

Revision History

Revision History	Revision	Summary of changes
11/14/2017	1.0	Initial version

© 2017 Brocade Communications Systems, Inc. All Rights Reserved.

This Brocade Communications Systems, Inc. Security Policy for Brocade® MLXe® NetIron® Ethernet 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 10
2 Overview 10
2.1 Tamper Evident Seal Application requirement 11
2.2 Differences in features and services across MLXe Hardware family 11
2.2.1 IPSec, MACsec and HTTPS protocol support comparison 11
2.2.2 Power Supply support 12
2.3 Block Diagram 13
3 Brocade MLXe series 14
4 Ports and Interfaces 26
4.1 Brocade MLXe series 26
4.1.1 MLXe MR2 Management Modules (Management cards) 27
4.1.2 BR-MLX-10GX20-M, BR-MLX-10GX20-X2, BR-MLX-1GX20-U10G-M and BR-MLX-1GX20-U10G-X2 line cards 27
4.1.3 BR-MLX-10GX4-IPSEC-M interface line card 27
4.1.4 MLXe Status LED 28
4.2 Modes of Operation 29
4.3 Module Validation Level 29
5 Roles and Services 30
5.1 Roles 30
5.1.1 The Crypto-officer role 30
5.1.2 Port Configuration Administrator role 30
5.1.3 User role 30
5.1.4 IKEv2/IPsec Peer role 30
5.1.5 MACsec Peer role 30
5.1.6 NTP Peer role 30
5.2 Services (Services in Approved mode) 31
5.2.1 Services accessible by Crypto-officer role 34
5.2.1.1 Console 34
5.2.1.2 HTTPS server 34
5.2.1.3 IKEv2/IPsec 35
5.2.1.4 MACsec 36
5.2.1.5 NTP 36
5.2.1.6 SCP 36
5.2.1.7 SNMP 37
5.2.1.8 SSHv2 37
5.2.1.9 Syslog 38
5.2.1.10 TLS client 38
5.2.2 Services accessible by Port Configuration Administrator role 39

5.2.2.1 Console 39
5.2.2.2 HTTPS server 39
5.2.2.3 IKEv2/IPsec 39
5.2.2.4 MACsec 39
5.2.2.5 NTP 39
5.2.2.6 SNMP 39
5.2.2.7 SSHv2 39
5.2.2.8 Syslog 39
5.2.2.9 TLS client 40
5.2.3 Services accessible by User role 40
5.2.3.1 Console 40
5.2.3.2 HTTPS server 40
5.2.3.3 IKEv2/IPsec 40
5.2.3.4 MACsec 40
5.2.3.5 NTP 40
5.2.3.6 SNMP 40
5.2.3.7 SSHv2 41
5.2.3.8 Syslog 41
5.2.3.9 TLS client 41
5.2.4 Services accessible by IKEv2/IPsec Peer role 41
5.2.4.1 IKEv2/IPsec 41
5.2.5 Services accessible by MACsec Peer role 41
5.2.5.1 MACsec 41
5.2.6 Services accessible by NTP Peer role 41
5.2.6.1 NTP 41
5.3 Non-Approved Mode Services 42
5.3.1 Non-Approved Algorithms 46
6 Algorithm certificates 47
6.1 Algorithm certificates in MLXe 47
6.2 Non-Approved but allowed cryptographic methods 49
7 Policies 50
7.1 Security Rules 50
7.1.1 Cryptographic Module Operational Rules 53
7.2 Authentication 53
7.2.1 Line Authentication Method 54
7.2.2 Enable Authentication Method 54
7.2.3 Local Authentication Method 54
7.2.4 RADIUS Authentication Method 55
7.2.5 TACACS+ Authentication Method 55

7.2.6 Strength of Authentication 55
7.2.6.1 IKEv2/IPsec Peer Role 55
7.2.6.2 MACsec Peer Role 56
7.2.6.3 All other roles 56
7.3 Access Control and Critical Security Parameters (CSPs) 57
7.3.1 Access Control and Critical Security Parameters (CSPs) for the Crypto-officer role 57
7.3.2 Access Control and Critical Security Parameters (CSPs) for Port Configuration Administrator role 59
7.3.3 Access Control and Critical Security Parameters (CSPs) for User role 61
7.3.4 Access Control and Critical Security Parameters (CSPs) for IKEv2/IPsec Peer role 63
7.3.5 Access Control and Critical Security Parameters (CSPs) for MACsec role 64
7.3.6 Access Control and Critical Security Parameters (CSPs) for NTP Peer role 64
7.3.7 CSP Zeroization 65
7.4 Physical Security 65
8 Crypto-officer Guidance 66
8.1 FIPS Approved Mode Status 66
8.2 FIPS Approved Mode 68
8.2.1 Invoking FIPS Approved Mode 68
8.2.2 Negating FIPS Approved Mode 69
9 Mitigation of other attacks 69
10 Glossary 70
11 Appendix A: Tamper Evident Seal Application Procedure 71
11.1 Brocade MLXe devices 71
11.1.1 MLXe-4 device 71
11.1.2 MLXe-8 device 73
11.1.3 MLXe-16 device 75
11.1.4 MLXe-32 device 77
12 Appendix B: Critical Security Parameters 88
12.1 Authentication Key 88
12.2 KDF 90
12.3 Line card (LP) DRBG 93
12.4 Management card (MP) DRBG 94
12.5 Private Keys 95
12.6 Public Keys 99
12.7 Session Keys 104
12.8 Shared Secret 106
13 Appendix C: CKG as per SP800-133 111
14 Appendix D: Components Excluded from FIPS 140-2 Requirements 111

Table of tables:

Table 1 - Overview – NetIron devices – Support for IPSec, MACsec and HTTPS protocol 11
Table 2 - Overview –MLXe product interface line card support for IPSec and MACsec protocols 12
Table 3 - Overview – Power Supply support for MLXe products 12
Table 4 - MLXe Series Firmware Version 14
Table 5 - MLXe Series (bundled SKU) Part Numbers 15
Table 6 - MLXe Management Card Part Numbers 15
Table 7 - MLXe Interface Line Card Part Numbers 16
Table 8 - MLXe Interface Line Card Software Upgrade License 16
Table 9 - MLXe Switch Fabric Module Part Numbers 17
Table 10 MLXe Power Supply Module Part Numbers 17
Table 11- MLXe Fan Module Part Numbers 17
Table 12 - MLXe Filler Panel Part Numbers 17
Table 13 - Validated MLXe Configurations 19
Table 14 - Physical/Logical Interface Correspondence 26
Table 15 - 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 28
Table 16 - Power and fan status LEDs for the MR2 Management Module 28
Table 17 - NetIron Security Levels 29
Table 18 – List of services in Approved mode of operation 31
Table 19 - FIPS Approved Cryptographic Functions 32
Table 20 - Non-Approved Cryptographic Functions Allowed in FIPS Approved Mode 33
Table 21 - Functions/Services, Roles in Non-Approved Mode Services 45
Table 22 - Non-Approved Algorithms 46
Table 23 - Algorithm Certificates for the MLXe MR2 Management Modules (Management cards) 48
Table 24 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 48
Table 25 - Algorithm Certificates for BR-MLX-10GX4-IPSEC-M interface line cards 49
Table 26 - Power-Up Self-Tests - Cryptographic Known Answer Tests (KAT) 51
Table 27 - Conditional Self-Tests 52
Table 28 - Summary of authentication methods available for each role 54
Table 29 - Access Control and CSPs for the Crypto-officer role 58
Table 30 - Access Control and CSPs for the Port Configuration role 60
Table 31 - Access Control and CSPs for the User role 62
Table 32 - Access Control and CSPs for the IKEv2/IPsec Peer role 63
Table 33 - Access Control and CSPs for the MACsec role 64
Table 34 - Access Control and CSPs for the NTP Peer role 64
Table 35 - Inspection of Physical Security Mechanisms 65
Table 36 - Sample output - MLXe in non-Approved mode 66
Table 37 - Sample output - MLXe in FIPS Approved mode 67

Table 38 - Mitigation of other attacks....69
Table 39 - Glossary....70
Table 40 - Acronyms used in appendix B....88
Table 41 – SKUs Excluded from FIPS 140-2 requirement - MLXe DC Power Supply Modules.... 111

Table of figures:

Figure 1 - Block Diagram....13
Figure 2 – Brocade MLXe-4....20
Figure 3 – Brocade MLXe-4: Starting from left to right clockwise: Left side, Rear side, Bottom side, Top side, and Right side....20
Figure 4 – Brocade MLXe-8 front view....21
Figure 5 – Brocade MLXe-8: Starting from left to right clockwise: Left side, Rear side, Bottom side, Top side, and Right side....21
Figure 6 – Brocade MLXe-16 – front view....22
Figure 7 – Brocade MLXe-16: Starting from left to right clockwise: Left side, Rear side, Bottom side, Top side, and Right side....23
Figure 8 – Brocade MLXe-32 – front view....24
Figure 9 – Brocade MLXe-32: Starting from left to right clockwise: Front side, Left side, Rear side, Right side, Bottom side, and Top side....25
Figure 10 - Front view of Brocade MLXe-4 with security seals....71
Figure 11 - Rear view of Brocade MLXe-4 device with security seals....72
Figure 12 - Front view of Brocade MLXe-8 device with security seals....73
Figure 13 - Rear view of Brocade MLXe-8 device with security seals....74
Figure 14 - Front view of Brocade MLXe-16 device with security seals....75
Figure 15 - Rear view of Brocade MLXe-16 device with security seals....76
Figure 16 - Front overview of MLXe-32 Configuration 1 with tamper labels....78
Figure 17 - Front upper chassis of MLXe-32 Configuration 1 with tamper labels....79
Figure 18 - Front middle chassis (grill) of MLXe-32 Configuration 1 with tamper labels....79
Figure 19 - Front lower chassis of MLXe-32 Configuration 1 with tamper labels....80
Figure 20 - Front overview of MLXe-32 Configuration 2 with tamper labels....81
Figure 21 - Front overview of MLXe-32 Configuration 2 with tamper labels....82
Figure 22 - Front middle chassis (grill) of MLXe-32 Configuration 2 with tamper labels....82
Figure 23 - Front lower chassis of MLXe-32 Configuration 2 with tamper labels....83
Figure 24 - Label 31 example of MLXe-32....84
Figure 25 - Label 11 example of MLXe-32....84
Figure 26 - Back overview of MLXe-32 with tamper labels....85
Figure 27 - Back upper chassis of MLXe-32 with tamper labels....86
Figure 28 - Back lower chassis of MLXe-32 with tamper labels....87

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.

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.

Brocade MLXe series devices are chassis devices. Each MLXe chassis contains slots for management cards (also known as management modules, see Table 6), Switch Fabric Module (SFM; see Table 9), and interface line cards (see, Table 7). 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 6);
    - One management card runs in active mode while the other is in standby mode.
- One or more Switch Fabric Modules (SFM, see Table 9)
- One or more interface line cards (also, referred to as interface modules; see, Table 7)
- 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.

NEXT PAGE →

2.1 Tamper Evident Seal Application requirement

For an MLXe series to operate as a validated cryptographic module, the tamper evident seals supplied in Brocade XBR-000195 must be installed as defined in section, 11 - 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.

2.2 Differences in features and services across MLXe 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.

2.2.1 IPSec, MACsec and HTTPS protocol support comparison

Tables below show the support for IPSec, MACsec, and HTTPS protocol across NetIron product families.

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

Product Family	Support for IPSec	Support for MACsec	Support for HTTPS
MLXe series	☑ Supports IPSec feature on the IPSec capable interface line cards	☑ Supports MACsec feature on the MACsec capable interface line cards	☑ Provides HTTPS Client/Server support on the management cards

Table 1 - Overview – NetIron devices – Support for IPSec, MACsec and HTTPS protocol

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

Table below shows the specific MLXe interface line cards that support IPsec and MACsec protocol:

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

Table 2 - Overview –MLXe product interface line card support for IPSec and MACsec protocols

2.2.2 Power Supply support

Tables below show the available power supply support for MLXe 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 3 - Overview – Power Supply support for MLXe products

NEXT PAGE →

2.3 Block Diagram

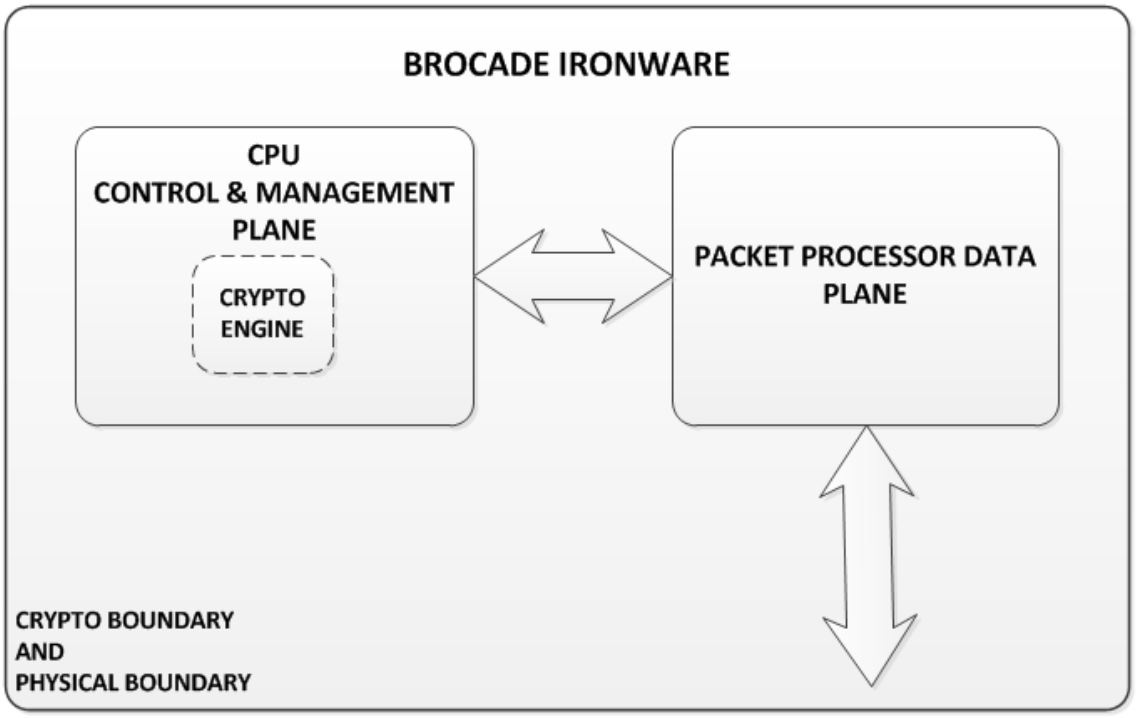

Figure 1 - Block Diagram

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

3 Brocade MLXe series

Firmware
Multi-Service IronWare R06.0.00aa

Table 4 - MLXe Series Firmware Version

Following table provides information on contents of bundled MLXe product SKUs:

SKU	MFG Part Number	Brief Description
BR-MLXE-8-MR2-M-AC	P/N: 80-1007225-01	Brocade MLXe-8 AC system with 1 MR2 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-8-MR2-M-DC	P/N: 80-1007226-01	Brocade MLXe-8 DC system with 1 MR2 management card, 2 high speed switch fabric modules, 2 1800W DC 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 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-16-MR2-M-DC	P/N: 80-1006828-02	Brocade MLXe-16 DC system with 1 MR2 management card, 3 high speed switch fabric modules, 4 1800W DC 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 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-M-DC	P/N: 80-1007254-05	Brocade MLXe-32 DC system with 1 MR2 management card, 7 high speed switch fabric modules, 4 3000W DC power supplies, 10 exhaust fan assembly kits and air filter. Power cord not included.
BR-MLXE-4-MR2-X-AC	P/N: 80-1006874-03	Brocade MLXe-4, AC system with 1 MR2 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-4-MR2-X-DC	P/N: 80-1006875-03	Brocade MLXe-4 DC system with 1 MR2 management card, 2 high speed switch fabric modules, 1 1800W DC power supply, 4 exhaust fan assembly kits and air filter. Power cord not included.

SKU	MFG Part Number	Brief Description
BR-MLXE-32-MR2-X-AC	P/N: 80-1007255-04	Brocade MLXe-32 AC system with 1 XMR MR2 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-DC	P/N: 80-1007256-05	Brocade MLXe-32 DC system with 1 XMR MR2 management card, 7 high speed switch fabric modules, 4 3000W DC power supplies, 10 exhaust fan assembly kits and air filter. Power cord not included.

Table 5 - MLXe Series (bundled SKU) Part Numbers

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.
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 6 - MLXe Management Card Part Numbers

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

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 (with factory installed BR-MLX-1GX20-U10G-MUPG software license)
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 (with factory installed BR-MLX-1GX20-U10G-X2UPG software license).
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 7 - MLXe Interface Line Card Part Numbers

SKU	MFG Part Number	Brief Description
BR-MLX-1GX20-U10G-MUPG	80-1008425-01	Software: An upgrade license for twenty (20) port (M) blades to upgrade ports from 1G to 10G.
BR-MLX-1GX20-U10G-X2UPG	80-1008424-01	Software: An upgrade license for twenty (20) port (X2) blades to upgrade ports from 1G to 10G.

Table 8 - MLXe Interface Line Card Software Upgrade License

NEXT PAGE →

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
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
NI-X-32-HSF	P/N: 80-1008686-01	MLXe high speed switch fabric module for 32-slot chassis

Table 9 - MLXe Switch Fabric Module Part Numbers

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
BR-MLXE-32-ACPWR-3000	P/N: 80-1003969-02	32-slot MLXe AC 3000W power supply
BR-MLXE-DCPWR-1800	P/N:80-1003972-01	16-slot, 8-slot and 4-slot MLXe DC 1800W power supply
BR-MLXE-32-DCPWR-3000	P/N: 80-1003970-03	32-slot MLXe DC 3000W power supply

Table 10 MLXe Power Supply Module Part Numbers

SKU	MFG Part Number	Brief Description
BR-MLXE-4-FAN	P/N:80-1004114-01	MLXe-4 exhaust fan assembly kit
BR-MLXE-8-FAN	P/N:80-1004113-01	MLXe-8 exhaust fan assembly kit
BR-MLXE-16-FAN	P/N:80-1004112-01	MLXe-16 exhaust fan assembly kit
BR-MLXE-32-FAN	P/N: 80-1004469-01	MLXe-32 exhaust fan assembly kit

Table 11- MLXe Fan Module Part Numbers

SKU	MFG Part Number	Brief Description
NI-X-MPNL	P/N:80-1004760-02	NetIron XMR/MLX Series management card blank panel
NI-X-IPNL	P/N: 80-1006511-02	NetIron XMR/MLX Series interface line card blank panel
NI-X-SF3PNL	P/N:80-1004757-02	NetIron XMR/MLX switch fabric module blank panel
NI-X-SF1PNL	P/N:80-1003009-01	NetIron XMR/MLX switch fabric module blank panel for 4-slot chassis
NI-X-PWRPNL	P/N:80-1003052-01	NetIron XMR/MLX power supply blank panel for 8-slot, 16-slot and 32-slot chassis
NI-X-PWRPNL-A	P/N: 80-1003053-01	NetIron XMR/MLX power supply blank panel for 4-slot chassis

Table 12 - MLXe Filler Panel Part Numbers

NEXT PAGE →

Validated MLXe configurations are listed below.

Chassis Model	Module Descriptions	Modules (quantities)
MLXe-4 Configuration	Management card(s):	BR-MLX-MR2-X (2)
	Interface line card(s):	BR-MLX-10GX20-X2 (1), and BR-MLX-1GX20-U10G-X2 (1), and BR-MLX-10GX4-IPSEC-M (1)
	License(s):	BR-MLX-1GX20-U10G-X2UPG (2)
	Switch Fabric module:	NI-X-4-HSF (2)
	Filler Panels:	NI-X-SF1PNL (1), and NI-X-IPNL (1)
	Fan:	BR-MLXE-4-FAN (4)
	Power:	BR-MLXE-ACPWR-1800 (2), and NI-X-PWRPNL-A (2)
MLXe-8 Configuration	Management card(s):	BR-MLX-MR2-M (2)
	Interface line card(s):	BR-MLX-10GX20-M (1), and BR-MLX-10GX4-IPSEC-M (1)
	License(s):	BR-MLX-1GX20-U10G-MUPG (1)
	Switch Fabric module:	NI-X-16-8-HSF (2)
	Filler Panels:	NI-X-SF3PNL (2), and NI-X-IPNL (6)
	Fan:	BR-MLXE-8-FAN (4)
	Power:	BR-MLXE-ACPWR-1800 (2), and NI-X-PWRPNL (2)
MLXe-16 Configuration	Management card(s):	BR-MLX-MR2-M (2)
	Interface line card(s):	BR-MLX-10GX20-M (1), and BR-MLX-10GX4-IPSEC-M (1)
	License(s):	BR-MLX-1GX20-U10G-MUPG (1)
	Switch Fabric module:	NI-X-16-8-HSF (3)
	Filler Panels:	NI-X-SF3PNL (1), and NI-X-IPNL (13)
	Fan:	BR-MLXE-16-FAN (4)
	Power:	BR-MLXE-ACPWR-1800 (4), and NI-X-PWRPNL (4)

Chassis Model	Module Descriptions	Modules (quantities)
MLXe-32 Configuration 1	Management card(s):	BR-MLX-32-MR2-M (2)
	Interface line card(s):	BR-MLX-10GX20-M (1), and BR-MLX-1GX20-U10G-M (1), and BR-MLX-10GX4-IPSEC-M (1)
	License(s):	BR-MLX-1GX20-U10G-MUPG (2)
	Switch Fabric module:	NI-X-32-HSF (8)
	Filler Panels:	NI-X-IPNL (29), NI-X-MPNL (2)
	Fan:	BR-MLXE-32-FAN (10)
	Power:	BR-MLXE-32-ACPWR-3000 (4), and NI-X-PWRPNL (4)
MLXe-32 Configuration 2	Management card(s):	BR-MLX-32-MR2-X (2)
	Interface line card(s):	BR-MLX-10GX20-X2 (1), and BR-MLX-1GX20-U10G-X2 (1), and BR-MLX-10GX4-IPSEC-M (1)
	License(s):	BR-MLX-1GX20-U10G-X2UPG (2)
	Switch Fabric module:	NI-X-32-HSF (8)
	Filler Panels:	NI-X-IPNL (27), NI-X-MPNL (2)
	Fan:	BR-MLXE-32-FAN (10)
	Power:	BR-MLXE-32-ACPWR-3000 (4), and NI-X-PWRPNL (4)

Table 13 - Validated MLXe Configurations

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

Images for MLXe series models are displayed below:

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 13.

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 →

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 13.

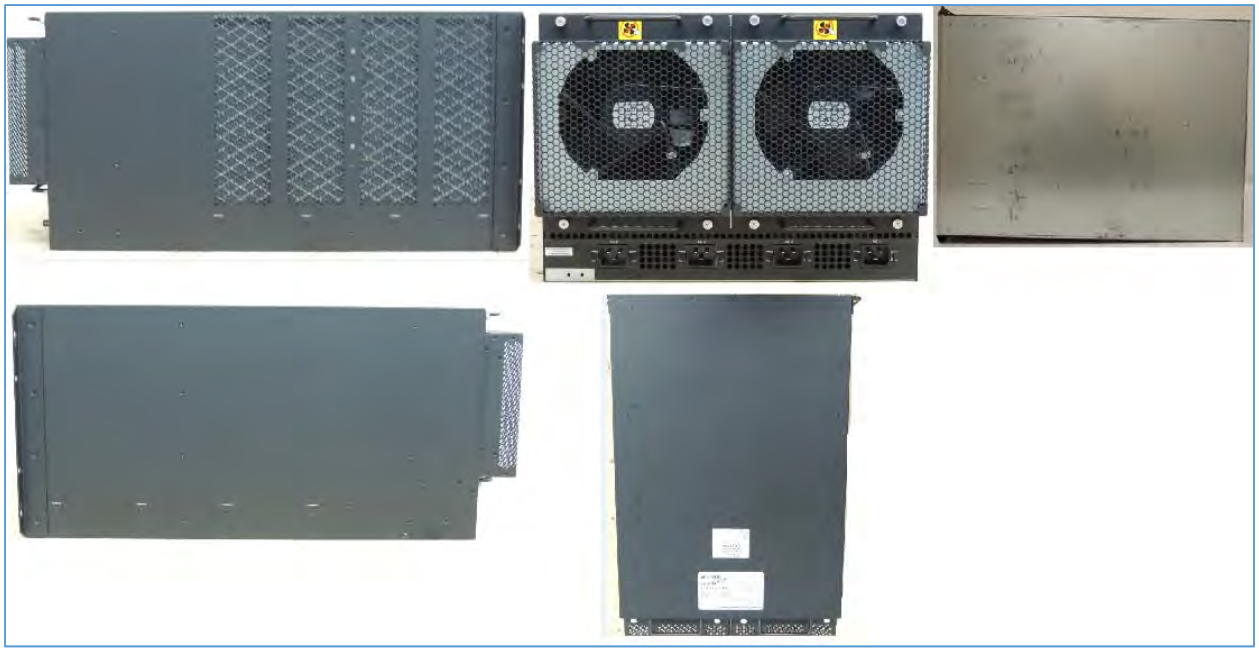

Figure 5 – Brocade MLXe-8: Starting from left to right clockwise: Left side, Rear side, Bottom side, Top side, and Right side

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 13.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

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 →

MLXe-32 images

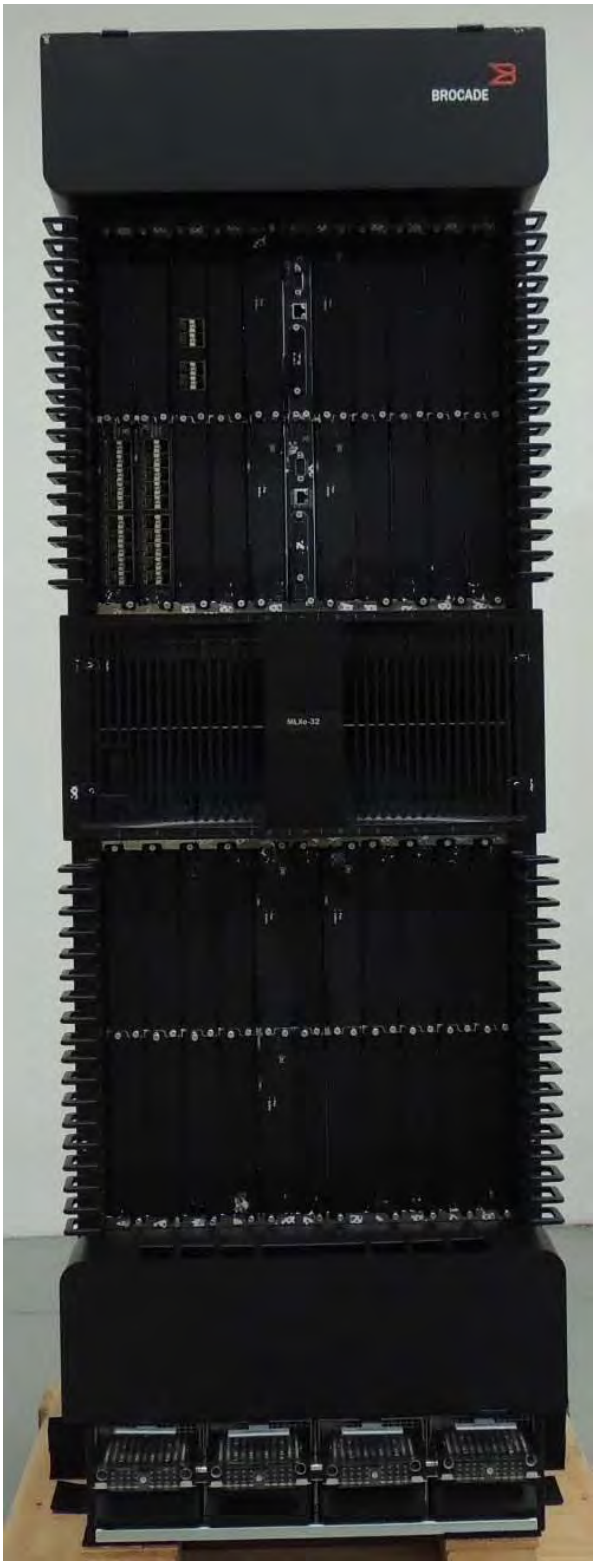

Figure 8 – Brocade MLXe-32 – front view

NEXT PAGE →

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 Ports and Interfaces

Each MLXe series device provides Networking ports, Console, 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 device (MLXe) 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 *(see Note 1, below)*	
Console	**Status output**
LEDs	
Management Port	
Networking ports	
PCMCIA *(see Note 1, below)*	
Power plugs	**Power**

Table 14 - Physical/Logical Interface Correspondence

Note 1: PCMCIA Interface is latent functionality covered via a filler panel and Tamper Evident Label.

4.1 Brocade MLXe series

MLXe series supports varieties of interface line cards. Some of them do not support any cryptographic operations and are not included in the FIPS validation. Interface line cards provide Ethernet ports with multiple connector types and transmission rates. Models in the series (largest in the series being MLXe-32) can provide up to:

- 1536, 1 Gigabit Ethernet Networking ports
- 768, 10 Gigabit Ethernet Networking ports
- 128, 40 Gigabit Ethernet Networking ports
- 64, 100 Gigabit Ethernet Networking ports

NEXT PAGE →

4.1.1 MLXe MR2 Management Modules (Management cards)

MLXe MR2 Management Modules (Management cards) are part of the FIPS Validation as per Section 3 of this document, Table 13. 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

4.1.2 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 13.

The 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

The BR-MLX-1GX20-U10G-M and BR-MLX-1GX20-U10G-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 1GE mode
- LED indicators
- Power and status LEDs

4.1.3 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 13. 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

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

4.1.4 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 6, Table 7 and Table 9).

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 15 - 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

Power and status LEDs for all Management cards are described in table below (for a list of all applicable Management cards see Table 6, - 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 16 - Power and fan status LEDs for the MR2 Management Module

4.2 Modes of Operation

The NetIron validated cryptographic module has two modes of operation:

- FIPS Approved mode and
- Non-Approved mode.

Both these modes enforce digital signature based firmware load test. Section 5.2 Services (Services in Approved mode) and section 6 (Algorithm certificates) describe services and cryptographic algorithms available in FIPS Approved mode.

Section 8.2.1, FIPS Approved Mode, describes how to invoke FIPS Approved mode.

4.3 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 17 - NetIron Security Levels

NEXT PAGE →

5 Roles and Services

5.1 Roles

In FIPS Approved mode, NetIron devices support many different authenticated roles.

5.1.1 The Crypto-officer role

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.

5.1.2 Port Configuration Administrator role

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.

5.1.3 User role

The User role on the device in FIPS Approved mode has read-only privileges and no configuration mode access (user).

5.1.4 IKEv2/IPsec Peer role

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.

5.1.5 MACsec Peer role

A peer device which establishes a MACsec connection with the cryptographic module.

5.1.6 NTP Peer role

This role performs the NTP operation.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

5.2 Services (Services in Approved mode)

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

For all other services, an operator must authenticate to the device, see section 7.2, Authentication.

Service	Additional Information
Console	No additional information is provided here.
HTTPS server	This service provides HTTP server connection over TLS, thus providing HTTPS server service.
IKEv2/IPsec	This service uses the configured keys to establish IKEv2 negotiation and establish an IPsec tunnel. Then this service encrypts and decrypts the data that needs to be transported over the IPsec tunnel that was established by IKEv2/IPsec negotiation service. Supported by MLXe interface line cards: • BR-MLX-10GX4-IPSEC-M
MACsec	This service provides a secure MACsec connection between two peers. 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
NTP	This service provides NTP protocol support to synchronize time over a network
SCP	This service provides secure file transfer over SSHv2 protocol
SNMP	This service provides SNMPv3 protocol in authPriv mode for secure MIB access
SSHv2	This service provides secure connection to the CLI.
Syslog	This service provides Syslog generation capability over UDP transport
TLS client	This service provides a secure outbound TLS client connection to a remote TLS server

Table 18 – List of services in Approved mode of operation

Note that additional algorithm related information and details are available in sections 6.1 and 6.2)

NEXT PAGE →

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

Cryptographic Function	Hardware Platform
AES: Advanced Encryption Standard	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
DRBG: Deterministic Random Bit Generator	All devices
ECDSA: Elliptic Curve Digital Signature Algorithm	All devices
HMAC: Keyed-Hash Message Authentication Code	All devices
KBKDF: SP800-108 Key Based Key Derivation Function (CTR_Mode)	All devices
KTS: SP800-38F Key Transport Scheme	All devices
RSA: Rivest Shamir Adleman	All devices
SHS: Secure Hash Standard	All devices

Table 19 - FIPS Approved Cryptographic Functions

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

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

Algorithm	Caveat	Use
Diffie-Hellman	Provides 112 bits of encryption strength	Key establishment within SSHv2 protocol and TLS v1.0/1.1 and TLSv1.2 protocols
Diffie-Hellman (CVL Cert. #712)	Provides 112 bits of encryption strength	Key establishment within IKEv2 protocol
Elliptic Curve Diffie-Hellman (CVL Cert. #713) Supported curves: P-256, P-384	Provides 128 or 192 bits of encryption strength	Key establishment within IKEv2 protocol
HMAC-MD5	Used in RADIUS for operator authentication only (HMAC-MD5 is not exposed to the operator)	RADIUS Operator Authentication
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)	TLS 1.0/1.1 KDF
MD5	Used in TACACS+ for operator authentication only (MD5 is not exposed to the operator)	TACACS+ Operator Authentication
NDRNG		Seeding for the Approved DRBG. The minimum number of bits of entropy generated by the module for use in key generation is 112-bits.
RSA Key Wrapping	Provides 112 bits of encryption strength	Key establishment within TLS v1.0/1.1 and TLS v1.2

Table 20 - Non-Approved Cryptographic Functions Allowed in FIPS Approved Mode

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

5.2.1 Services accessible by Crypto-officer role

This section only lists supported services accessible by the Crypto-officer role. 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.

5.2.1.1 Console

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.

This service can be used to configure and view following operations:

- PKI offline enrollment function:

  This function provides PKI support for offline loading of certificates and CRLs and offline certificate enrollment. This feature allow the user to generate the Certificate Signing Request and display it on the MLXe CLI.

5.2.1.2 HTTPS server

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

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.

NEXT PAGE →

5.2.1.3 IKEv2/IPsec

The Crypto-officer can configure the IKEv2/IPsec service.

The Crypto-officer role on the IPsec supported interface line card, allows IKEv2 and IPsec sessions to be established with a remote peer based on the IKEv2 and IPsec configuration on the device.

1) IKEv2 profile:
   a) Auth profile
      i) Keypair:
         (1) ECDSA P-256, and P-384

   OR

      ii) Pre-shared keys:
         (1) IKEv2 and IPsec PSK
   b) IKE security parameters
      i) The following cipher sequence is supported for IKEv2:
         (1) aes-256-cbc
         (2) aes-128-cbc
   c) IKE proposal
      i) The following key-exchange (KEX) is supported for IKEv2:
         (1) diffie-hellman-group-14
         (2) EC diffie-hellman-group-19
         (3) EC diffie-hellman-group-20
      ii) The following Message Authentication Code (MAC) is used for integrity check:
         (1) HMAC-SHA-256
         (2) HMAC-SHA-384
      iii) The following PRF is supported for IKEv2:
         (1) SHA-256
         (2) SHA-384
2) IPsec profile:
   a) The following cipher sequence is supported for IPsec:
      i) aes-256-gcm
      ii) aes-128-gcm

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

5.2.1.4 MACsec

The Crypto-officer can configure the MACsec service.

The Crypto-officer role is available on the MACsec supported interface line card and allows MKA and MACsec sessions to be established with a remote peer based on the MACsec configuration on the device.

1. MACsec group
    a. Encryption cipher supported:
        i. aes-128-gcm
    b. Integrity checksum supported:
        i. aes-128-cmac
    c. Key encryption (wrapping) supported:
        i. aes-128-kw
    d. Key derivation function (KDF):
        i. SP800-108-KDF
2. MACsec interface:
    a. Assign to a MACsec group
    b. Pre-shared keys
        i. Connectivity Association key (CAK)
        ii. Connectivity Association Key Name (CKN)

5.2.1.5 NTP

The Crypto-officer role is used to configure the NTP service. The NTP [same as NTPv4] Network Time Protocol configuration and time statistics details can be viewed.

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.

5.2.1.6 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.

NEXT PAGE →

5.2.1.7 SNMP

The SNMP service within Crypto-officer role allows read/write access to the SNMP MIB within the NetIron device as per the capability of the SNMP agent, using SNMPv3 version in authPriv security mode.

SNMPv1 and SNMPv2c are blocked in FIPS mode. Only SNMPv3 in authPriv mode is allowed while other modes are blocked. 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.

5.2.1.8 SSHv2

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

The module supports SSHv2 in both client and server modes. This service provides a secure session between a NetIron device and an SSHv2 client/server. The NetIron device authenticates an SSHv2 client/server 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 (DH Group 14)

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 7.2 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.

NEXT PAGE →

This service can be used to configure and view following operations:

- PKI offline enrollment function:

  This function provides PKI support for offline loading of certificates and CRLs and offline certificate enrollment. This feature allow the user to generate the Certificate Signing Request and display it on the MLXe CLI.

5.2.1.9 Syslog

The Crypto-office can configure the syslog settings.

This service can be used to view the syslog configuration settings.

This service can be used to view the syslog audit records saved on the cryptographic module.

5.2.1.10 TLS client

This service can be used to configure and view statistics for following protocol operations:

- OpenFlow.
  - A peer Openflow controller device which establishes an OpenFlow connection with the cryptographic module. 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. This is the OpenFlow active mode of operation.
- File Copy
  - File copy command uses HTTP protocol over TLS transport to transfer files between the device and a HTTP server.
    NOTE: No device firmware image can be transferred to the device using this service.

The device uses 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

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

5.2.2 Services accessible by Port Configuration Administrator role

This section only lists supported services accessible by Port Configuration Administrator. The Port Configuration Administrator role management privilege level allows read-and-write access for port configuration, but not for global (system-wide) parameters.

5.2.2.1 Console

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.

This service is described in Section 5.2.1.1 above.

5.2.2.2 HTTPS server

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.

This service is described in Section 5.2.1.2 above.

5.2.2.3 IKEv2/IPsec

The Port Configuration Administrator role can read the configuration for this service.

This service is described in section 5.2.1.3 above.

5.2.2.4 MACsec

The Port Configuration Administrator role can read the configuration for this service.

This service is described in section 5.2.1.4 above.

5.2.2.5 NTP

The Port Configuration Administrator role can read the configuration for this service.

This service is described in section 5.2.1.5 above.

5.2.2.6 SNMP

The Port Configuration Administrator role can read the configuration for this service.

This service is described in section 5.2.1.7 above.

5.2.2.7 SSHv2

The Port Configuration Administrator role provides access to all the port configuration commands. That is, all sub-commands within "`interface`" 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.

This service is described in Section 5.2.1.8 above.

5.2.2.8 Syslog

This service can be used to view the syslog configuration settings and the syslog audit records saved on the cryptographic module.

This service is described in section 5.2.1.9 above.

5.2.2.9 TLS client

This service can be used to view the configuration and statistics for following protocol operations:

- OpenFlow.
- File Copy

See, section 5.2.1.10 for more details on supported TLS cipher list.

5.2.3 Services accessible by User role

This section only lists supported services accessible by User role. The User role management privilege level allows access to the User EXEC, and Privileged EXEC commands, but only with read access.

5.2.3.1 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.

5.2.3.2 HTTPS server

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.

This service is described in Section 5.2.1.2 above.

5.2.3.3 IKEv2/IPsec

The User role can read the configuration for this service.

This service is described in section 5.2.1.3 above.

5.2.3.4 MACsec

The User role can read the configuration for this service.

This service is described in section 5.2.1.4 above.

5.2.3.5 NTP

The User role can read the configuration for this service.

This service is described in section 5.2.1.5 above.

5.2.3.6 SNMP

SNMP service within the User role allows read-only access to the SNMP MIB within the NetIron device.

This service is described in detail in section 5.2.1.7 above.

5.2.3.7 SSHv2

The User role can only perform read operation.

This service is described in Section 5.2.1.8 above.

5.2.3.8 Syslog

This service can be used to view the syslog configuration settings.

This service can be used to view the syslog audit records saved on the cryptographic module.

This service is described in section 5.2.1.9 above.

5.2.3.9 TLS client

This service can be used to view the configuration and statistics for following protocol operations:

- OpenFlow.
- File Copy

See, section 5.2.1.10 for more details on supported TLS cipher list.

5.2.4 Services accessible by IKEv2/IPsec Peer role

This section only lists supported services accessible by IKEv2/IPsec Peer role.

5.2.4.1 IKEv2/IPsec

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 IKEv2 and IPsec configuration on the device.

NOTE: Following protocols relies on the security strength provided by this service:

- L2 Over IPsec

This service is described in section 5.2.1.3 above.

5.2.5 Services accessible by MACsec Peer role

This section only lists supported services accessible by MACsec Peer role.

5.2.5.1 MACsec

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.

This service is described in section 5.2.1.4 above.

5.2.6 Services accessible by NTP Peer role

This section only lists supported services accessible by NTP Peer role.

5.2.6.1 NTP

This role utilizes the NTP service which implements the NTP protocol for time synchronization.

This service is described in section 5.2.1.5 above.

5.3 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
BGP	Crypto-officer role	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)
Diagnostics	Crypto-officer role	This service provides diagnostic and status information for various operations within the module. Modes – Not Applicable Key sizes – Not Applicable (plaintext; no cryptography)
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)
MPLS	Crypto-officer role	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
NTP (Authentication using MD5)	Crypto-officer role	Network Time Protocol Modes: MD5 for authentication Key sizes: 20 bytes
OpenFlow over TCP	Crypto-officer role	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. This service over TLS is a service in the Approved mode. See section 5.2.1.10 for more information. This is an implicit service, configured by Crypto-officer role. Modes: Not Applicable Key sizes: Not Applicable (plaintext; no cryptography)

Function/Service	Role(s)	Additional Details
OSPFv2	Crypto-officer role	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)
OSPFv3	Crypto-officer role	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
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
SSHv2	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 Groups: DH Group1 (768-bit), DH Group14 (2048-bit) (non-compliant) Modes: SP800-135 SSHv2 KDF (non-compliant) Hash function: SHA-1

Function/Service	Role(s)	Additional Details
Syslog over TLS	Crypto-officer role	Syslog is a standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. SYSLOG over TLS is only supported in the non-approved mode. This is an implicit service, configured by Crypto-officer role. Modes: RSA (non-compliant) Key sizes: 2048-bit Modes: Diffie-Hellman Group 14 Key sizes: 2048-bit MODP Modes: SP800-135 TLS v1.0 KDF (non-compliant) Key sizes: Not applicable Modes: SP800-135 TLS v1.2 KDF (non-compliant) Key sizes: Not applicable Modes: HMAC-MD5 Key sizes: 160-bit Modes: HMAC-SHA-1 (non-compliant), HMAC-SHA-256 (non-compliant) Key sizes:160-bit, 256-bit Modes: AES-CBC (non-compliant) Key sizes: 128-bit, 256-bit
TACACS	Crypto-officer role	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)
Telnet	Crypto-officer role, Port Configuration Administrator role, User role	Telnet is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP). Modes – Not Applicable Key sizes – Not Applicable (plaintext; no cryptography)
TFTP	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)

Function/Service	Role(s)	Additional Details
"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)
VRRP/VRRP-E Layer 3	Crypto-officer role	Virtual Router Redundancy Protocol (VRRP) and Virtual Router Redundancy Protocol Enhanced (VRRP-E). Execution of this service in Layer 3 mode (plaintext) is only supported in the non-approved mode. This is an implicit service, configured by Crypto-officer role. Modes: Layer 3 mode Key sizes: Not Applicable (plaintext; no cryptography)
VSRP	Crypto-officer role	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)

Table 21 - Functions/Services, Roles in Non-Approved Mode Services

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

5.3.1 Non-Approved Algorithms

The module provides the following non-FIPS approved algorithms in the non-Approved mode of operation. The use of any such service in Table 21 (- Functions/Services, Roles in Non-Approved Mode Services) is an explicit violation of this Security Policy and is explicitly disallowed by this Security Policy:

Algorithm	Use
AES (non-compliant)	Encryption/Decryption
DES	Encryption/Decryption
Diffie-Hellman Group 1	Key Establishment – Non-compliant less than 112 bits of encryption strength
Diffie-Hellman Group 14	Key Establishment
HMAC-MD5	Keyed Hash
HMAC-SHA-1 (non-compliant)	Keyed Hash
HMAC-SHA-256 (non-compliant)	Keyed Hash
HMAC-SHA-1-96 (non-compliant)	Keyed Hash
MD5	Message Digest
RSA	Key Wrapping – non-compliant less than 112 bits of encryption strength
SHA-1 (non-compliant)	Hashing
SNMPv3 KDF (non-compliant)	Key Derivation
SP800-135 SSHv2 KDF (non-compliant)	Key Derivation
SP800-135 TLS v1.0 KDF (non-compliant)	Key Derivation
SP800-135 TLS v1.2 KDF (non-compliant)	Key Derivation
Triple-DES (non-compliant)	Encryption/Decryption

Table 22 - Non-Approved Algorithms

NEXT PAGE →

6 Algorithm certificates

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

6.1 Algorithm certificates in MLXe

CAVP Certificate	Algorithm	Standard	Mode / Method	Key Lengths, Curves or Moduli	Use
2717	AES	FIPS 197, SP 800-38A	ECB, CBC, CTR	128, 192, 256	Data Encryption/Decryption NOTE: AES-ECB is an underlying algorithm; AES-ECB alone is not supported by the cryptographic module in the FIPS Approved Mode.
2946	AES	FIPS 197, SP 800-38B, SP 800-38F	CMAC, KW	128	Generation/Verification Key Wrapping/Unwrapping
3144	AES	FIPS 197, SP 800-38A	CFB128	128	Data Encryption/Decryption
175	CVL TLS 1.0/1.1, SSH	SP 800-135 Revision 1			Key Derivation
393	CVL TLS 1.2	SP 800-135 Revision 1			Key Derivation
404	CVL SNMPv3	SP 800-135 Revision 1			Key Derivation
454	DRBG	SP 800-90A Revision 1	CTR_DRBG (AES-256)		Deterministic Random Bit Generation NOTE: Hash_based DRBG is not supported by the cryptographic module in the FIPS Approved Mode.
761	ECDSA	FIPS 186-4	PKG PKV SigGen SigVer	P-256, P-384	Public Key Generation Public Key Validation Digital Signature Generation and Verification
1696	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256	160, 256	Message Authentication
35	KBKDF	SP 800-108	CTR_Mode		Key Derivation
1413	RSA	FIPS 186-4	SHA-1, SHA-256 PKCS v1.5	1024, 2048	Digital Signature Generation and Verification NOTE: 1024-bit key size is not supported by the cryptographic module in the FIPS Approved Mode.
2282	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest NOTE: SHA-224 and SHA-512 are not supported by the cryptographic module in the FIPS Approved Mode.

Table 23 - Algorithm Certificates for the MLXe MR2 Management Modules (Management cards)

CAVP Certificate	Algorithm	Standard	Mode / Method	Key Lengths, Curves or Moduli	Use
2154	AES	FIPS 197, SP 800-38A SP 800-38D	ECB, GCM	128	Data Encryption/Decryption NOTE: AES-ECB is an underlying algorithm; AES-ECB alone is not supported by the cryptographic module in the FIPS Approved Mode.

Table 24 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

CAVP Certificate	Algorithm	Standard	Mode / Method	Key Lengths, Curves or Moduli	Use
#1648	AES	FIPS 197, SP 800-38A SP 800-38D	ECB, GCM, CBC, CFB128, OFB, CTR	128, 192, 256	Data Encryption/ Decryption NOTE: AES-ECB is an underlying algorithm; AES-ECB alone is not supported by the cryptographic module in the FIPS Approved Mode. NOTE: AES-CFB, AES-OFB and AES-CTR are not supported by BR-MLX-10GX4-IPSEC-M.
#2154	AES	FIPS 197, SP 800-38A SP 800-38D	ECB, GCM	128	Data Encryption/Decryption NOTE: AES-ECB is an underlying algorithm; AES-ECB alone is not supported by the cryptographic module in the FIPS Approved Mode.
#3478	AES	FIPS 197, SP 800-38A SP 800-38D	ECB, GCM	128, 256	Data Encryption/Decryption NOTE: AES-ECB is an underlying algorithm; AES-ECB alone is not supported by the cryptographic module in the FIPS Approved Mode.
#712	CVL All of SP 800-56A Except KDF	SP 800-56Arev2	FFC	(2048, 224), (2048, 256)	Key Agreement
#713	CVL All of SP 800-56A Except KDF (CVL)	SP 800-56Arev2	ECC	P-256, P-384	Key Agreement
#1029	CVL IKEv2	SP 800-135 Revision 1			Key Derivation

CAVP Certificate	Algorithm	Standard	Mode / Method	Key Lengths, Curves or Moduli	Use
#684	DRBG	SP 800-90A Revision 1	Hash_Based (SHA-256)		Deterministic Random Bit Generator
#809	ECDSA	FIPS 186-4	PKG PKV SigGen SigVer	P-256, P-384	Public Key Generation Public Key Validation Digital Signature Generation and Verification
#2848	HMAC	FIPS 198-1	HMAC-SHA-256, HMAC-SHA-384	256, 384	Message Authentication
#934	SHS	FIPS 180-4	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512		Message Digest NOTE: SHA-1, SHA-224 and SHA-512 are not supported by the cryptographic module.

Table 25 - Algorithm Certificates for BR-MLX-10GX4-IPSEC-M interface line cards

NOTES:

1. 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: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/validation
2. Operators should reference the transition tables that are available at the CMVP Web site in special publication SP 800-131A (https://csrc.nist.gov/publications/detail/sp/800-131a/rev-1/final). The data in the tables will inform users of the risks associated with using a particular algorithm and a given key length.
3. 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.

6.2 Non-Approved but allowed cryptographic methods

See Table 20 (- Non-Approved Cryptographic Functions Allowed in FIPS Approved Mode) for additional information on Non-Approved Cryptographic Functions Allowed in FIPS Approved Mode.

7 Policies

7.1 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 used in the IKEv2/IPSec service 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 used in the MACsec service 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 96-bit IV is constructed as per the IEEE 802.1AE Standard.

   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
Three-Key Triple-DES KAT (encrypt) (non-compliant)	✓
Three-Key Triple-DES KAT (decrypt) (non-compliant)	✓
AES-128 (ECB, CBC and CFB128) KAT (encrypt)	✓
AES-128 (ECB, CBC and CFB128) KAT (decrypt)	✓
AES-128 CMAC KAT (generation and verification)	✓
AES-KW KAT (wrap)	✓
AES-KW KAT (unwrap)	✓
ECDSA P-256 and P-384 pairwise consistency test (sign)	✓
ECDSA P-256 and P-384 pairwise consistency test (verify)	✓
SHA-1, 256, 384, 512 KAT (hashing)	✓
HMAC-SHA-1, 256, 384, 512 KAT (keyed hashing)	✓

KAT tests	MLXe product
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	✓
SP800-108 KBKDF KAT	✓
AES-128, 256 GCM KAT (encrypt)	✓
AES-128, 256 GCM KAT (decrypt)	✓
ECDH (P-384) Primitive “Z” Computation KAT	✓

Table 26 - Power-Up Self-Tests - Cryptographic Known Answer Tests (KAT)

ii) Firmware Integrity Test: (CRC 16 and Digital Signature using RSA 2048 SHA-256). The module first performs a CRC-16 test. If the CRC-16 test passes successfully, the module will then proceed with the RSA 2048 SHA-256 signature verification. If the RSA 2048 SHA-256 signature verification test passes successfully, the module has successfully executed its Firmware Integrity Test.

*Note: The module must pass **both** the CRC-16 and RSA 2048 SHA-256 Signature Verification independently to successfully execute the Firmware Integrity Test.*

iii) Critical functions test: RSA 2048 encrypt/decrypt

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 Management Processors (MP) 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>
```

If the error was on the Line Processors (LP), the message logging will display the message shown below.

```
Module (#) is reset by mgmt. (reason: FIPS KAT failure)

System: Module in slot (#) is rebooted due to <Reason String>
```

Where (#) indicates the slot number.

After displaying the failure messages, the module reboots.

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

Conditional Self-Tests	MLXe 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)	✓
ECDSA P-256 and P-384 Pairwise Consistency Test (verify)	✓
Firmware Load Test: RSA 2048 SHA-256 Signature Verification	✓
Bypass Test: Alternating Bypass Test	✓
Manual Key Entry Test	Not Applicable

Table 27 - Conditional Self-Tests

i) Message reporting for failure of Conditional Self-Tests

If the Management Processors (MP) detects an error during the Conditional Self-Test, it displays and logs the message shown below.

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

If the error was on the Line Processors (LP), the message logging will display the message shown below.

```
Module is down. reason <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 5.2 is inhibited during key generation, self-tests, zeroization, and error states.

8) 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

11) All procedural zeroization methods shall be performed by the operator of the module while the operator is in control of the module (i.e. physically present to observe the method has completed successfully.)

7.1.1 Cryptographic Module Operational Rules

In order to operate an MLXe devices 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 devices.

MLXe devices implement FIPS Approved SP800-90A Deterministic Random Bit Generator (DRBG) in Counter (CTR) Mode.

MLXe devices use FIPS Approved key generation methods:

- RSA public and private keys
- ECDSA public and private keys

MLXe devices restrict key entry and key generation to authenticated roles.

7.2 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.

Roles	Authentication
The Crypto-officer role	Line Authentication Method, Enable Authentication Method, Local Authentication Method, RADIUS Authentication Method, TACACS+ Authentication Method
Port Configuration Administrator role	Line Authentication Method, Enable Authentication Method, Local Authentication Method, RADIUS Authentication Method, TACACS+ Authentication Method
User role	Line Authentication Method, Enable Authentication Method, Local Authentication Method, RADIUS Authentication Method, TACACS+ Authentication Method
IKEv2/IPsec Peer role	ECDSA keys or Pre-shared key
MACsec Peer role	Pre-shared key
NTP Peer role	Pre-shared key

Table 28 - Summary of authentication methods available for each role

NEXT PAGE →

7.2.1 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.

7.2.2 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.

7.2.3 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).

7.2.4 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.

7.2.5 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.

7.2.6 Strength of Authentication

This section describes the strength of each authentication method

7.2.6.1 IKEv2/IPsec Peer Role

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.

7.2.6.2 MACsec Peer Role

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.

7.2.6.3 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 and maximum 16 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.

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

7.3 Access Control and Critical Security Parameters (CSPs)

This section details how the CSPs are used by each service for a given role.

This section summarizes the access operators have to the CSPs in each service for a given role. The table entries have the following meanings:

- x – Operator can use the value of the item (for example encrypt with an encryption key),
- r – Operator can read the value of the item (for example view the configuration),
- w – Operator can write a new value for the item, and
- d – Operator can delete the value of the item (zeroize) by executing a `fips zeroize all` command. See item 4a in Section 8.2.1 for further details.
- n/a – Indicates that CSP is not used by the service.

For further details on a given CSP, please reference section 12 (Appendix B: Critical Security Parameters) and search for the CSP number listed in column "CSP #".

7.3.1 Access Control and Critical Security Parameters (CSPs) for the Crypto-officer role

Access control and CSPs for Crypto-officer role is shown in table below:

CSP #	Service / CSP	Console	HTTPS Server	IKEv2/IPsec	MACsec	NTP	SCP	SNMP	SSHv2	Syslog	TLS client
24	SSHv2 Host RSA Private Key (2048 bit)	wd	n/a	n/a	n/a	n/a	x	n/a	xwd	n/a	n/a
22	SSHv2 Client RSA Private Key	wd	n/a	n/a	n/a	n/a	x	n/a	xwd	n/a	n/a
23	SSHv2 DH Group-14 Private Key 2048 bit MODP	d	n/a	n/a	n/a	n/a	xwd	n/a	xwd	n/a	n/a
62	SSHv2 DH Shared Secret Key (2048 bit)	d	n/a	n/a	n/a	n/a	xwd	n/a	xwd	n/a	n/a
51	SSHv2/SCP Session Keys (128, 192 and 256 bit AES CBC and AES CTR)	d	n/a	n/a	n/a	n/a	xwd	n/a	xwd	n/a	n/a
5	SSHv2/SCP Authentication Key (HMAC-SHA-1, 160 bits)	d	n/a	n/a	n/a	n/a	xwd	n/a	xwd	n/a	n/a
11	SSHv2 KDF Internal State	d	n/a	n/a	n/a	n/a	xwd	n/a	xwd	n/a	n/a
25	TLS Host RSA Private Key (RSA 2048 bit)	rwd	x	n/a	n/a	n/a	rw	n/a	rwd	n/a	x
26	TLS Host DH Group-14 Private Key 2048 bit MODP	d	xwd	n/a	n/a	n/a	n/a	n/a	d	n/a	xwd
65	TLS Pre-Master Secret	d	xwd	n/a	n/a	n/a	n/a	n/a	d	n/a	xwd
64	TLS Master Secret	d	xwd	n/a	n/a	n/a	n/a	n/a	d	n/a	xwd
12	TLS KDF Internal State	d	xwd	n/a	n/a	n/a	n/a	n/a	d	n/a	xwd
52	TLS Session Key	d	xwd	n/a	n/a	n/a	n/a	n/a	d	n/a	xwd
6	TLS Authentication Key	d	xwd	n/a	n/a	n/a	n/a	n/a	d	n/a	xwd
21	MP DRBG Key	xd	x	x	x	n/a	x	n/a	xd	n/a	x
18	MP DRBG Internal State	xd	x	x	x	n/a	x	n/a	xd	n/a	x

CSP #	Service / CSP	Console	HTTPS Server	IKEv2/IPsec	MACsec	NTP	SCP	SNMP	SSHv2	Syslog	TLS client
19	MP DRBG Seed	xd	x	x	x	n/a	x	n/a	xd	n/a	x
20	MP DRBG Value V	xd	x	x	x	n/a	x	n/a	xd	n/a	x
61	NTP secret	rwd	n/a	n/a	n/a	x	rwd	n/a	rwd	n/a	n/a
14	LP DRBG Internal State	d	n/a	x	n/a	n/a	n/a	n/a	d	n/a	n/a
15	LP DRBG Seed	d	n/a	x	n/a	n/a	n/a	n/a	d	n/a	n/a
16	LP DRBG Value C	d	n/a	x	n/a	n/a	n/a	n/a	d	n/a	n/a
17	LP DRBG Value V	d	n/a	x	n/a	n/a	n/a	n/a	d	n/a	n/a
4	Local - User Password	rwd	rwd	n/a	n/a	n/a	rw	n/a	rwd	n/a	n/a
3	Local - Port Administrator Password	rwd	rwd	n/a	n/a	n/a	rw	n/a	rwd	n/a	n/a
2	Local - Crypto-officer Password	xrwd	xrwd	n/a	n/a	n/a	xrw	x	xrwd	n/a	n/a
59	RADIUS Secret	xrwd	xrwd	n/a	n/a	n/a	xrw	n/a	xrwd	n/a	n/a
63	TACACS+ Secret	xrwd	xrwd	n/a	n/a	n/a	xrw	n/a	xrwd	n/a	n/a
60	SNMPv3 secret	rwd	n/a	n/a	n/a	n/a	rw	x	rwd	n/a	n/a
13	SNMPv3 KDF State	n/a	n/a	n/a	n/a	n/a	n/a	xwd	n/a	n/a	n/a
47	Firmware Load RSA Public Key	x	n/a	n/a	n/a	n/a	x	n/a	x	n/a	n/a
36	SSHv2 Host RSA Public Key (2048 bit)	rwd	n/a	n/a	n/a	n/a	xrw	n/a	xrwd	n/a	n/a
33	SSHv2 Client RSA Public Key	rwd	n/a	n/a	n/a	n/a	xrw	n/a	xrwd	n/a	n/a
35	SSHv2 DH Group-14 Public Key 2048 bit MODP	d	n/a	n/a	n/a	n/a	xwd	n/a	xwd	n/a	n/a
34	SSHv2 DH Group-14 Peer Public Key 2048 bit MODP	d	n/a	n/a	n/a	n/a	xwd	n/a	Xwd	n/a	n/a
37	TLS Host RSA Public Key (RSA 2048 bit)	rwd	x	n/a	n/a	n/a	rw	n/a	rwd	n/a	x
38	TLS Peer Public Key (RSA 2048 bit)	d	xd	n/a	n/a	n/a	n/a	n/a	d	n/a	xd
39	TLS Host DH Group-14 Public Key 2048 bit MODP	d	xwd	n/a	n/a	n/a	n/a	n/a	n/a	n/a	xwd
40	TLS Peer DH Group-14 Public Key 2048 bit MODP	d	xd	n/a	n/a	n/a	n/a	n/a	n/a	n/a	xd
44	IKEv2 ECDSA Public Key (P-256)	rwd	n/a	x	n/a	n/a	rw	n/a	rwd	n/a	n/a
45	IKEv2 ECDSA Public Key (P-384)	rwd	n/a	x	n/a	n/a	rw	n/a	rwd	n/a	n/a
57	MKA Connectivity Association Key (CAK)	rwd	n/a	n/a	x	n/a	rw	n/a	rwd	n/a	n/a
58	MKA Connectivity Key Name (CKN)	rwd	n/a	n/a	x	n/a	rw	n/a	rwd	n/a	n/a
10	MKA SP800-108 KDF State	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
30	IKEv2 ECDSA Private Key (P-256)	rwd	n/a	n/a	n/a	n/a	rw	n/a	rwd	n/a	n/a
31	IKEv2 ECDSA Private Key (P-384)	rwd	n/a	n/a	n/a	n/a	rw	n/a	rwd	n/a	n/a
56	IKEv2 Pre-Shared Key (PSK)	rwd	n/a	n/a	n/a	n/a	rw	n/a	rwd	n/a	n/a

Table 29 - Access Control and CSPs for the Crypto-officer role

NEXT PAGE →

7.3.2 Access Control and Critical Security Parameters (CSPs) for Port Configuration Administrator role

Access control and CSPs for Port Configuration Administrator role is shown in table below:

CSP #	Service / CSP	Console	HTTPS Server	IKEv2/IPsec	MACsec	NTP	SNMP	SSHv2	Syslog	TLS client
24	SSHv2 Host RSA Private Key (2048 bit)	n/a	n/a	n/a	n/a	n/a	n/a	x	n/a	n/a
22	SSHv2 Client RSA Private Key	n/a	n/a	n/a	n/a	n/a	n/a	x	n/a	n/a
23	SSHv2 DH Group-14 Private Key 2048 bit MODP	n/a	n/a	n/a	n/a	n/a	n/a	xwd	n/a	n/a
62	SSHv2 DH Shared Secret Key (2048 bit)	n/a	n/a	n/a	n/a	n/a	n/a	xwd	n/a	n/a
51	SSHv2/SCP Session Keys (128, 192 and 256 bit AES CBC and AES CTR)	n/a	n/a	n/a	n/a	n/a	n/a	xwd	n/a	n/a
5	SSHv2/SCP Authentication Key (HMAC-SHA-1, 160 bits)	n/a	n/a	n/a	n/a	n/a	n/a	xwd	n/a	n/a
11	SSHv2 KDF Internal State	n/a	n/a	n/a	n/a	n/a	n/a	xwd	n/a	n/a
25	TLS Host RSA Private Key (RSA 2048 bit)	n/a	x	n/a	n/a	n/a	n/a	n/a	n/a	x
26	TLS Host DH Group-14 Private Key 2048 bit MODP	n/a	xwd	n/a	n/a	n/a	n/a	n/a	n/a	xwd
65	TLS Pre-Master Secret	n/a	xwd	n/a	n/a	n/a	n/a	n/a	n/a	xwd
64	TLS Master Secret	n/a	xwd	n/a	n/a	n/a	n/a	n/a	n/a	xwd
12	TLS KDF Internal State	n/a	xwd	n/a	n/a	n/a	n/a	n/a	n/a	xwd
52	TLS Session Key	n/a	xwd	n/a	n/a	n/a	n/a	n/a	n/a	xwd
6	TLS Authentication Key	n/a	xwd	n/a	n/a	n/a	n/a	n/a	n/a	xwd
21	MP DRBG Key	n/a	x	n/a	n/a	n/a	n/a	x	n/a	n/a
18	MP DRBG Internal State	n/a	x	n/a	n/a	n/a	n/a	x	n/a	n/a
19	MP DRBG Seed	n/a	x	n/a	n/a	n/a	n/a	x	n/a	n/a
20	MP DRBG Value V	n/a	x	n/a	n/a	n/a	n/a	x	n/a	n/a
61	NTP secret	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
14	LP DRBG Internal State	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
15	LP DRBG Seed	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
16	LP DRBG Value C	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
17	LP DRBG Value V	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
4	Local - User Password	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
3	Local - Port Administrator Password	x	x	n/a	n/a	n/a	n/a	x	n/a	n/a
2	Local - Crypto-officer Password	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
59	RADIUS Secret	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
63	TACACS+ Secret	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
60	SNMPv3 secret	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
13	SNMPv3 KDF State	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
47	Firmware Load RSA Public Key	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
36	SSHv2 Host RSA Public Key (2048 bit)	r	n/a	n/a	n/a	n/a	n/a	xr	n/a	n/a

CSP #	Service / CSP	Console	HTTPS Server	IKEv2/IPsec	MACsec	NTP	SNMP	SSHv2	Syslog	TLS client
33	SSHv2 Client RSA Public Key	r	n/a	n/a	n/a	n/a	n/a	xr	n/a	n/a
35	SSHv2 DH Group-14 Public Key 2048 bit MODP	n/a	n/a	n/a	n/a	n/a	n/a	xwd	n/a	n/a
34	SSHv2 DH Group-14 Peer Public Key 2048 bit MODP	n/a	n/a	n/a	n/a	n/a	n/a	xd	n/a	n/a
37	TLS Host RSA Public Key (RSA 2048 bit)	n/a	x	n/a	n/a	n/a	n/a	n/a	n/a	x
38	TLS Peer Public Key (RSA 2048 bit)	n/a	x	n/a	n/a	n/a	n/a	n/a	n/a	x
39	TLS Host DH Group-14 Public Key 2048 bit MODP	n/a	xwd	n/a	n/a	n/a	n/a	n/a	n/a	xwd
40	TLS Peer DH Group-14 Public Key 2048 bit MODP	n/a	xd	n/a	n/a	n/a	n/a	n/a	n/a	xd
44	IKEv2 ECDSA Public Key (P-256)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
45	IKEv2 ECDSA Public Key (P-384)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
57	MKA Connectivity Association Key (CAK)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
58	MKA Connectivity Key Name (CKN)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
10	MKA SP800-108 KDF State	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
30	IKEv2 ECDSA Private Key (P-256)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
31	IKEv2 ECDSA Private Key (P-384)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
56	IKEv2 Pre-Shared Key (PSK)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Table 30 - Access Control and CSPs for the Port Configuration role

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

7.3.3 Access Control and Critical Security Parameters (CSPs) for User role

Access control and CSPs for User role is shown in table below:

CSP #	Service / CSP	Console	HTTPS Server	IKEv2/IPsec	MACsec	NTP	SNMP	SSHv2	Syslog	TLS client
24	SSHv2 Host RSA Private Key (2048 bit)	n/a	n/a	n/a	n/a	n/a	n/a	x	n/a	n/a
22	SSHv2 Client RSA Private Key	n/a	n/a	n/a	n/a	n/a	n/a	x	n/a	n/a
23	SSHv2 DH Group-14 Private Key 2048 bit MODP	n/a	n/a	n/a	n/a	n/a	n/a	xwd	n/a	n/a
62	SSHv2 DH Shared Secret Key (2048 bit)	n/a	n/a	n/a	n/a	n/a	n/a	xwd	n/a	n/a
51	SSHv2/SCP Session Keys (128, 192 and 256 bit AES CBC and AES CTR)	n/a	n/a	n/a	n/a	n/a	n/a	xwd	n/a	n/a
5	SSHv2/SCP Authentication Key (HMAC-SHA-1, 160 bits)	n/a	n/a	n/a	n/a	n/a	n/a	xwd	n/a	n/a
11	SSHv2 KDF Internal State	n/a	n/a	n/a	n/a	n/a	n/a	xwd	n/a	n/a
25	TLS Host RSA Private Key (RSA 2048 bit)	n/a	x	n/a	n/a	n/a	n/a	n/a	n/a	x
26	TLS Host DH Group-14 Private Key 2048 bit MODP	n/a	xwd	n/a	n/a	n/a	n/a	n/a	n/a	xwd
65	TLS Pre-Master Secret	n/a	xwd	n/a	n/a	n/a	n/a	n/a	n/a	xwd
64	TLS Master Secret	n/a	xwd	n/a	n/a	n/a	n/a	n/a	n/a	xwd
12	TLS KDF Internal State	n/a	xwd	n/a	n/a	n/a	n/a	n/a	n/a	xwd
52	TLS Session Key	n/a	xwd	n/a	n/a	n/a	n/a	n/a	n/a	xwd
6	TLS Authentication Key	n/a	xwd	n/a	n/a	n/a	n/a	n/a	n/a	xwd
21	MP DRBG Key	n/a	x	n/a	n/a	n/a	n/a	x	n/a	n/a
18	MP DRBG Internal State	n/a	x	n/a	n/a	n/a	n/a	x	n/a	n/a
19	MP DRBG Seed	n/a	x	n/a	n/a	n/a	n/a	x	n/a	n/a
20	MP DRBG Value V	n/a	x	n/a	n/a	n/a	n/a	x	n/a	n/a
61	NTP secret	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
14	LP DRBG Internal State	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
15	LP DRBG Seed	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
16	LP DRBG Value C	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
17	LP DRBG Value V	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
4	Local - User Password	x	x	n/a	n/a	n/a	x	x	n/a	n/a
3	Local - Port Administrator Password	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
2	Local - Crypto-officer Password	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
59	RADIUS Secret	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
63	TACACS+ Secret	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
60	SNMPv3 secret	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
13	SNMPv3 KDF State	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
47	Firmware Load RSA Public Key	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
36	SSHv2 Host RSA Public Key (2048 bit)	r	n/a	n/a	n/a	n/a	n/a	xr	n/a	n/a

CSP #	Service / CSP	Console	HTTPS Server	IKEv2/IPsec	MACsec	NTP	SNMP	SSHv2	Syslog	TLS client
33	SSHv2 Client RSA Public Key	r	n/a	n/a	n/a	n/a	n/a	xr	n/a	n/a
35	SSHv2 DH Group-14 Public Key 2048 bit MODP	n/a	n/a	n/a	n/a	n/a	n/a	xwd	n/a	n/a
34	SSHv2 DH Group-14 Peer Public Key 2048 bit MODP	n/a	n/a	n/a	n/a	n/a	n/a	xd	n/a	n/a
37	TLS Host RSA Public Key (RSA 2048 bit)	n/a	x	n/a	n/a	n/a	n/a	n/a	n/a	x
38	TLS Peer Public Key (RSA 2048 bit)	n/a	x	n/a	n/a	n/a	n/a	n/a	n/a	x
39	TLS Host DH Group-14 Public Key 2048 bit MODP	n/a	xwd	n/a	n/a	n/a	n/a	n/a	n/a	xwd
40	TLS Peer DH Group-14 Public Key 2048 bit MODP	n/a	xd	n/a	n/a	n/a	n/a	n/a	n/a	xd
44	IKEv2 ECDSA Public Key (P-256)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
45	IKEv2 ECDSA Public Key (P-384)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
57	MKA Connectivity Association Key (CAK)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
58	MKA Connectivity Key Name (CKN)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
10	MKA SP800-108 KDF State	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
30	IKEv2 ECDSA Private Key (P-256)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
31	IKEv2 ECDSA Private Key (P-384)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
56	IKEv2 Pre-Shared Key (PSK)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Table 31 - Access Control and CSPs for the User role

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

7.3.4 Access Control and Critical Security Parameters (CSPs) for IKEv2/IPsec Peer role

Access control and CSPs for IKEv2/IPsec Peer role is shown in table below:

CSP #	Service / CSP	IKEv2/IPsec
27	IKEv2 DH Group-14 Private Key 2048 bit MODP	xwd
41	IKEv2 DH Group-14 Public Key 2048 bit MODP	xwd
53	IKEv2 DH Group-14 Shared Secret 2048 bit MODP	xwd
30	IKEv2 ECDSA Private Key (P-256)	xd
31	IKEv2 ECDSA Private Key (P-384)	xd
44	IKEv2 ECDSA Public Key (P-256)	xd
45	IKEv2 ECDSA Public Key (P-384)	xd
28	IKEv2 ECDH Group-19 Private Key (P-256)	xwd
29	IKEv2 ECDH Group-20 Private Key (P-384)	xwd
42	IKEv2 ECDH Group-19 Public Key (P-256)	xwd
43	IKEv2 ECDH Group-20 Public Key (P-384)	xwd
54	IKEv2 ECDH Group-19 Shared Secret (P-256)	xwd
55	IKEv2 ECDH Group-20 Shared Secret (P-384)	xwd
48	IKEv2 Encrypt/Decrypt Key	xwd
1	IKEv2/IPsec Authentication Key	xwd
49	IPsec ESP Encrypt/Decrypt Key	xwd
7	IKEv2 KDF State	xwd
56	IKEv2 Pre-Shared Key (PSK)	xd
15	LP DRBG Seed	xd
16	LP DRBG Value C	xd
17	LP DRBG Value V	xd
14	LP DRBG Internal State	xd
32	PKI SCEP Enrollment RSA 2048-bit Private Key	xwd
46	PKI SCEP Enrollment RSA 2048-bit Public Key	xwd

Table 32 - Access Control and CSPs for the IKEv2/IPsec Peer role

NEXT PAGE →

7.3.5 Access Control and Critical Security Parameters (CSPs) for MACsec role

Access control and CSPs for MACsec Peer role is shown in table below:

CSP #	Service / CSP	MACsec
8	MKA Integrity Checksum Key (ICK)	xwd
9	MKA Key Encryption Key (KEK)	xwd
50	MKA Secure Association Key (SAK)	xwd
10	MKA SP800-108 KDF State	xwd
57	MKA Connectivity Association Key (CAK)	x
58	MKA Connectivity Key Name (CKN)	X

Table 33 - Access Control and CSPs for the MACsec role

7.3.6 Access Control and Critical Security Parameters (CSPs) for NTP Peer role

Access control and CSPs for NTP Peer role is shown in table below:

CSP #	Service / CSP	NTP
61	NTP secret	x

Table 34 - Access Control and CSPs for the NTP Peer role

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

7.3.7 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.

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.

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) NetIron devices.

All other CSPs can be zeroized by executing the "`fips zeroize all`" command. This command can be executed via the Console and SSHv2 service.

7.4 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, 11 - 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 35 - Inspection of Physical Security Mechanisms

8 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, 11 - 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.

8.1 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 8.2 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 36 - Sample output - MLXe 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 37 - Sample output - MLXe in FIPS Approved mode

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

8.2 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. 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`"
9. VLL with RSVP continues to be unsupported for L2 Over IPsec feature

Entering FIPS Approved mode also clears:

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

FIPS Approved mode enables:

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

8.2.1 Invoking FIPS Approved Mode

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

1) Assume Crypto-officer role

   a) Initially, in the default configuration, there is no authentication data (default password) set for the Crypto-officer. The Crypto-officer role is assumed by the human operator, physically present and in control of the module, who is authorized to perform the steps outlined in this section via the console terminal.

      As part of configuration to invoke the FIPS approved mode, the Crypto-officer shall chose an authentication method and enter the "Local - Crypto-officer Password (MLXe-MP-MGMT card)".

      Note: The authentication methods available for assuming the Crypto-officer role through the console terminal port are defined in Section 7.2. 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) All procedural zeroization methods shall be performed by the operator of the module while the operator is in control of the module (i.e. physically present to observe the method has completed successfully.)

5) 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.

6) Once the module completes zeroization, configure all users of the module and authentication methods as per Section 7.2.

7) Enter command: "`enable strict-password-enforcement`"

8) Enter command: `write memory`

a) The device saves the running configuration as the startup configuration

9) Enter command: reload

a) The device reboots, does a Power-On Self-Test and if successful, begins operation in FIPS Approved mode.

10) Enter command: `fips show`

a) The device displays the FIPS-related status, which should confirm the security policy is the default security policy.

11) Inspect the physical security of the module, including placement of tamper evident labels according to section, 11 - Appendix A: Tamper Evident Seal Application Procedure.

8.2.2 Negating FIPS Approved Mode

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 7.2.

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.

9 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 38 - Mitigation of other attacks

10 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 39 - Glossary

NEXT PAGE →

11 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.

11.1 Brocade MLXe devices

11.1.1 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 10 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 11 for correct seal orientation and positioning.

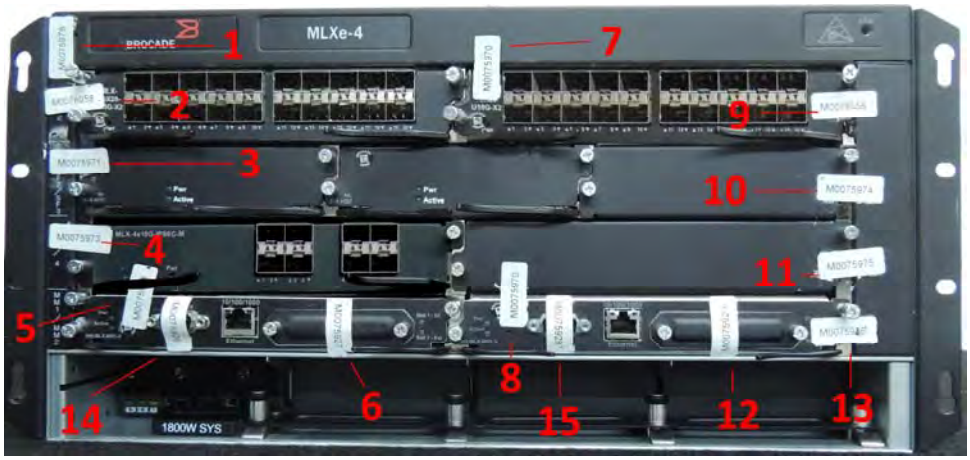

Figure 10 - Front view of Brocade MLXe-4 with security seals

NEXT PAGE →

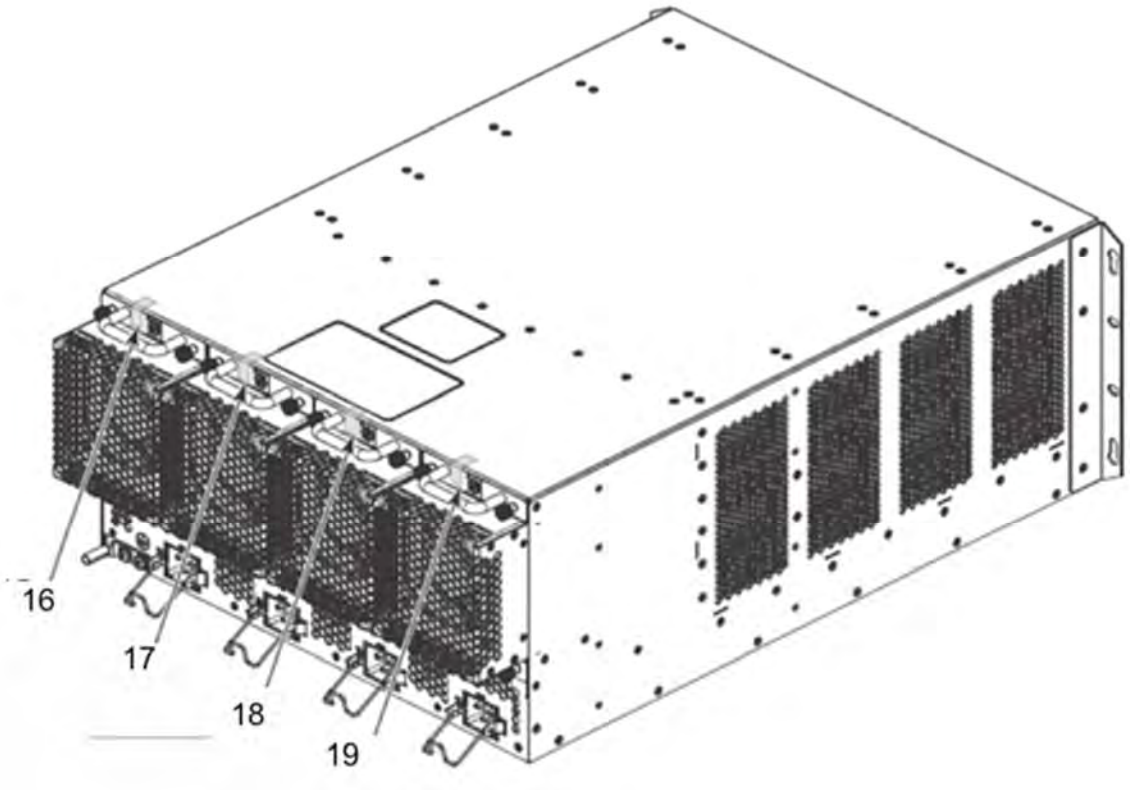

Figure 11 - Rear view of Brocade MLXe-4 device with security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

11.1.2 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 12 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 13 for correct seal orientation and positioning.

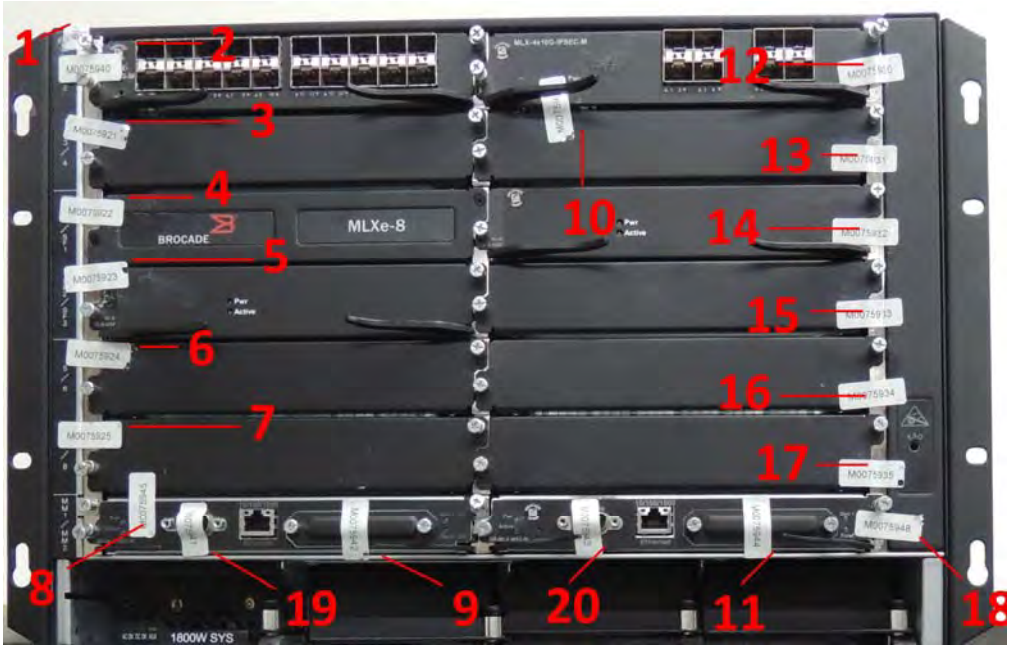

Figure 12 - Front view of Brocade MLXe-8 device with security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

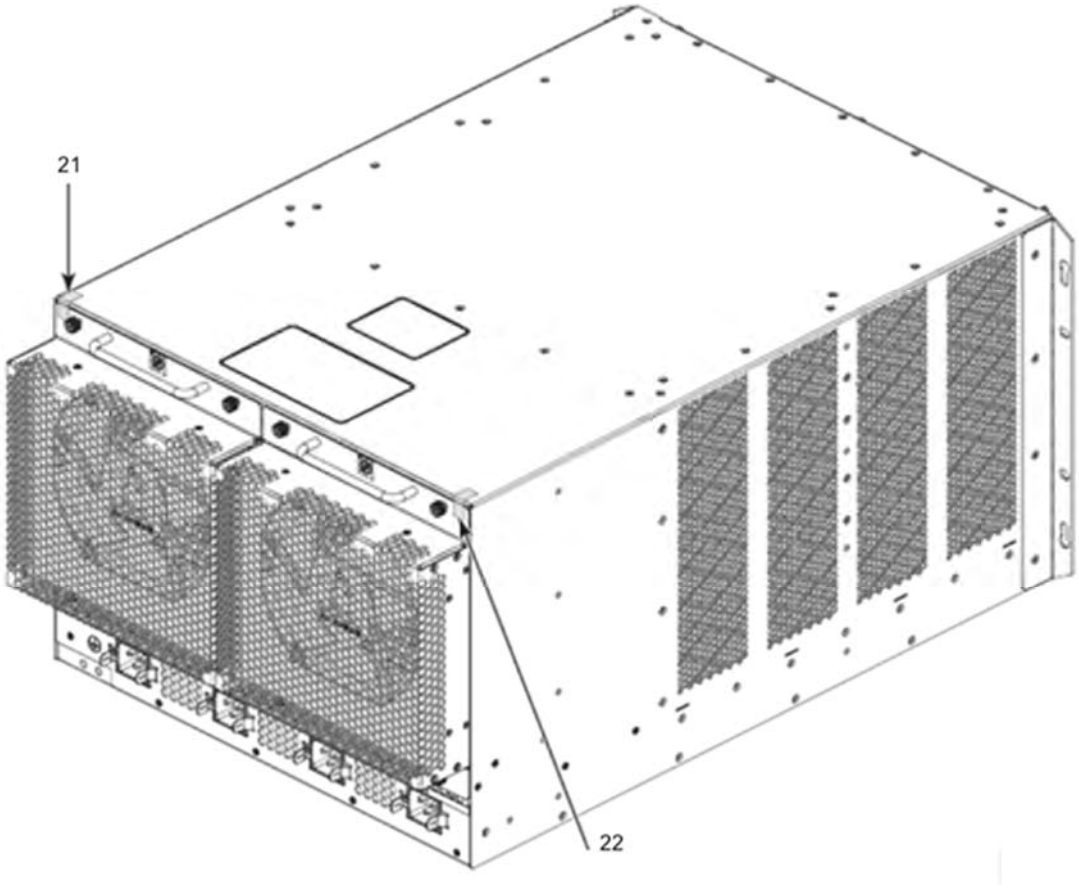

Figure 13 - Rear view of Brocade MLXe-8 device with security seals

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

11.1.3 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 14 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 15 for correct seal orientation and positioning.

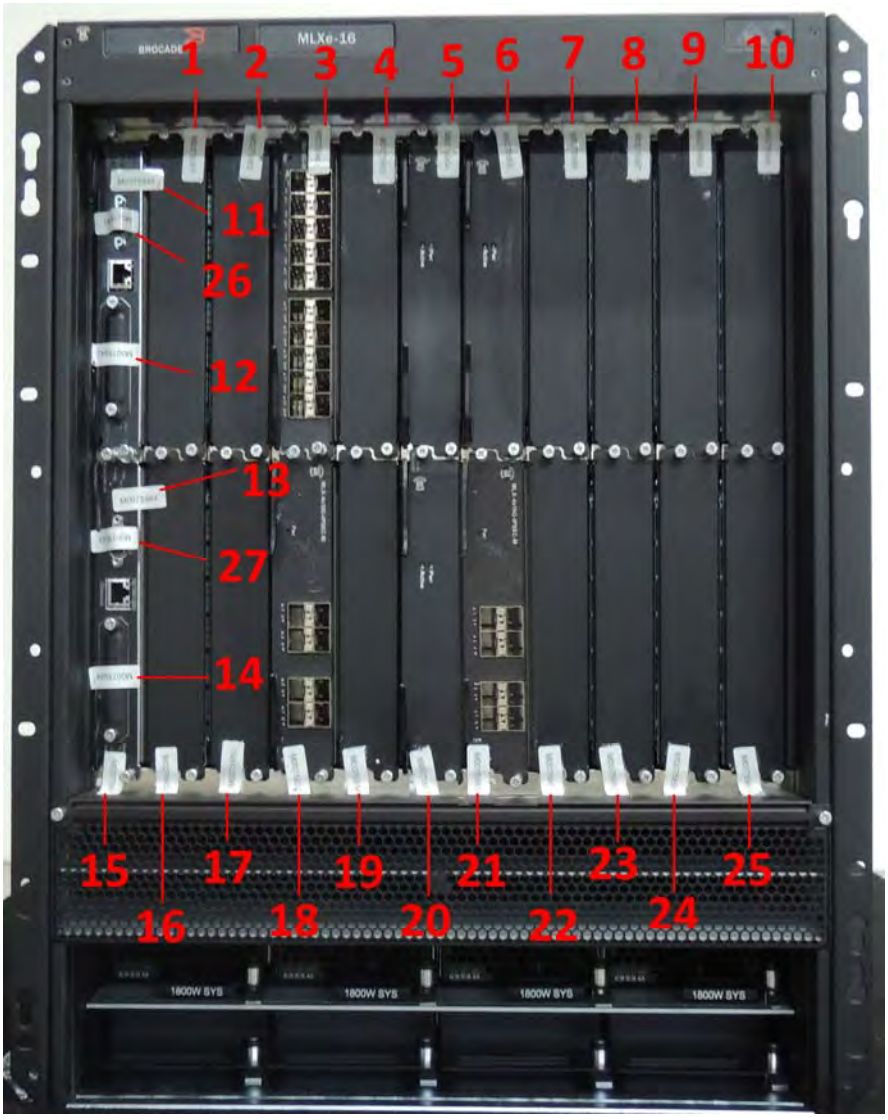

Figure 14 - Front view of Brocade MLXe-16 device with security seals

NEXT PAGE →

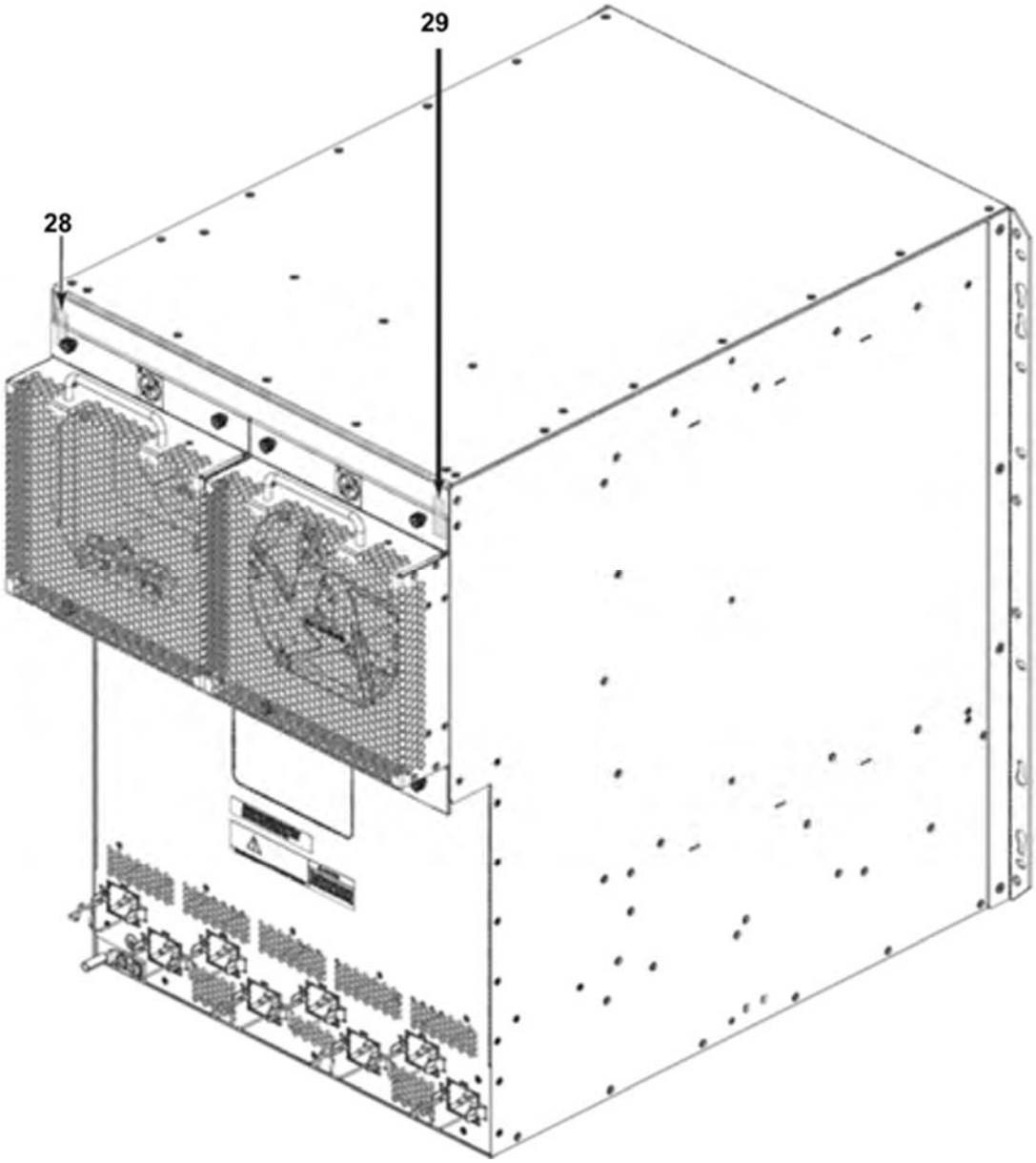

Figure 15 - Rear view of Brocade MLXe-16 device with security seals

NEXT PAGE →

11.1.4 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 →

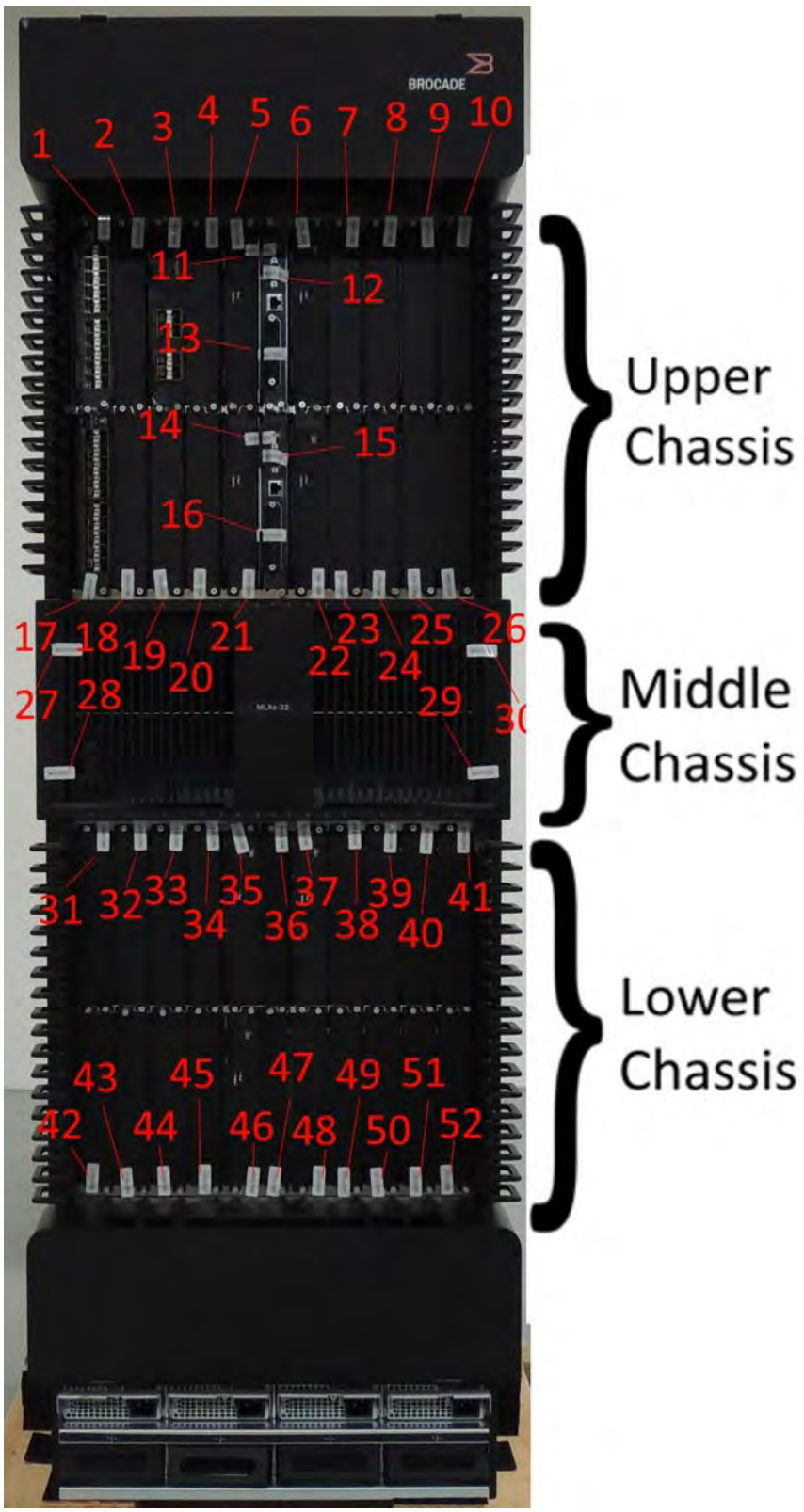

Figure 16 - Front overview of MLXe-32 Configuration 1 with tamper labels

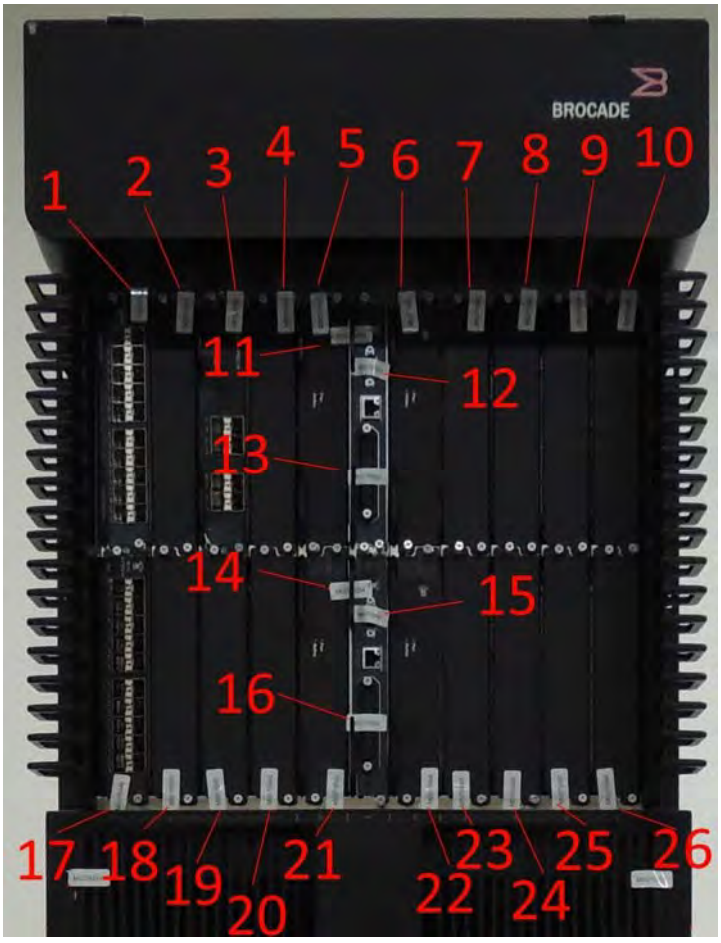

Figure 17 - Front upper chassis of MLXe-32 Configuration 1 with tamper labels

Figure 18 - Front middle chassis (grill) of MLXe-32 Configuration 1 with tamper labels

NEXT PAGE →

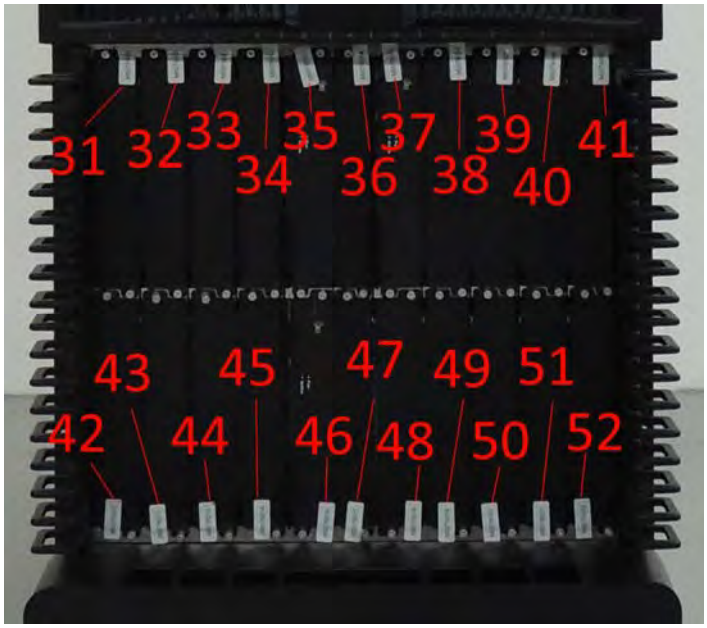

Figure 19 - Front lower chassis of MLXe-32 Configuration 1 with tamper labels

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

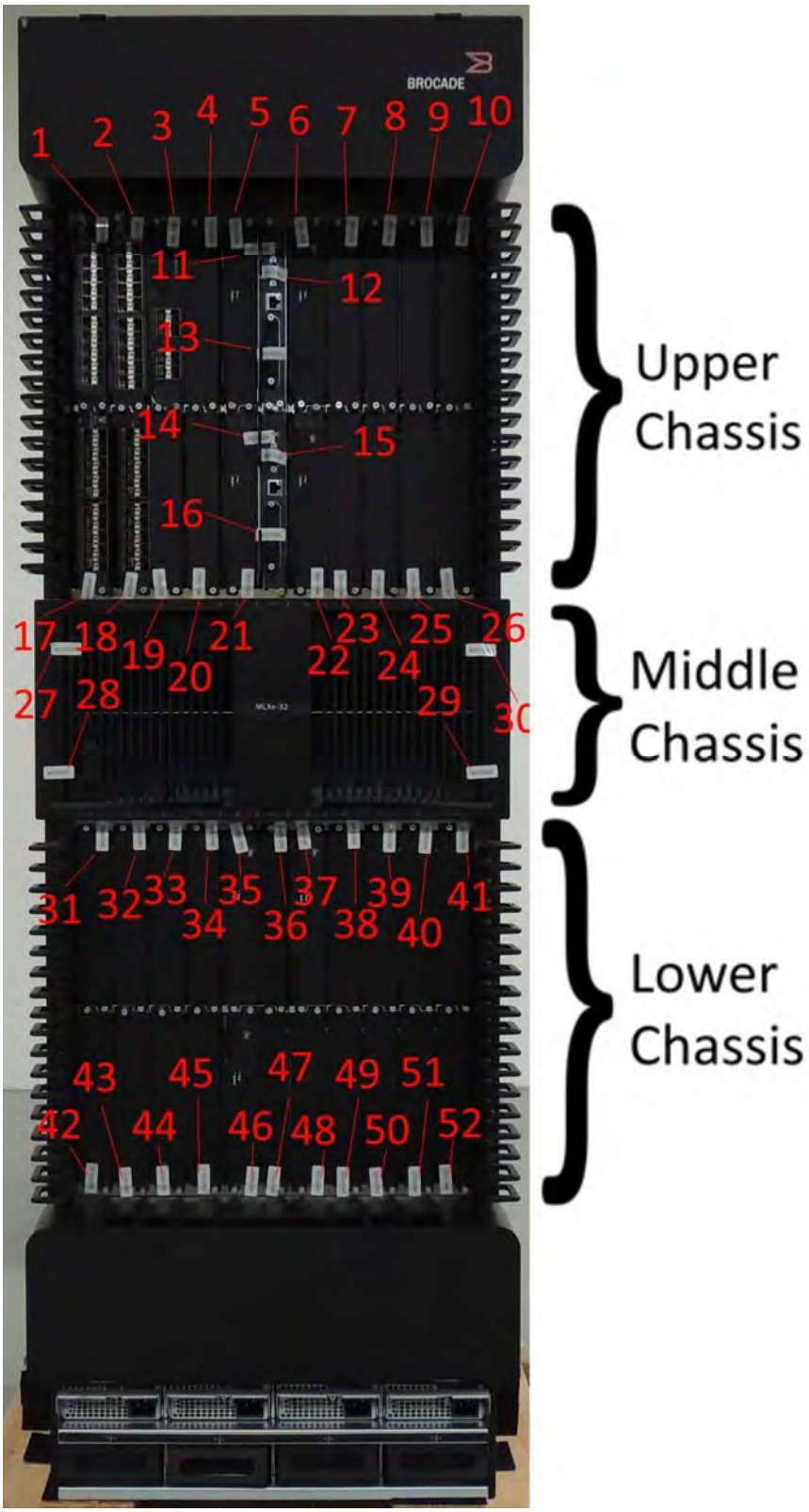

Figure 20 - Front overview of MLXe-32 Configuration 2 with tamper labels

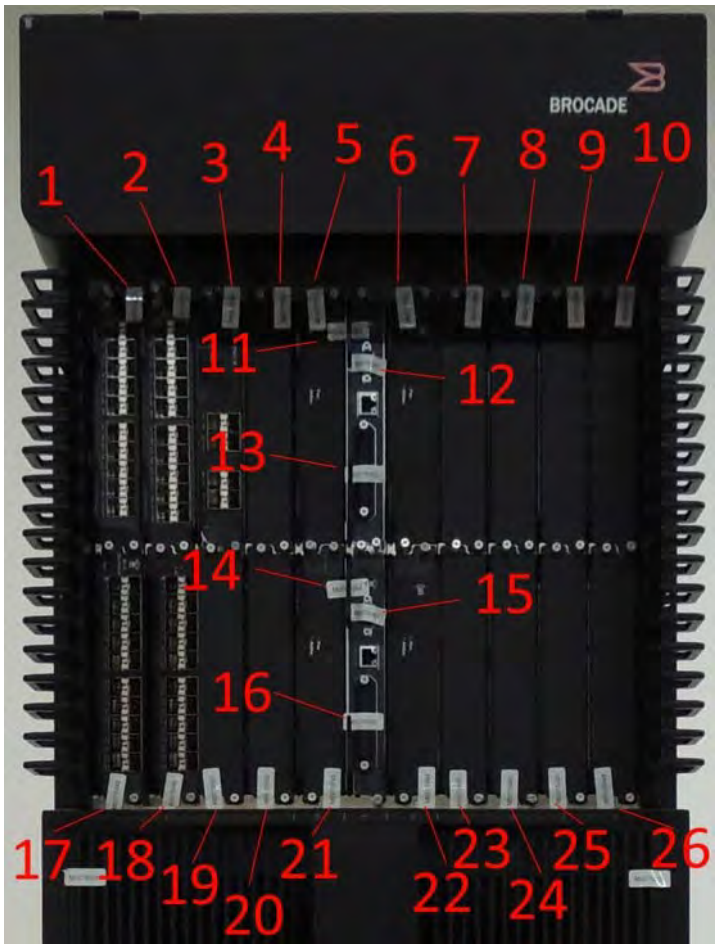

Figure 21 - Front overview of MLXe-32 Configuration 2 with tamper labels

Figure 22 - Front middle chassis (grill) of MLXe-32 Configuration 2 with tamper labels

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

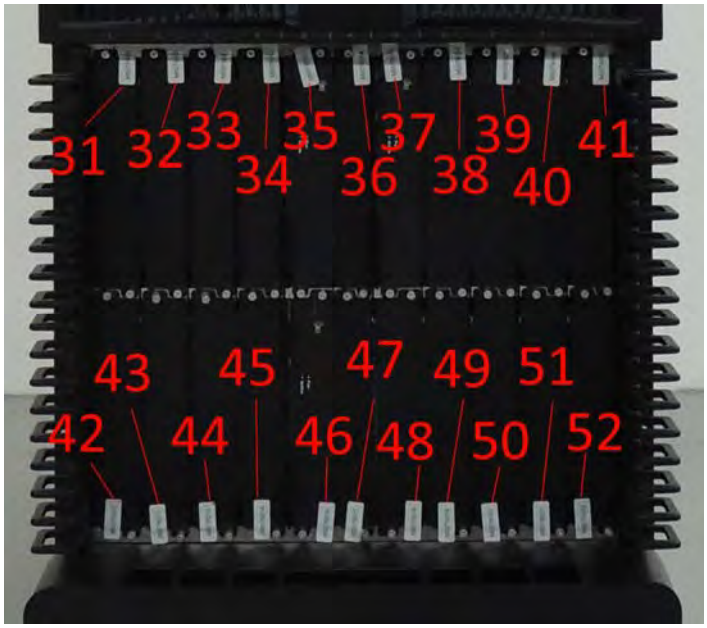

Figure 23 - Front lower chassis of MLXe-32 Configuration 2 with tamper labels

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

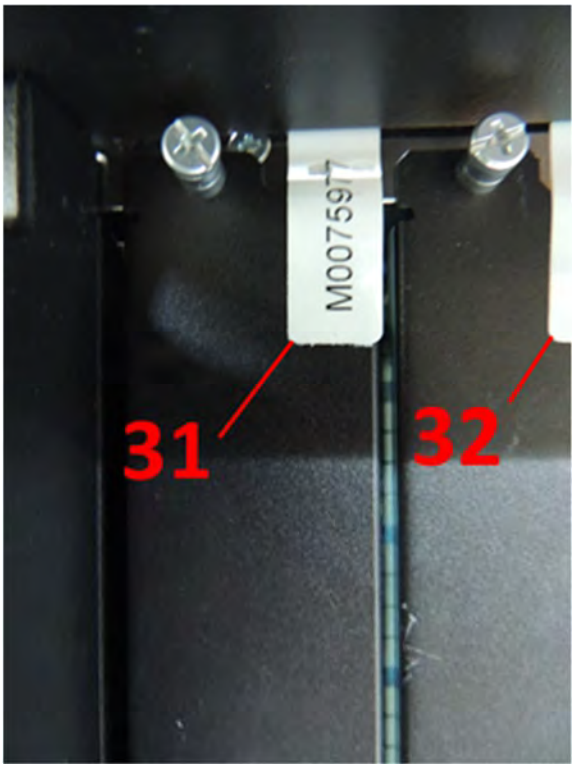

Figure 24 - Label 31 example of MLXe-32

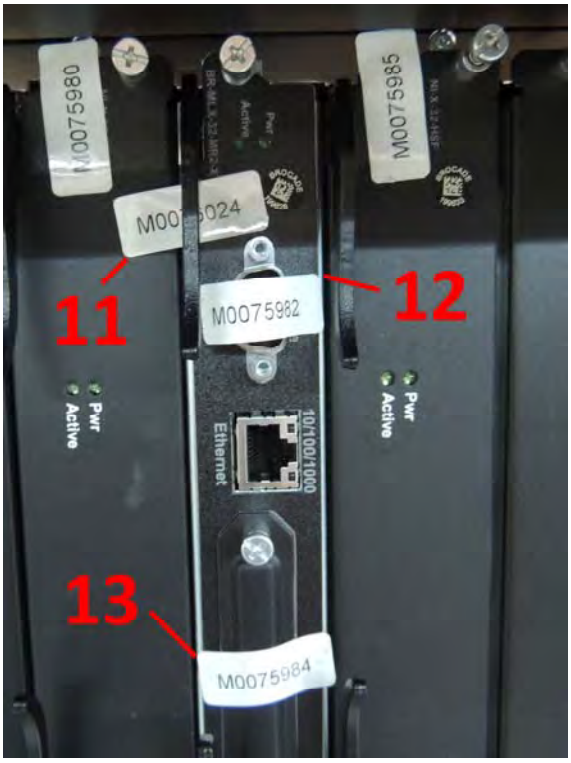

Figure 25 - Label 11 example of MLXe-32

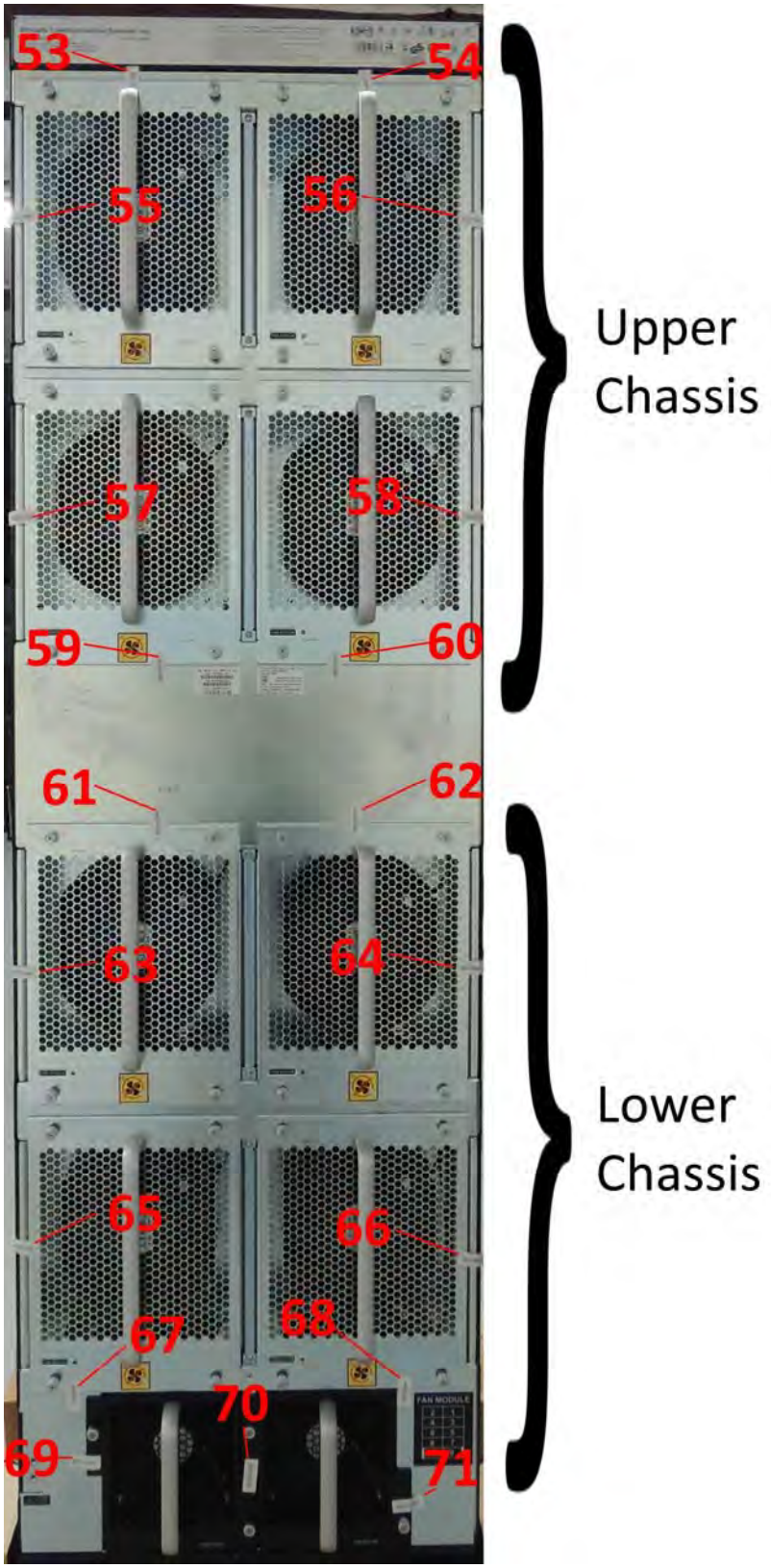

Figure 26 - Back overview of MLXe-32 with tamper labels

Figure 27 - Back upper chassis of MLXe-32 with tamper labels

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

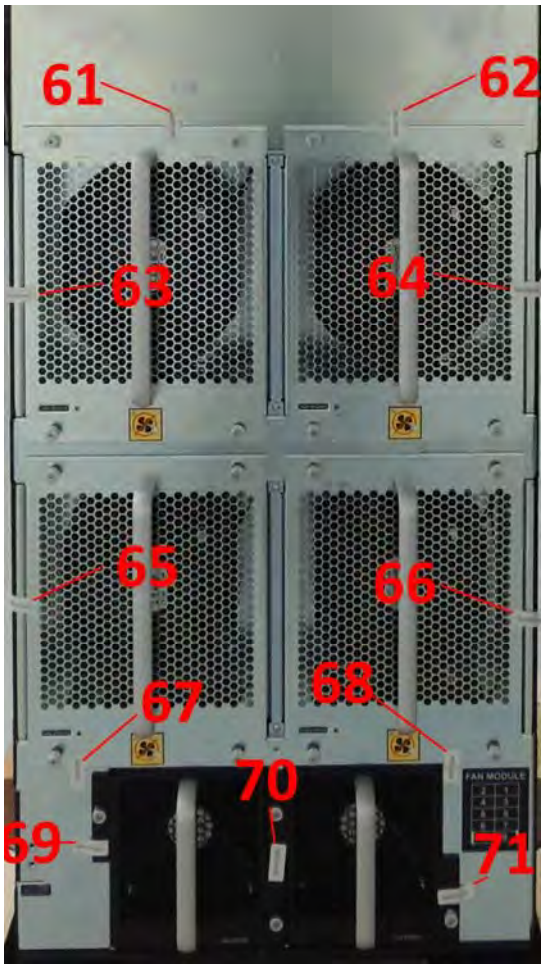

Figure 28 - Back lower chassis of MLXe-32 with tamper labels

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

12 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

Table 40 - Acronyms used in appendix B

The module supports the following CSPs and public keys:

12.1 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)

- 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)

- 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)

- 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)

- 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)

- 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

12.2 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: Derived from SP800-108 KDF (Key agreement via “MACsec” service)
- 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: Derived from SP800-108 KDF (Key agreement via “MACsec” service)
- 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)

- 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)

- 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

12.3 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

12.4 Management card (MP) DRBG

18) MP DRBG Internal State (MLXe-MP-MGMT card)

- 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)

- 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)

- 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)

- 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

12.5 Private Keys

*** SSHv2 ***

22) SSHv2 Client RSA Private Key (MLXe-MP-MGMT card)

- 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)

- 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)

- 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)

- 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.

12.6 Public Keys

*** SSHv2 ***

33) SSHv2 Client RSA Public Key (MLXe-MP-MGMT card)

- 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)

- 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)

- 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)

- 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)

- 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)

- 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)

45) IKEv2 ECDSA Public Key (P-384) (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)

- 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)

- 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

12.7 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 (Key agreement via “IKEv2/IPsec” service)
- 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 (Key agreement via “IKEv2/IPsec” service)
- 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 via “MACsec” service - AES key wrapped with the KEK; Allowed as per FIPS 140-2 IG D.9 (MLXe-MP-MGMT card) (OR)

Key agreement via “MACsec” service – derived from SP800-108 KDF (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)

- 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) key agreement via “SSHv2” service; 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)

- 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 (Key agreement via “TLS client” service) ; 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

12.8 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) (MLXe-MP-MGMT and MLXe-MACsec cards)

- 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)

- 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)

- 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)

- 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)

- 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)

- 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)

- 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)

- 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 when 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; OR Key agreement: TLS DH Key Agreement: allowed method as per FIPS 140-2 IG D.8 Scenario 4

- 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

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

NEXT PAGE →

13 Appendix C: CKG as per SP800-133

In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP800-133 (vendor affirmed). The resulting generated seed, for asymmetric key generation, is the unmodified output from SP800-90A DRBG. Please see Appendix B above for further details.

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

The internal circuitry and power-related components included within the following SKUs do not have any security relevance and have been excluded from FIPS 140-2 requirements:

SKU	MFG Part Number	Brief Description
BR-MLXE-DCPWR-1800	P/N:80-1003972-01	16-slot, 8-slot and 4-slot MLXe DC 1800W power supply
BR-MLXE-32-DCPWR-3000	P/N: 80-1003970-03	32-slot MLXe DC 3000W power supply

Table 41 – SKUs Excluded from FIPS 140-2 requirement - MLXe DC Power Supply Modules

REST OF THIS PAGE WAS INTENTIONALLY LEFT BLANK