Brocade® MLXe® NetIron® Ethernet Routers

FIPS 140-2 Non-Proprietary Security Policy

Document Version 1.1

April 10, 2017

Brocade Communications

Revision History

Revision Date	Revision	Summary of Changes
01/11/2016	1.0	Initial Draft
04/10/2017	1.1	CAVP algorithm certificate numbers for HMAC and CVL were updated.

This Brocade Communications Systems, Inc. Security Policy for Brocade MLXe series embodies Brocade Communications Systems' confidential and proprietary intellectual property. Brocade Systems retains all title and ownership in the Specification, including any revisions.

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

Table of contents:

Table of tables:

Table of figures:

1 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.

This release introduces a new interface card BR-MLX-10GX4-IPSEC-M, which has built-in capability to negotiate IKEv2 sessions and establish IPSec tunnels to allow Virtual Private Networks (VPN) to be created within the network. In addition, BR-MLX-10GX4-IPSEC-M has PHY level support for MACsec protocol. This release also enables MACsec protocol within the BR-MLX-10GX20-M or BR-MLX-10GX20-X2 interface card.

2 Overview

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

Brocade MLXe series devices are chassis devices. Each MLXe chassis contains slots for MR2 management cards, Switch Fabric Modules (SFM), and BR-MLX-10GX20-M, BR-MLX-10GX20-X2, BR-MLX-10GX4-IPSEC-M line cards (interface modules). The SFM pass data packets between the various modules. The interface modules themselves forward data without any cryptographic operation or pass data packets to a management module, if any cryptographic operation has to be performed.

The cryptographic boundary of a Brocade MLXe series device is a chassis with two management cards; one management card runs in active mode while the other is in standby mode. Two line cards (interface modules), BR-MLX-10GX20-M, BR-MLX-10GX20-X2, BR-MLX-10GX4-IPSEC-M, are part of the cryptographic boundary. The fan tray assemblies are part of the cryptographic boundary and can be replaced in the field. The power supplies are not part of the cryptographic boundary. Unpopulated switch fabric module and interface slots are covered by opaque filler panels, which are part of the cryptographic boundary.

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

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.

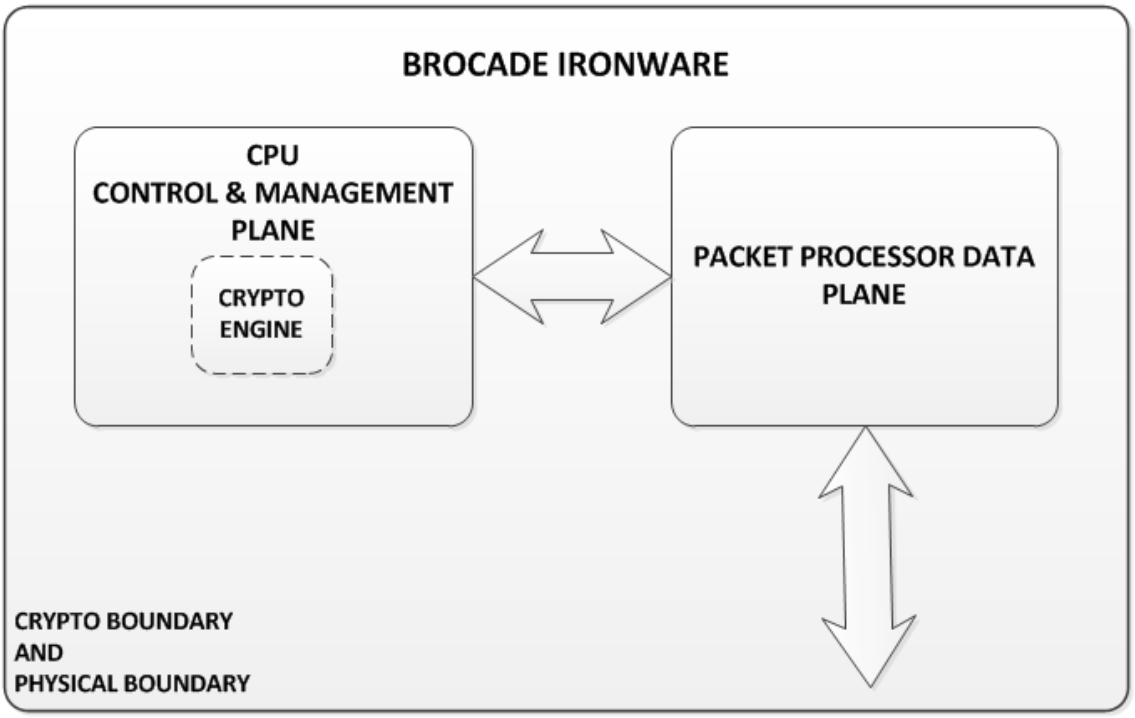

Figure 1 - Block Diagram

3 Brocade MLXe series

Firmware
Multi-Service IronWare R05.8.00a

Table 1 MLXe Series Firmware Version

SKU	MFG Part Number	Brief Description
BR-MLXE-4-MR2-M-AC	P/N: 80-1006870-01	Brocade MLXe-4, AC system with 1 MR2 management module, 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-M-DC	P/N: 80-1006872-01	Brocade MLXe-4 DC system with 1 MR2 management module, 2 high speed switch fabric modules, 1 1800W DC power supply, 4 exhaust fan assembly kits and air filter. Power cord not included.
BR-MLXE-8-MR2-M-AC	P/N: 80-1007225-01	Brocade MLXe-8 AC system with 1 MR2 management module, 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 module, 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 module, 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 module, 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-4-MR2-X-AC	P/N: 80-1006874-03	Brocade MLXe-4, AC system with 1 MR2 management module, 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 module, 2 high speed switch fabric modules, 1 1800W DC power supply, 4 exhaust fan assembly kits and air filter. Power cord not included.
BR-MLXE-8-MR2-X-AC	P/N: 80-1007227-03	Brocade MLXe-8 AC system with 1 MR2 management module, 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-X-DC	P/N: 80-1007228-03	Brocade MLXe-8 DC system with 1 MR2 management module, 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-X-AC	P/N: 80-1006829-04	Brocade MLXe-16 AC system with 1 MR2 management module, 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-X-DC	P/N: 80-1006834-04	Brocade MLXe-16 DC system with 1 MR2 management module, 3 high speed switch fabric modules, 4 1800W DC power supplies, 2 exhaust fan assembly kits and air filter. Power cord not included.

Table 2 MLXe Series Part Numbers

SKU	MFG Part Number	Brief Description
BR-MLX-MR2-M	P/N: 80-1005643-01	Brocade MLX system management module, 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) module 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-10GX20-M	P/N:80-1007878-02	Brocade MLXe twenty (20)-port 10-GBE/1-GBE (M) combo module with IPv4/IPv6/MPLS hardware support. Requires SFP+ and SFP optics. Supports 512K IPv4 routes in FIB. Requires high speed switch fabric modules
BR-MLX-10GX20-X2	P/N:80-1007911-02	Brocade MLXe twenty (20)-port 10-GBE/1-GBE (X2) combo module 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) module with 512K IPv4 or 128K IPv6 routes in hardware. It requires MR2 management module and High Speed Switch Fabric module (hSFM).

Table 3 MLXe Management and Interface Module Part Numbers

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

Table 4 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-DCPWR-1800	P/N: 80-1003972-01	16-slot, 8-slot and 4-slot MLXe DC 1800W power supply
NI-X-ACPWR	P/N: 80-1003811-02	16-slot, 8-slot and 4-slot MLXe AC 1200W power supply
NI-X-DCPWR	P/N: 80-1002756-03	16-slot, 8-slot and 4-slot MLXe DC 1200W power supply

Table 5 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

Table 6 MLXe Fan Module Part Numbers

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

Table 7 MLXe Filler Panel Part Numbers

Validated MLXe configurations are listed below.

Chassis Model	Module Descriptions	Modules (quantities)
MLXe-4 Configuration 1	Management modules(s):	BR-MLX-MR2-M (2)
	Interface module(s):	BR-MLX-10GX20-M (1) or BR-MLX-10GX20-X2 (1), and BR-MLX-10GX4-IPSEC-M (1)
	Switch Fabric:	NI-X-4-HSF (2)
	Filler Panels:	NI-X-SF1PNL (1), NI-X-IPNL (2)
	Fan:	BR-MLXE-4-FAN (4)
	Power:	BR-MLXE-ACPWR-1800 (1), or BR-MLXE-DCPWR-1800 (1) and NI-X-PWRPNL-A (3)
MLXe-4 Configuration 2	Management modules(s):	BR-MLX-MR2-X (2)
	Interface module(s):	BR-MLX-10GX20-X2 (1) and BR-MLX-10GX4-IPSEC-M (1)
	Switch Fabric:	NI-X-4-HSF (2)
	Filler Panels:	NI-X-SF1PNL (1), NI-X-IPNL (2)
	Fan:	BR-MLXE-4-FAN (4)
	Power:	BR-MLXE-ACPWR-1800 (1), or BR-MLXE-DCPWR-1800 (1), and NI-X-PWRPNL-A (3)
MLXe-8 Configuration 1	Management modules(s):	BR-MLX-MR2-M (2)
	Interface module(s):	BR-MLX-10GX20-M, or BR-MLX-10GX20-X2 (1) and BR-MLX-10GX4-IPSEC-M (1)
	Switch Fabric:	NI-X-16-8-HSF (2)
	Filler Panels:	NI-X-SF3PNL (1), NI-X-IPNL (7)
	Fan:	BR-MLXE-8-FAN (2)
	Power:	BR-MLXE-ACPWR-1800 (2), or BR-MLXE-DCPWR-1800 (2), and NI-X-PWRPNL (2)

MLXe-8 **Configuration 2**	Management modules(s):	BR-MLX-MR2-X (2)
	Interface module(s):	BR-MLX-10GX20-X2 (1) and BR-MLX-10GX4-IPSEC-M (1)
	Switch Fabric:	NI-X-16-8-HSF (2)
	Filler Panels:	NI-X-SF3PNL (1), NI-X-IPNL (7)
	Fan:	BR-MLXE-8-FAN (2)
	Power:	BR-MLXE-ACPWR-1800 (2), or BR-MLXE-DCPWR-1800 (2), and NI-X-PWRPNL (2)
MLXe-16 **Configuration 1**	Management modules(s):	BR-MLX-MR2-M (2)
	Interface module(s):	BR-MLX-10GX20-M (1), or BR-MLX-10GX20-X2 (1) and BR-MLX-10GX4-IPSEC-M (1)
	Switch Fabric:	NI-X-16-8-HSF (3)
	Filler Panels:	NI-X-SF3PNL (1), NI-X-IPNL (14)
	Fan:	BR-MLXE-16-FAN (2)
	Power:	BR-MLXE-ACPWR-1800 (4), or BR-MLXE-DCPWR-1800 (4), and NI-X-PWRPNL(4)
MLXe-16 **Configuration 2**	Management modules(s):	BR-MLX-MR2-X (2)
	Interface module(s):	BR-MLX-10GX20-X2 (1) and BR-MLX-10GX4-IPSEC-M (1)
	Switch Fabric:	NI-X-16-8-HSF (3)
	Filler Panels:	NI-X-SF3PNL (1), NI-X-IPNL (14)
	Fan:	BR-MLXE-16-FAN (2)
	Power:	BR-MLXE-ACPWR-1800 (4), or BR-MLXE-DCPWR-1800 (4), and NI-X-PWRPNL(4)

Table 8 Validated MLXe Configurations

Figure 2 - 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 8.

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

Figure 4 - MLXe-8

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 8.

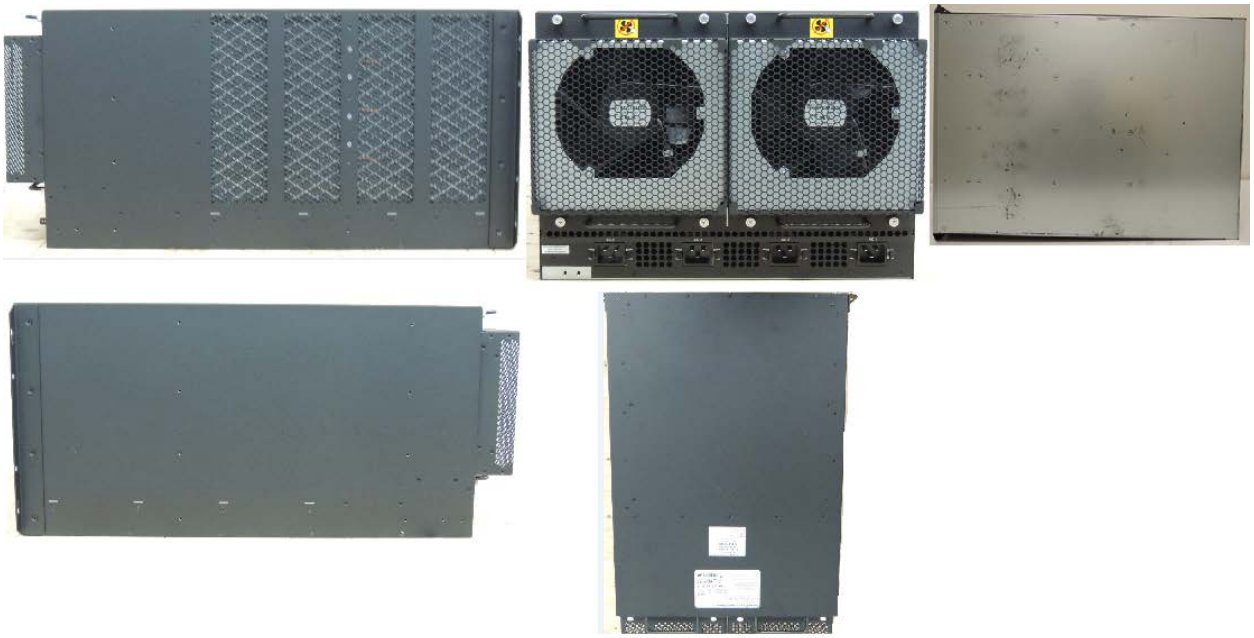

Figure 5 - MLXe-8: Starting from left to right: Left side, Rear side, Bottom side, Right side, and Top side

Figure 6 - MLXe-16

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 8.

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

4 Ports and Interfaces

Each MLXe device provides network ports, management connectors, and status LED. This section describes the physical ports and the interfaces they provide for Data input, Data output, Control input, and Control output.

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

Physical Interface	Logical Interface
Networking ports	Data input
Console	
Networking ports	Data output
Console	
Networking ports	Control input
Console	
PCMCIA	
Networking ports	Status output
Console	
LED	
PCMCIA	
Power plugs	Power

Table 9 Physical/Logical Interface Correspondence

While not included in this validation, the Brocade MLXe series supports a variety of interface modules. The interface modules provide Ethernet ports with multiple connector types and transmission rates. Models in the series up to MLXe-16 can provide:

- 384 10 Gigabit Ethernet ports per chassis
- 768 Gigabit Ethernet ports per chassis

4.1 MLXe MR2 Management cards

The MR2 management module provides physical ports and status indicators. The MR2's major features are listed below.

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

4.2 BR-MLX-10GX20-M and BR-MLX-10GX20-X2 interface cards

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

- 20 port 1/10GE combo port
- LED indicators
- Power and status LEDs

4.3 BR-MLX-10GX4-IPSEC-M interface card

The BR-MLX-10GX4-IPSEC-M interface card provides physical ports and status indicators.
The BR-MLX-10GX4-IPSEC-M card's major features are listed below.

- 4 port 1/10GE combo SFP & 4 port 1/10GE SFP+ ports
- LED indicators
- Power and status LEDs

4.4 Status LEDs

Power and status LEDs for the BR-MLX-10GX20-M, BR-MLX-10GX20-X2, BR-MLX-10GX4-IPSEC-M interface modules are described in table below.

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 module
	Off	The module is functioning as the standby management module.
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 10 Power and status LEDs for BR-MLX-10GX20-M, BR-MLX-10GX20-X2, BR-MLX-10GX4-IPSEC-M Interface Modules

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 module
	Off	The module is functioning as the standby management module.
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 11 Power and fan status LEDs for the MR2 Management Module

4.5 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 6 describes services and cryptographic algorithms available in FIPS Approved mode.

Section 8.1.1.1 FIPS Approved Mode describes how to invoke FIPS Approved mode.

4.6 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 12 NetIron Security Levels

5 Roles

In FIPS Approved mode, NetIron devices support five authenticated roles: Crypto-officer, Port Configuration Administrator, User, MACsec Peer, and IKEv2 Peer:

1. 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.
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.
3. User Role: The User role on the device in FIPS Approved mode has read-only privileges and no configuration mode access (user).
4. MACsec Peer: A peer device which establishes a MACsec connection with the cryptographic module.
5. IKEv2 Peer: Role assumed when using the IKEv2 Authentication Key.

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

6 Services

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

For all other services, an operator must authenticate to the device as described in Section 7.2 Authentication.

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

The following subsections describe services available to operators based on role. Each description includes lists of cryptographic functions and critical security parameter (CSP) associated with the service.

The table below summarizes the available FIPS Approved cryptographic functions.

Label	Cryptographic Function
AES	Advanced Encryption Standard
SHS	Secure Hash Standard
HMAC	Keyed-Hash Message Authentication Code
DRBG	Deterministic Random Bit Generator
RSA	Rivest Shamir Adleman
CVL	SSHv2 and TLS v1.0/1.1 and TLS v1.2 Key Derivation Function, SNMPv3 KDF, IKEv2 KDF, SP800-56A (ECC, FFC)
Triple-DES NOTICE: Two-key Triple-DES and Three-key Triple-DES are NOT available within any service in the Approved mode of operation. Two-key Triple-DES is not available within any service in the non-FIPS Approved mode of operation. Three-key Triple-DES is available in the non-FIPS Approved mode of operation	Triple Data Encryption Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
KBKDF	SP800-108 Key Based Key Derivation Function (CTR_Mode)

Table 13 FIPS Approved Cryptographic Functions

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

Label	Cryptographic Function
KW	RSA key transport (within TLS v1.0/1.1 and TLS v1.2 protocol) (key wrapping; key establishment methodology provides 112 bits of encryption strength)
DH	Diffie-Hellman (within SCP/SSHv2 protocol) (key agreement; key

	establishment methodology provides 112 bits of encryption strength)
MD5	Message-Digest Algorithm
NDRNG	Nondeterministic Random Number Generator used for generation of seeds for DRBG only
HMAC-MD5	Used to support RADIUS authentication
HMAC-SHA1-96 (non-compliant)	Used for OSPFv3 authentication

Table 14 Non-Approved Cryptographic Functions Allowed in FIPS Approved Mode

6.1 User Role Services

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

6.1.1 SSHv2

The module supports SSHv2. This service provides a secure session between a NetIron device and an SSHv2 client. The NetIron device authenticates an SSHv2 client and provides an encrypted communication channel. An operator may use an SSHv2 session for managing the device via the command line interface. The following cipher sequence is supported for SSHv2: aes-256-ctr, aes-192-ctr, aes-128-ctr, aes-256-cbc, aes-192-cbc and aes-128-cbc.

NetIron devices support three kinds of SSHv2 client authentication: password, keyboard interactive and 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 or 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.

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

6.1.2 HTTPS

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 cipher suites TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA and TLS_DHE_RSA_WITH_AES_256_CBC_SHA.

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’s credentials. The challenge dialog box does not close unless the operator provides the Crypto-officer’s access credentials. After three failed attempts, the page ‘Protected Object’ is displayed, in effect disallowing any changes from the web.

6.1.3 SNMP

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

6.1.4 Console

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

6.2 Port Configuration Administrator Role Services

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

6.2.1 SSHv2

This service is described in Section 6.1.1 above.

The port configuration administrator will have 7 commands, which allows this user to run show commands, run ping or traceroute and the enable command which allows this user to re-authenticate as described in Section 6.1.1. Within the configuration mode, this role provides access to all the port configuration commands. That is, all sub-commands within “interface eth 1/1” command. This operator cannot transfer and store software images and configuration files between the network and the system. However, this operator can review the configuration.

6.2.2 HTTPS

This service is described in Section 6.1.2 above.

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

6.2.3 SNMP

This service is described in Section 6.1.3 above.

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

6.2.4 Console

This service is described in Section 6.1.4 above.

Console access as the Port Configuration Administrator provides an operator with the same capabilities as User Console commands plus configuration commands associated with a network port on the device. The commands available to operator within the Port Configuration Administrator role are same as those mentioned in the SSHv2 service in Section 6.1.1.

6.3 Crypto-officer Role Services

The Crypto-officer 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.

6.3.1 SSHv2

This service is described in Section 6.1.1 above.

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

6.3.2 SCP

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

6.3.3 HTTPS

This service is described in Section 6.1.2 above.

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

6.3.4 SNMP

This service is described in Section 6.1.3 above.

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

6.3.5 Console

This service is described in Section 6.1.4 above.

Console commands provide an authenticated Crypto-officer 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; afterwards the operator may securely import additional pairs of RSA host keys over a secured SSHv2 connection. To enable the Web Management service, the operator would securely import a pair of RSA host keys and a digital certificate using corresponding commands (over a secured SSHv2 connection), and enable the HTTPS server.

6.4 MACsec Peer Role Services

6.4.1 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.

6.5 IKEv2 Peer Role Services

6.5.1 IKEv2 Negotiation – IPsec Traffic

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

6.6 Non-Approved Mode Services

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

Role(s)	Function/Service	Additional Details
Crypto-officer Role	TFTP	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 (no cryptography)
Crypto-officer Role, Port Configuration Administrator Role, User Role	Telnet	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 (no cryptography)
Crypto-officer Role, User Role	HTTP	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 (no cryptography)
Crypto-officer Role, User Role	SNMP	SNMPv1, SNMPv2c and SNMPv3 in noAuthNoPriv, authNoPriv modes . Modes – DES in authPriv mode for SNMPv3 Key sizes – DES 56 bits
Crypto-officer Role, Port Configuration Administrator Role, User Role	SSHv2	Secure Shell (SSHv2) is a cryptographic (encrypted) network protocol for initiating text-based shell sessions on remote machines in a secure way. Modes – RSA Key sizes – 1024 bit Modes – Triple-DES Key sizes – Three-Key Triple-DES

Table 15 Roles, Functions/Services in Non-Approved Mode Services

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 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.

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 cryptographic module performs the following tests:
   a) Power-up Self-Tests:
      (i) Cryptographic Known Answer Tests (KAT):
         (1) Three-Key Triple-DES KAT (encrypt)
         (2) Three-Key Triple-DES KAT (decrypt)
         (3) AES-128, 192, 256-bit key sizes KAT (encrypt)
         (4) AES-128, 192, 256-bit key sizes KAT (decrypt)
         (5) AES-CMAC KAT
         (6) AES-KW KAT (wrap)
         (7) AES-KW KAT (unwrap)
         (8) ECDSA KAT (sign)
         (9) ECDSA KAT (verify)
         (10) SHA-1, 256, 384, 512 KAT (hashing)
         (11) HMAC-SHA-1, 256 KAT (hashing)
         (12) RSA 2048 bit key size KAT (encrypt)
         (13) RSA 2048 bit key size KAT (decrypt)
         (14) RSA 2048 bit key size, SHA-256, 384, 512 Hash KAT (signature generation)
         (15) RSA 2048 bit key size, SHA-256, 384, 512 Hash KAT (signature verification)
         (16) SP800-90A DRBG KAT
         (17) SP800-135 TLS v1.0/1.1 KDF KAT
         (18) SP800-135 SSHv2 KDF KAT
         (19) SP800-135 TLS v1.2 KDF KAT
         (20) SP800-135 SNMPv3 KDF KAT
         (21) SP800-135 IKEv2 KDF KAT
         (22) SP800-108 KBKDF KAT
         (23) AES GCM KAT
         (24) ECDH KAT
      (ii) Firmware Integrity Test: (CRC 16)

(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.
```

(iv) If the module detects an error during the POST, at the conclusion of the test, the console displays the message shown below. After displaying the failure message, the module reboots.

```
Crypto Module Failed <Reason String>
```

b) Conditional Self-Tests:

(i) Continuous Random Number Generator (RNG) Test: performed on non-Approved RNG.

(ii) Continuous Random Number Generator Test: performed on DRBG.

(iii) RSA 2048 SHA-256 Pairwise Consistency Test (Sign/Verify)

(iv) RSA 2048 SHA-256 Pairwise Consistency Test (Encrypt/Decrypt)

(v) ECDSA Pairwise Consistency Test (Sign/Verify)

(vi) Firmware Load Test: RSA 2048 SHA-256 Signature Verification

(vii) Bypass Test: Alternating Bypass Test

(viii) Manual Key Entry Test: N/A

4) 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.

5) Data output to services defined in Section 6 Services is inhibited during key generation, self-tests, zeroization, and error states.

6) Do not enable or configure DH Group 14 and DH Group 19 IKEv2 CSPs in FIPS mode.

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

8) 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

7.1.1 Cryptographic Module Operational Rules

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

Do not make external communication channels/ports available before initialization of an MLXe series device.

MLXe series devices use a FIPS Approved random number generator implementing Algorithm CTR_DRBG based on hash functions.

MLXe series devices ensure that the random number seed and seed key input do not have same value. The devices generate seed keys and do not accept a seed key entered manually.

MLXe series devices use FIPS Approved key generation methods:

- RSA public and private keys

MLXe series devices test the prime numbers generated for RSA keys using Miller-Rabin Test.

MLXe series 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/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/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.

7.2.1 Line Authentication Method

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

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

7.2.5 TACACS/TACACS+ Authentication Method

The TACACS and TACACS+ methods use one or more TACACS/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/TACACS+ authentication, a Crypto-officer must configure TACACS/TACACS+ server settings along with authentication and authorization settings.

7.2.6 Strength 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.

Knowledge of IKEv2 Authentication Key:

Due to the key size being 384 bits, the probability that a random attempt will succeed or a false acceptance will occur is 1/2^384, which is less than 1/1,000,000.

The maximum attempts allowed in a one minute period is equal to three attempts. Therefore, the probability of a random success in a one minute period is 3/2^384, which is less than 1/100,000.

7.3 Access Control and Critical Security Parameters (CSPs)

Table 16 and Table 17 summarize the access operators in each role have to CSPs. Blank table cells indicate that there is no security relevance between the role and the CSP. The table entries have the following meanings:

- r – Operator can read the value of the item,
- w – Operator can write a new value for the item,
- x – Operator can use the value of the item (for example encrypt with an encryption key), and
- d – Operator can delete the value of the item (zeroize) by executing a `fips zeroize all` command. See item 4a in Section 8.1.1.1 for further details.

ROLE➔	Crypto-officer					User				Port Administrator		
CSP / Service	SSHv2	SCP	HTTPS	SNMP	Console	SSHv2	HTTPS	SNMP	Console	SSHv2	HTTPS	Console
SSHv2 Host RSA Private Key (2048 bit)	xwd	x			wd	x				x		
SSHv2 Client RSA Private Key	xwd	x			wd	x				x		
SSHv2 DH Group-14 Private Key (2048 bit)	xwd	x			wd	x				x		
SSHv2 DH Shared Secret Key (2048 bit)	x	x			xd	x				x		
SSHv2/SCP Session Keys (128, 192 and 256 bit (AES CBC and AES CTR)	x	x			xd	x				x		
SSHv2/SCP Authentication Key (HMAC-SHA-1, 160 bits)	x	x			xd	x				x		
SSHv2 KDF Internal State	x	x			xd	x				x		
TLS Host RSA Private Key (RSA 2048 bit)	rwd		x		rwd		x				x	
TLS Pre-Master Secret			x		xd		x				x	
TLS Master Secret			x		xd		x				x	
TLS KDF Internal State	xd		x		xd		x				x	
TLS Session Key			x		xd		x				x	
TLS Authentication Key			xd		xd		x				x	
MP DRBG Seed	x	x	x		xd	x	x			x	x	
MP DRBG Value V	x	x	x		xd	x	x			x	x	
MP DRBG Key	x	x	x		xd	x	x			x	x	
MP DRBG Internal State	xd	x	x		xd	x	x			x	x	
User Password	xrwd	xrwd	xrwd	x	xrwd	x	x	x	x			
Port Administrator Password	xrwd	xrwd	rwd		xrwd					x	x	x
Crypto-officer Password	xrwd	xrwd	xrwd		xrwd							
RADIUS Secret	xrwd	xrwd	xrwd		xrwd	x	x		x	x	x	x
TACACS+ Secret	xrwd	xrwd	xrwd		xrwd	x	x		x	x	x	x
Firmware Load RSA Public Key	x		x		xd							
SSHv2 Host RSA Public Key	xrwd	xrw			rwd	x				x		
SSHv2 Client RSA Public Key	xrwd	xrwd			xrwd	x				x		
SSHv2 DH Public Key	x	x			xd	x				x		

SSHv2 DH Peer Public Key	x	x			xd	x				x		
ROLE➔	**Crypto-officer**					**User**				**Port Administrator**		
CSP / Services	**SSHv2**	**SCP**	**HTTPS**	**SNMP**	**Console**	**SSHv2**	**HTTPS**	**SNMP**	**Console**	**SSHv2**	**HTTPS**	**Console**
TLS Host Public Key (RSA 2048 bit)	rwd		x		rwd		x				x	
TLS Peer Public Key (RSA 2048 bit)	rwd		x		rwd		x				x	
ECDSA Public Key (P-384)	rwd	rw			rwd							
Connectivity Association Key (CAK)	wd	rwd			wd							
Connectivity Key Name (CKN)	rwd	rwd			rwd							
SP800-108 KDF State	rwd				rwd							
ECDSA Private Key (P-384)	rwd	rw			rwd							
IKE Pre-Shared Key (PSK)	rwd				rwd							

Table 16 Access Control Policy and Critical Security Parameters (CSPs)

ROLE ➔	**MACsec Peer**	**IKEv2 Peer**
CSP / Service	**MACsec**	**IKEv2 Negotiation - IPsec Traffic**
Integrity Checksum Key (ICK)	xrwd	
Key Encryption Key (KEK)	xrwd	
Secure Association Key (SAK)	xrwd	
SP800-108 KDF State	xrwd	
Connectivity Association Key (CAK)	rd	
Connectivity Key Name (CKN)	rd	
ECDSA Private Key (P-384)		xrd
ECDSA Public Key (P-384)		xrd
ECDH Private Key (P-384)		xrwd
ECDH Public Key (P-384)		xrwd
ECDH Shared Secret (P-384)		xrwd
IKEv2 Encrypt/Decrypt Key		xrwd
IKEv2 Authentication Key		xrwd
ESP Encrypt/Decrypt Key		xrwd
IKEv2 KDF State		xrwd
IKE Pre-Shared Key (PSK)		xrd

LP DRBG Seed		xrd
LP DRBG Value V		xrd
LP DRBG Value C		xrd
LP DRBG Internal State		xrd

Table 17 MACsec and IPSec Access Control Policy and Critical Security Parameters (CSPs)

7.3.1 CSP Zeroization

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

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

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.

Executing the "`no fips enable`" command zeroizes all host key pairs.

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

7.4 Physical Security

NetIron devices require the Crypto-officer to install tamper evident labels (TELs) in order to meet FIPS 140-2 Level 2 Physical Security requirements. The TELs are available from Brocade under part number XBR-000195. The Crypto-officer 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 Appendix A.

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 Appendix A.

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 FIPS Approved state after any intentional or unintentional reconfiguration of the physical security measures.

8.1 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 8.1.1 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).

FIPS mode: Administrative Status: OFF, Operational Status: OFF

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.

```
FIPS mode: Administrative Status: ON, Operational Status: OFF
Some shared secrets inherited from non-Approved mode may not be FIPS 140-2
compliant and have to be zeroized separately by the Crypto-officer before
the system is rebooted. This ensures that the data path of the system is not
immediately impacted after FIPS Approved mode is enabled administratively. A
separate command needs to be executed by the Crypto-officer in order to
zeroize all the configured shared secrets and keys.
The system needs to be reloaded to operationally enter FIPS Approved mode.
System Specific:
OS monitor mode access:                                        Disabled
Management Protocol Specific:
Telnet server:                                                 Disabled
TFTP Client:                                                   Disabled
HTTPS SSL 3.0:                                                 Disabled
SNMP Access to security objects:                               Disabled
Critical Security Parameter Updates across FIPS Boundary:
Protocol shared secret and host passwords:                     Clear
SSH RSA Host and Client Keys:                                  Clear
HTTPS RSA Host Keys and Signature:                             Clear


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 mode: Administrative Status: ON, Operational Status: ON System
Specific:
OS monitor mode access:                                        Disabled
Management Protocol Specific:
Telnet server:                                                 Disabled
TFTP Client:                                                   Disabled
```

HTTPS SSL 3.0:	Disabled
SNMP Access to security objects:	Disabled
Critical Security Parameter Updates across FIPS Boundary:	
Protocol shared secret and host passwords:	Clear
SSH RSA Host and Client Keys:	Clear
HTTPS RSA Host Keys and Signature:	Clear

8.1.1 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. Telnet access including the telnet server command
2. 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
3. Command ip ssh scp disable
4. TFTP access
5. SNMP access to CSP MIB objects
6. Access to all commands that allows debugging memory content within the monitor mode
7. HTTP access including the web-management http command
8. HTTPS SSL 3.0 access
9. Command web-management allow-no-password
10. Do not enable or configure DH Group 14 and DH Group 19 IKEv2 CSPs in FIPS mode

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

Algorithm	Support	Certificate
Advanced Encryption Standard (AES)	128, 192, and 256-bit keys, ECB and CBC mode, CMAC, KTS, CFB-128, CTR, GCM	#2717 #2946 #3030 #3144
Advanced Encryption Standard (AES)	KTS with 112 bits of encryption strength	#2946

Triple Data Encryption Algorithm (Triple-DES) NOTICE: Two-key Triple-DES and Three-key Triple-DES are NOT available within any service in the Approved mode of operation. Two-key Triple-DES is not available within any service in the non-FIPS Approved mode of operation. Three-key Triple-DES is available in the non-FIPS Approved mode of operation.	KO 1, 2 ECB and CBC mode	#1634
Secure Hash Algorithm	SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	#2282
Keyed-Hash Message Authentication code (HMAC)	HMAC SHA-1, HMAC SHA-256	#1696
Deterministic Random Bit Generator (DRBG)	SP800-90A CTR_DRBG	#454
Rivest Shamir Adleman Signature Algorithm (RSA) NOTICE: The module does not support 1024-bit keys in FIPS Mode	1024-bit and 2048-bit keys	#1413
Component Test Key Derivation Function (CVL)	TLS v1.0/1.1 KDF	#175
Component Test Key Derivation Function (CVL)	TLS v1.2 KDF	#393
Component Test Key Derivation Function (CVL)	SSHv2 KDF	#175
Component Test Key Derivation Function (CVL)	SNMPv3 KDF	#404
SP800-108 (KBKDF)	CTR_Mode	#35
ECDSA	P-384 *(Note: P-256 is latent; not exposed within any available service)*	#546

Table 18 Algorithm Certificates for the MLXe Series

Algorithm	Supports	Certificates
Advanced Encryption Standard (AES)	ECB (e only; 128); GCM	#2154

Table 19 Algorithm Certificates for BR-MLX-10GX20-M and BR-MLX-10GX20-X2 interface cards

Algorithm	Supports	Certificates
ECDSA	P-384 *(Note: P-256 is latent; not exposed within any available service)*	#593
Advanced Encryption Standard (AES) NOTICE: Brocade uses FreeScale AES Cert #1648. Only the AES modes listed in this table are used in this cryptographic module; all other modes listed in the FreeScale AES Cert #1648 are not supported by this cryptographic module.	ECB, GCM, CBC, CFB128, OFB, CTR	#1648
Advanced Encryption Standard (AES)	ECB, GCM	#3030
Keyed-Hash Message Authentication Code (HMAC)	HMAC-SHA-256, HMAC-SHA-384	#2883
Secure Hash Algorithm	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	#934
Deterministic Random Bit Generator (DRBG)	SP800-90A HASH_DRBG	#684
Component Test Key Derivation Function (CVL)	IKEv2	#1050
Component Test, All of SP800-56A Except KDF (CVL)	ECDH	#437

Table 20 Algorithm Certificates for BR-MLX-10GX4-IPSEC-M interface cards

NOTICE: Further details for each CAVP algorithm validation certificate, including but not limited to details on the associated processors, can be found at the CAVP website: http://csrc.nist.gov/groups/STM/cavp/validation.html

NOTICE: Operators should reference the transition tables that will be available at the CMVP Web site (http://csrc.nist.gov/groups/STM/cmvp/). The data in the tables will inform users of the risks associated with using a particular algorithm and a given key length.

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

The following non-Approved but allowed cryptographic methods are allowed within limited scope in the FIPS Approved mode of operation:

1. RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
2. Diffie-Hellman (key agreement; key establishment provides 112 bits of encryption strength)
3. MD5 – Used in the TLS v1.0 KDF in FIPS mode as per SP800-135 (MD5 is not exposed to the operator)
4. MD5 – Used in TACACS+ for operator authentication only (MD5 is not exposed to the operator)
5. HMAC-MD5 – Used to support RADIUS for operator authentication only (HMAC-MD5 is not exposed to the operator)
6. HMAC-SHA1-96 – Used for IPSec AH Authentication header, which is used for OSPFv3 authentication (Notice: The module provides a service to configure OSPFv3 authentication, however, use of OSPFv3 requires hardware that is not included within the scope of the validated configuration. Furthermore, the latent OSPFv3 authentication implemented by the module does not provide cryptographic protection, and is considered plaintext.).
7. NDRNG – Non-deterministic random number generator used for generation of seeds for DRBG only.

8.1.1.1 Invoking FIPS Approved Mode for Brocade MLXe Series Devices

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

1) Assume Crypto-officer role
   a) The authentication methods available for assuming the Crypto-officer role through the console terminal port are defined in Section 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) Enter command: `fips zeroize all`
   a) The device zeroizes the shared secrets use by various networking protocols including host access passwords, SSHv2 Host keys, and HTTPS host keys with the digital signature.
5) Save the running configuration: `write memory`
   a) The device saves the running configuration as the startup configuration
6) Reload the device
   a) The device resets, does a Power-On Self-Test and if successful, begins operation in FIPS Approved mode.
7) Enter command: `fips show`
   a) The device displays the FIPS-related status, which should confirm the security policy is the default security policy.
8) Inspect the physical security of the module, including placement of tamper evident labels according to Appendix A.

8.1.1.2 Negating FIPS Approved Mode for Brocade MLXe Series Devices

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

1) Enter command: `no fips enable`
   a) This will return the device back to normal, non-Approved mode by enabling the networking protocols that were disallowed in FIPS Approved mode of operation. For example, Telnet, HTTP, TFTP will be enabled again. In addition, the restrictions against the non-Approved cryptographic algorithms will also be lifted. For example, MD5, DES algorithms would be allowed.
   b) The device zeroizes the shared secrets used by various networking protocols including host access passwords, SSHv2 Host keys, and HTTPS host keys with the digital signature.
   c) Reload the device to begin non-Approved mode of operation.

9 Mitigation of other attacks

This module is not designed to mitigate against any attacks outside the scope of FIPS 140-2.

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
DSA	Digital Signature Algorithm
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

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 Applying Tamper Evident Seals to a Brocade 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 8 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 9 for correct seal orientation and positioning.

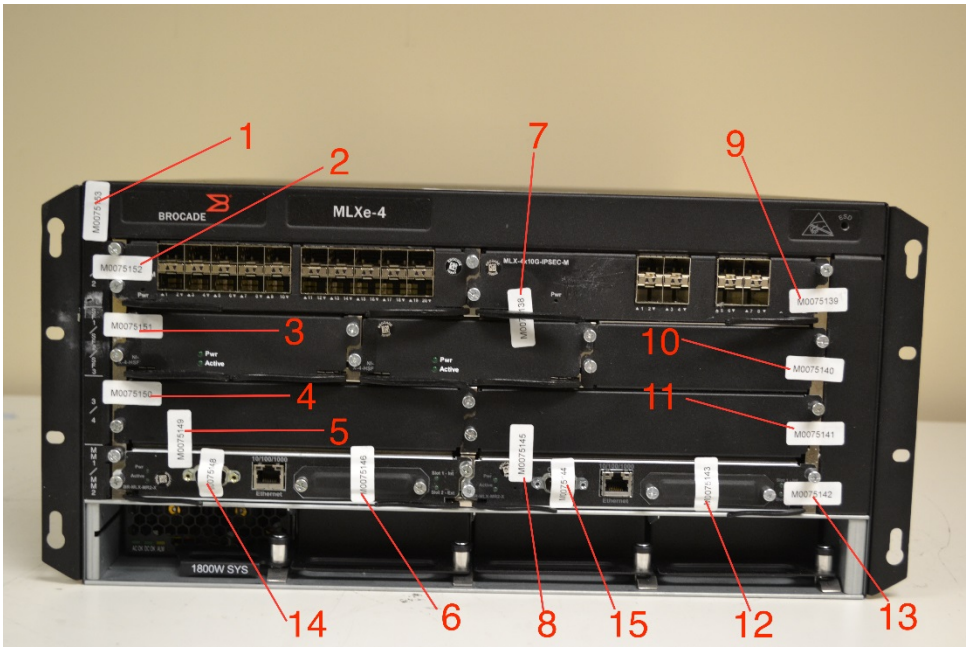

Figure 8 - Front view of Brocade MLXe-4 with security seals

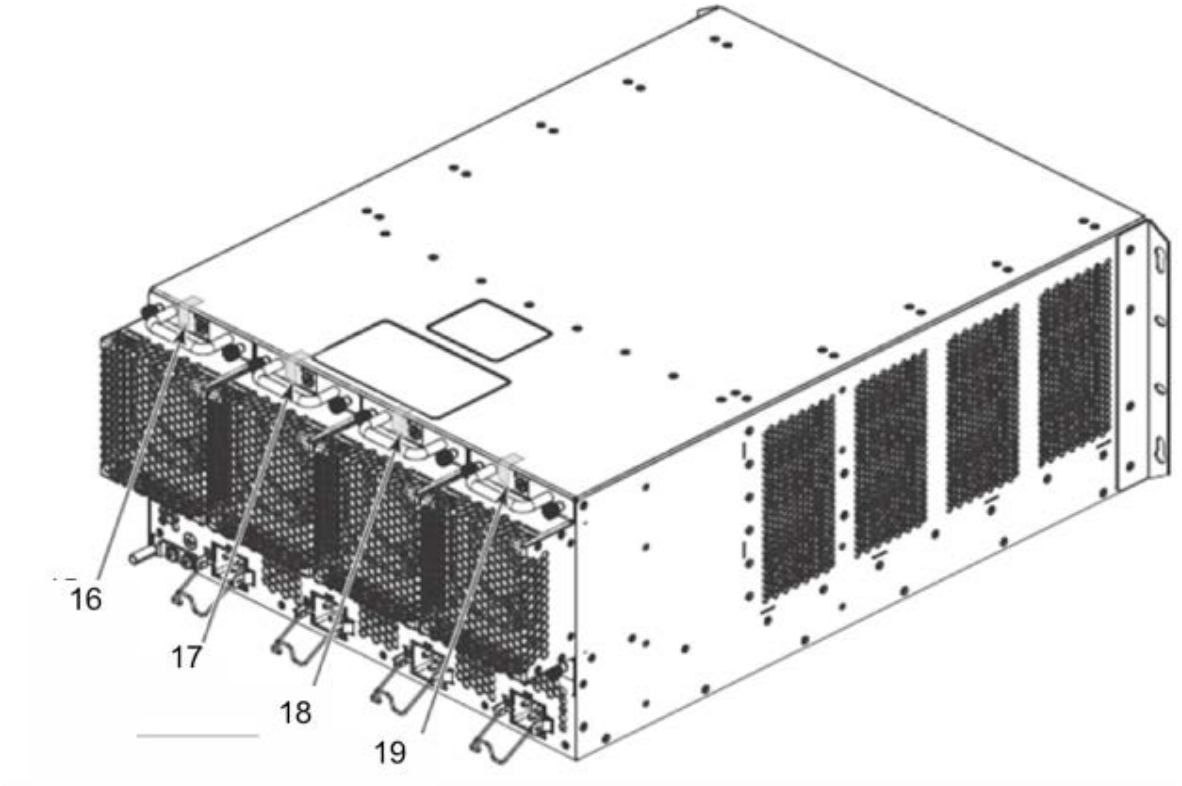

Figure 9 - Rear view of Brocade MLXe-4 device with security seals

11.2 Applying Tamper Evident Seals to a Brocade 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 10 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 11 for correct seal orientation and positioning.

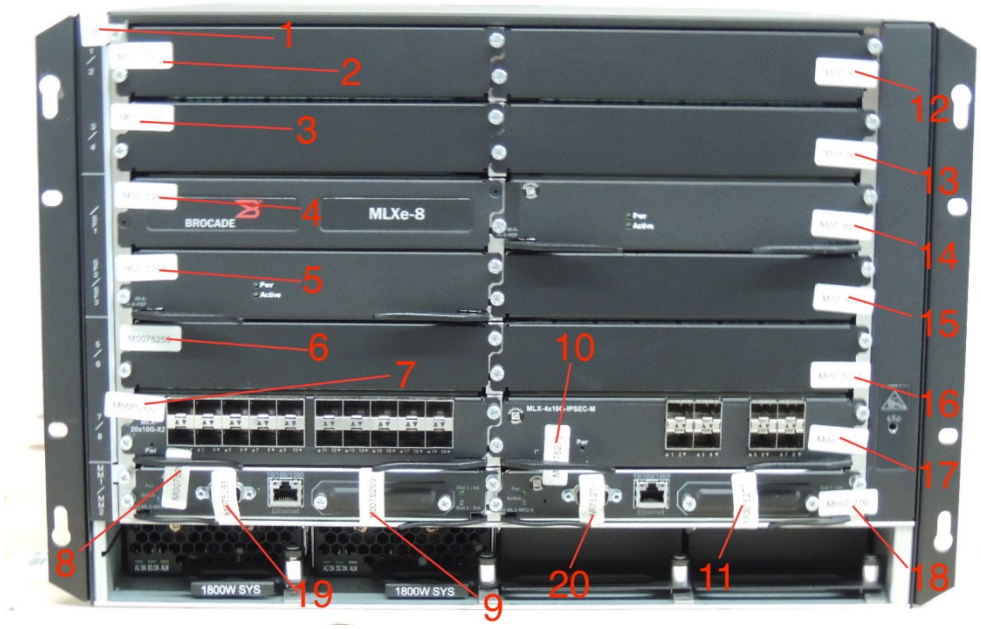

Figure 10 - Front view of Brocade MLXe-8 device with security seals

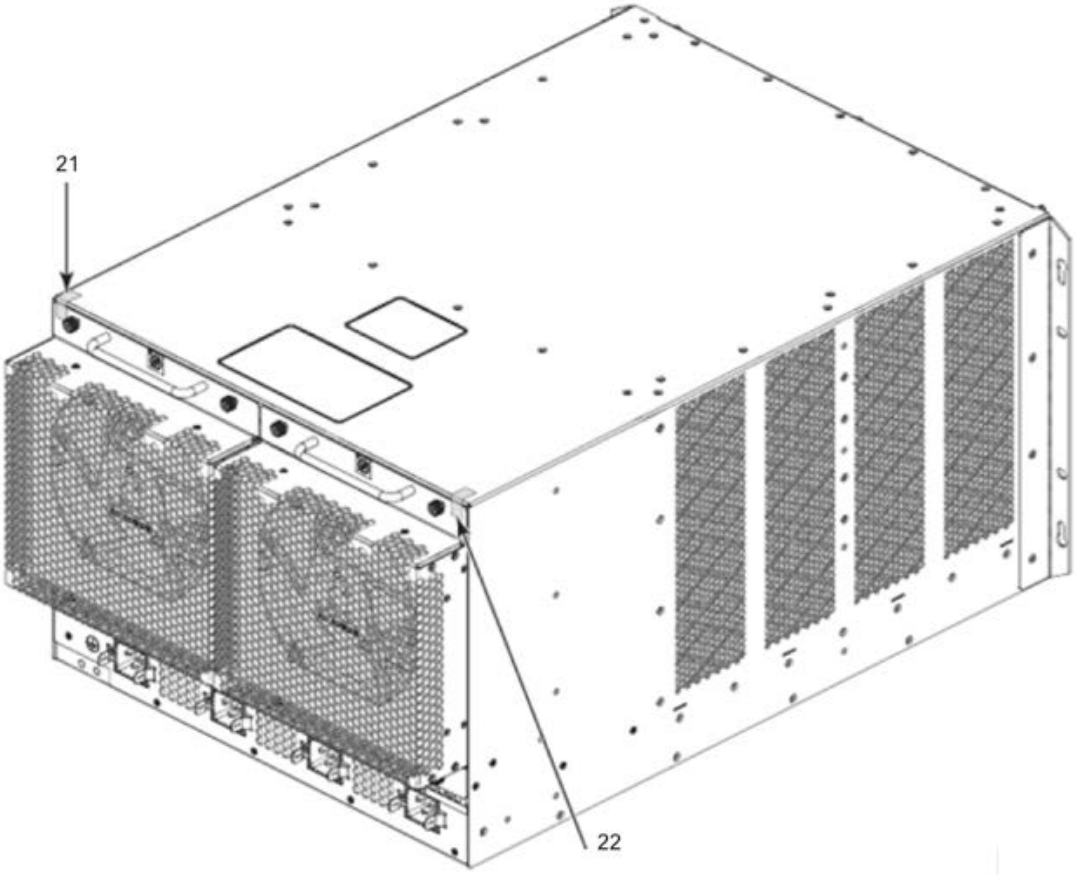

Figure 11 - Rear view of Brocade MLXe-8 device with security seals

11.3 Applying Tamper Evident Seals to a Brocade 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 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 back panel of the chassis to the flange of each of the two fan FRUs. See Figure 13 for correct seal orientation and positioning.

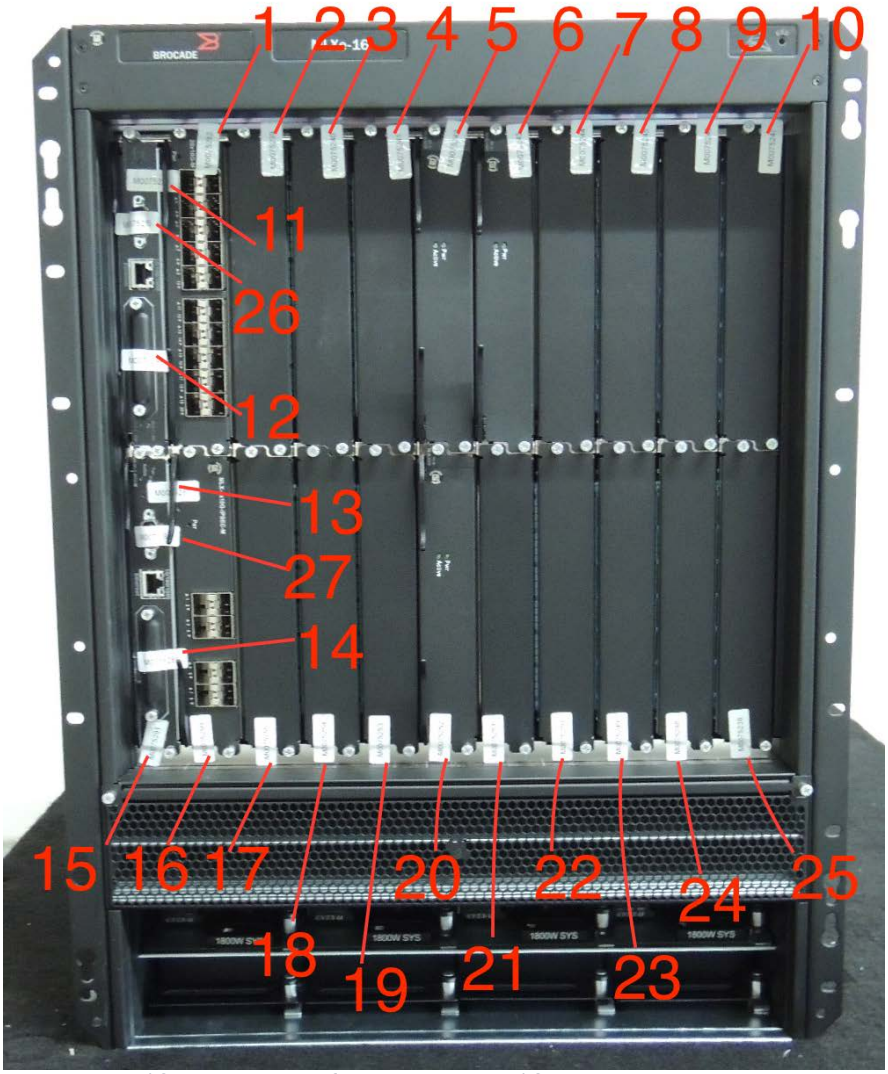

Figure 12 - Front view of Brocade MLXe-16 device with security seal

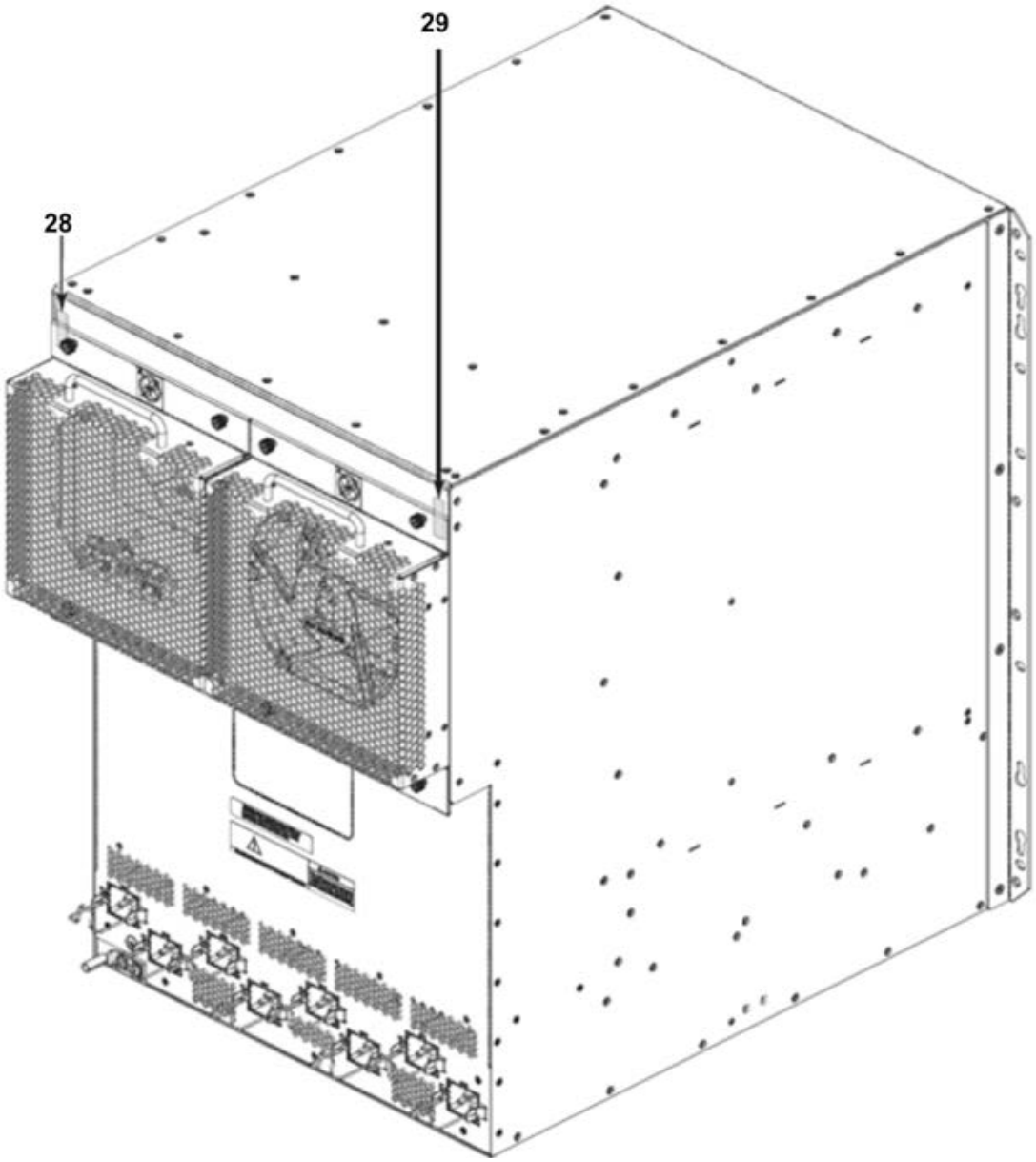

Figure 13 - Rear view of Brocade MLXe-16 device with security seals

12 Appendix B: Critical Security Parameters

The module supports the following CSPs and public keys:

1) SSHv2 Host RSA Private Key (2048 bit)
- 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

2) SSHv2 Client RSA Private Key
- 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

3) SSHv2 DH Group-14 Private Key (2048 bit)
- 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

4) SSHv2 DH Shared Secret Key (2048 bit)
- Description: Output from the DH Key agreement primitive - (K) and (H). Used in SSHv2 KDF to derive (client and server) session keys.
- 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

5) SSHv2/SCP Session Keys (128, 192 and 256 bit (AES CBC and AES CTR)
- Description: AES encryption key used to secure SSHv2/SCP
- Type: AES CBC Key
- Generation: N/A
- Establishment: SSHv2 DH Key Agreement and SSHv2 KDF (SP800-135 Section 5.2); allowed method as per FIPS 140-2 IG D.8 Scenario 4

- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
-Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

6) SSHv2/SCP Authentication Key (HMAC-SHA-1, 160 bits)
- 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

7) SSHv2 KDF Internal State
- Description: Used to generate Host encryption and authentication key
- Type: KDF
- 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

8) TLS Host RSA Private Key (RSA 2048 bit)
- 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

9) TLS Pre-Master Secret
- Description: Secret value used to establish the Session and Authentication key
- Type: TLS v1.0/1.1 and TLS v1.2 CSP
- Generation: N/A, established during the TLS v1.0/1.1 and TLS v1.2 handshake using RSA key transport
- Establishment: Key transport: RSA key wrapped over TLS v1.0/1.1 and TLS v1.2 session; allowed as per FIPS 140-2 IG D.9
- Entry: RSA key wrapped (after padding to block size) during TLS v1.0/1.1 and TLS v1.2 handshake
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

10) TLS Master Secret
- Description: 48 bytes secret value used to establish the TLS Session Key and
TLS Authentication Key
- 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

11) TLS KDF Internal State
- Description: Values of the KDF internal state.
- 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

12) TLS Session Key
- Description: 128 or 256 bit AES CBC key used to secure TLS v1.0/1.1 and TLS v1.2 sessions
- Type: AES CBC
- Generation: N/A
- Establishment: TLS v1.0/1.1 KDF and TLS v1.2 KDF as per SP800-135 Section 4.2.1 & 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4.
- Entry: N/A
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: User
- Zeroization: Session termination and "fips zeroize all" command

13) TLS Authentication Key
- Description: HMAC-SHA-1 key used to provide data authentication for TLS v1.0/1.1 sessions; HMAC-SHA-256 key 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

14) MP DRBG Seed
- 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

15) MP DRBG Value V
- 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

16) MP DRBG Key
- 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

17) MP DRBG Internal State
- 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

18) User Password
- Description: 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

19) Port Administrator Password
- Description: 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

20) Crypto-officer Password
- Description: 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

21) RADIUS Secret
- Description: Used to authenticate the RADIUS server (8 to 64 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 RAM and Compact Flash
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

22) TACACS+ Secret
- Description: Used to authenticate the TACACS+ server (8 to 64 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 RAM and Compact Flash
- Key-to-Entity: Process
- Zeroization: "fips zeroize all" command

**********Public Keys**********

23) Firmware Load RSA Public Key
- 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

24) SSHv2 Host RSA Public Key
- 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

25) SSHv2 Client RSA Public Key
- 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

26) SSHv2 DH Public Key
- Description: (2048 bit modulus); Used to establish shared secrets (SSHv2)

- 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

27) SSHv2 DH Peer Public Key
- Description: (2048 bit modulus); Used to establish shared secrets (SSHv2)
- Type: DH Peer Public Key
- Generation: N/A
- Establishment: N/A
- Entry: Plaintext
- Output: N/A
- Storage: Plaintext in RAM
- Key-to-Entity: Process

28) TLS Host Public Key (RSA 2048 bit)
- 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

29) TLS Peer Public Key (RSA 2048 bit)
- 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, Plaintext in Compact Flash
- Key-to-Entity: Process

30) ECDSA Public Key (P-384)
- Description: Public Key
- Type: ECDSA
- Generation: As per SP800-133 Section 6.1, key generation is performed as per FIPS 186-4 which is an Approved key generation method.
- Establishment: N/A
- Entry: N/A
- Output: Plaintext
- Storage: Plaintext in RAM, Plaintext in Compact Flash
- Key-to-Entity: IPSec Peer Role
- Zeroization: "fips zeroize all" command

31) ECDH Public Key (P-384)
- Description: 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
- Zeroization: "fips zeroize all" command

**********MACsec CSPs**********

32) Connectivity Association Key (CAK)
- Description: Connectivity Association Key - 128 bits in length
- 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
- Output: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Storage: Plaintext in RAM, Plaintext in Flash
- Key-to-Entity: Process User
- Zeroization: "fips zeroize all" command

33) Connectivity Key Name (CKN)
- Description: Connectivity Key Name – between 8 bits to 256bits in length
- 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
- Output: AES Encrypted & HMAC-SHA-1 authenticated over SSHv2 session
- Storage: Plaintext in RAM, Plaintext in Flash
- Key-to-Entity: Process User
- Zeroization: "fips zeroize all" command

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

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

36) Secure Association Key (SAK)
- Description: Secure association key
- Type: AES-GCM Key
- Generation: Approved as per FIPS 140-2 IG 7.10; derived from SP800-108 KDF
- Establishment: Key transport: AES key wrapped with the KEK; Allowed as per FIPS 140-2 IG D.9.
- Entry: Entered AES key wrapped with the KEK in MKA peer mode
- Output: Output AES key wrapped with the KEK in MKA server mode

- Storage: Plaintext in RAM, Plaintext in Broadcom chip
- Key-to-Entity: Process MACsec
- Zeroization: Session termination and "fips zeroize all" command

37) SP800-108 KDF State
- Description: KDF State
- 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

**********IPSec CSPs**********

38) ECDSA Private Key (P-384)
- Description: Private 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: N/A
- Output: N/A
- Storage: Local persistent on MM and running on Power PC Flash
- Key-to-Entity: IPSec Peer Role
- Zeroization: "fips zeroize all" command

39) ECDH Private Key (P-384)
- Description: 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

40) ECDH Shared Secret (P-384)
- Description: ECDH
- 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

41) IKEv2 Encrypt/Decrypt Key
- Description: Encryption/Decryption
- Type: AES 128 and AES 256
- 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

42) IKEv2 Authentication Key
- Description: Authentication
- Type: 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

43) ESP Encrypt/Decrypt Key
- Description: Encryption and Decryption
- Type: AES-256
- 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

44) IKEv2 KDF State
- Description: IKEv2 KDF State
- Type: 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

45) IKE Pre-Shared Key (PSK)
- Description: Pre-Shared Key
- Type: HMAC
- 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
- Output: Key transport: AES Encrypted & HMAC-SHA-1 authenticated over SCP/SSHv2 session; Approved as per FIPS 140-2 IG D.9
- Storage: Plaintext in RAM
- Key-to-Entity: IKEv2 SPI
- Zeroization: "fips zeroize all" command

46) LP DRBG Seed
- Description: Seeding material for the SP800-90A HASH_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

47) LP DRBG Value V
- 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

48) LP DRBG Value C
- 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

49) LP DRBG Internal State
- 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