DATA SHEET

Brocade MLX 4-Port 10 GbE IPsec Module

HIGHLIGHTS

- Provides an ideal solution for secure data center or hybrid cloud interconnect, campus core, and multisite connectivity, with lowest cost per encrypted bit
- Delivers hardware-based encryption with inline ports, helping to ensure data privacy without compromising performance or requiring complex deployment
- Leverages Suite B cryptographic algorithms, one of the industry's most stringent standards for interoperable network data encryption
- Supports jumbo frames as well as unicast and multicast features for voice, video, and data traffic in diverse, large-scale applications
- Maximizes investment protection through a programmable architecture provided by Brocade VersaScale Packet Processor technology

Pervasive Data Privacy without Compromising Network Performance

Today's organizations face a wide range of data privacy challenges, from cyber attacks and third-party snooping on private networks, to compliance requirements and growing demand for premium, secure services. Ensuring data privacy throughout the network is therefore imperative as organizations seek to enable secure operations without compromising growth, productivity, and profitability.

VPNs based on the IP Security (IPsec) protocol offer a cost-effective, scalable solution for service providers, enterprises, and public sector organizations seeking to securely connect remote sites, employees, and partners to networked systems and applications. IPsec provides robust security and encryption features to protect critical data, and can be deployed across any IP network. In addition, it functions efficiently end to end, at the network edge, and within the core network, making it ideal for site-to-site and various

Wire-Speed Embedded Encryption in a High-Performance Router

The Brocade® MLX® 4-port 10 GbE IPsec module for Brocade MLXe Core Routers provides inline IPsec encryption capabilities at wire speed, delivering pervasive data privacy without compromising performance or requiring complex deployments. With support for four ports of 10 GbE/1 GbE combo and four additional ports of 1 GbE, the module supports an industry-leading capacity of more than 44 Gbps per half-slot module and up to 128 ports of 10 GbE in a single Brocade MLXe system.The inline ports for IPsec deliver unmatched performance by requiring no service module to be used, freeing up slots in the chassis to be used for other routing applications.

Flexible Solution for Maximum Security

The Brocade MLX IPsec module is built on the Brocade VersaScale Packet Processor, designed to enable service innovation through programmability and flexibility without sacrificing performance. This programmability enables one of the strongest cryptographic suites for IPsec—Suite B—to be added in hardware to the Brocade MLXe Series. For additional security, the module supports IEEE 802.1AE (MACsec), which provides 128-bit MAC-layer hop-by-hop encryption for Local Area Network (LAN) use cases. Other advantages of the Brocade MLX IPsec module include multi-VRF support, deep buffers of 2 GB per module, and jumbo frames (9,000 bytes) support for dynamic traffic patterns caused by applications in cloud, mobile, and Big Data.

The module is well-suited for Internet route scalability, with support for up to 512,000 IPv4 routes or 256,000 IPv6 routes in the FIB. The module also supports all existing Brocade MLXe software features for IPv4, IPv6, Layer 2/3, and SDN OpenFlow functionality, and can coexist on the same Brocade MLXe system with all other 10 GbE, 40 GbE, and 100 GbE Brocade MLXe interface modules.

The transparent, inline IPsec encryption within the Brocade MLXe Router enables simplification and improved performance of secure network architectures. It enables the removal of dedicated encryption appliances or off-loads the burden of encryption processing from firewalls, thereby eliminating massive performance degradation of other security functions. Configuration and management of the IPsec encryption is performed along with the network port and other routing functions, simplifying operations and management. This module requires no additional software licenses or support.

Full Confidence in Data Integrity with Suite B

The Brocade MLX IPsec module provides Suite B Algorithm Suite 2 Encryption support in hardware. Suite B is globally recognized as an advanced, publicly available standard for cryptography. Brocade is implementing 256-bit IP-layer encryption with Suite B, providing significantly higher network security than most commonly used standards and ensuring confidence in the integrity of data being transmitted. Suite B cryptography secures information traveling over networks using four algorithms:

- **Encryption based on the Advanced Encryption Standard (AES):** Symmetric encryption
- **Elliptic Curve Digital Signature Algorithm (ECDSA):** Digital signatures
- **Elliptic Curve Diffie-Hellman (ECDH):** Key agreement
- **Secure Hash Algorithm 2 (SHA-384):** Message digest

Brocade Global Services

Brocade Global Services has the expertise to help organizations build scalable, efficient cloud infrastructures. Leveraging 15 years of expertise in storage, networking, and virtualization, Brocade Global Services delivers world-class professional services, technical support, and education services, enabling organizations to maximize their Brocade investments, accelerate new technology deployments, and optimize the performance of networking infrastructures.

Affordable Aquisition Options

Brocade Capital Solutions helps organizations easily address their IT requirements by offering flexible network acquisition and support alternatives. Organizations can select from purchase, lease, Brocade Network Subscription, and Brocade Subscription Plus options to align network acquisition with their unique capital requirements and risk profiles. To learn more, visit www.Brocade.com/CapitalSolutions.

Maximizing Investments

To help optimize technology investments, Brocade and its partners offer complete solutions that include professional services, technical support, and education. For more information, contact a Brocade sales partner or visit www.brocade.com.

Maximum Port Densities on Brocade MLXe Series Routers

Brocade MLXe Chassis	Wire-Speed 1 GbE Ports	Wire-Speed 10 GbE Ports
Brocade MLXe-4	16	16
Brocade MLXe-8	32	32
Brocade MLXe-16	64	64
Brocade MLXe-32	128	128

Software Feature Highlights

Strong Cryptography and Authentication

- Suite B Algorithm Suite 2 support for 256-bit IP-layer encryption
- Advanced Encryption Standard (AES-256)
  - Minimum Level of Security (minLOS): 192 bits
  - Galois Counter Mode (GCM) for ESP Encryption
- Authentication (Digital Signature)
  - X.509 v3 certificate for authentication of peers
  - ECDSA P-384 curve and the SHA-384 hash function for digital signature
- Internet Key Exchange/Establishment: IKEv2 (RFC 5996)
  - PRF-HMAC-SHA-384 (RFC 4868) for key generation/derivation
  - Cipher Block Chaining (CBC) for IKE encryption
  - ECDH over the curve P-384 (DH Group 20) for key exchange
  - Integrity for IKEv2 packet payload using SHA-384

Virtual Tunnel Interface (VTI)

- Multi-VRF support
  - IPv4 source and destination addresses of tunnel can be in either same or different VRF(s)
- Quality of Service (QoS)
  - Support for different QoS for voice, video, and data on the same VTI
  - COS from original packet is copied to ESP packet
- Routing
  - Support for OSPF and BGP on VTI
- Multicast
  - Support for PIM-SM and IGMP (static only) on VTI
  - Ingress and egress statistics
- Link aggregation
  - LAG support for load sharing and operational efficiency High availability
  - Support for high availability of VTI during switchover and upgrade, to ensure reliability and minimize traffic impact

Management

- PKI/DSA for Certificate Authority (CA) association, enrollment, and management
- X.509 v3 digital certificate management support—manual and protocol-based
  - Manually import certificates from local flash storagez
  - Online Certificate Status Protocol (OCSP)
  - Simple Certificate Enrollment Protocol (SCEP)
- SNMP v1/v2c and SNMP v3 for IPsec tunnel monitoring
- IPv4 and IPv6 management support
- In-band and out-of-band management
- Dead Peer Detection (DPD)

RFC Conformance for Encryption

- RFC5996 Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 4303 IP Encapsulating Security Payload (ESP)
- RFC 6379 Suite B Cryptographic Suites for IPsec
- RFC 5903 Elliptic Curve Groups Modulo a Prime (ECP Groups) for IKE and IKEv2
- RFC 4868 Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
- RFC 4754 IKE and IKEv2 Authentication using the Elliptic Curve Digital Signature Algorithm (ECDSA)
- RFC 4106 The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
- RFC 3602 AES with 128-bit keys in CBC Mode
- RFC 4806 Online Certificate Status Protocol (OCSP) Extensions to IKEv2
- FIPS PUB 186-3 Digital Signature Standard (DSS)
- SP800-56A Recommendationfor Pair-Wise Key EstablishmentSchemes Using Discrete Logarithm Cryptography

Product Support for Optics with Key Standards and Features

Optic Type	IEEE Standards	Domestic Safety Standards	International Safety Standards	Wavelength (nm)	Fiber Type	Maximum Cable Distance	Digital Optical Monitoring
1 GbE Optics							
E1MG-SX-OM	802.3z	FDA 21CFR 1040.10 Class 1, CSA 60950-1-03/ UL60950-1	EN 60825-1, EN 60950-1	850	MMF	220 m to 550 m	Yes
E1MG-LX-OM	802.3z			1,310	MMF/SMF	550 m to 10 km	Yes
E1MG-LHA-OM	802.3z			1,550	SMF	70 km	Yes
E1MG-LHB	802.3z			1,550		150 km with b0.18 dB/km cable, 91 km with standard 0.3 dB/km cable	No
E1MG-CWDM80-1XXX	802.3z			1,470 to 1,610		80 km	No
10 GbE Optics							
10G-SFPP-SR	802.3ae	FDA 21CFR 1040.10 Class 1, CSA 60950-1-03/ UL 60950-1	EN 60825-1, EN 60950-1	850	MMF	26 m to 300 m	Yes
10G-SFPP-LR	802.3ae			1,310	SMF	10 km	
10G-SFPP-ER	802.3ae			1,550	SMF	40 km	
10G-SFPP-ZR	802.3ae			1,550	SMF	80 km	
10G-SFPP-ZRD-T	802.3-2005 Clause 52 standard			102 C-band tunable wavelengths from 1,528 to 1,568 (50 GHz apart)	SMF	80 km	
10G-SFPP-LRM	802.3ae			1,310	MMF	220 m	
10G-SFPP-TWX-0XXX	802.3ae	Direct-attached SFP+ Twinax copper cables				1 m, 3 m, 5 m	No

Brocade MLX 4-Port 10 GbE IPsec Module Ordering Information

Part Number	Description
BR-MLX-10GX4-IPSEC-M	Brocade MLX 4-port 10 GbE/1 GbE combo and 4-port 1 GbE (-M) IPsec module with 512,000 IPv4 routes or 240,000 IPv6 routes in hardware

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com

BROCADE